Complete Software Guide for Junos® OS for EX4300 Switches, Release 13.2X50

Published: 2013-09-04

Copyright © 2013, Juniper Networks, Inc.
Table of Contents

About the Documentation ................................................... xcv
Documentation and Release Notes ......................................... xcv
Supported Platforms .......................................................... xcv
Using the Examples in This Manual ........................................ xcv
  Merging a Full Example .................................................. xcvi
  Merging a Snippet ........................................................ xcvi
Documentation Conventions ................................................. xcvii
Documentation Feedback .................................................... xcvi
Requesting Technical Support ................................................ xcix
  Self-Help Online Tools and Resources ................................ xcix
  Opening a Case with JTAC ................................................ c

Part 1  Getting Started with ELS
Chapter 1  Getting Started with ELS ..................................... 3
  Getting Started ........................................................... 3
    Getting Started with Enhanced Layer 2 Software .................. 3
    Using the ELS Translator Tool ....................................... 3
    Configuring a VLAN .................................................... 4
    Configuring the Native VLAN Identifier ............................ 4
    Configuring Layer 2 Interfaces ....................................... 4
    Configuring Layer 3 Interfaces ....................................... 5
    Configuring an IRB Interface ........................................ 5
    Configuring an Aggregated Ethernet Interface and Configuring LACP on That Interface ........................................ 6
    Enhanced Layer 2 CLI Configuration Statement and Command Changes .................................................. 7
  Enhanced Layer 2 CLI Configuration Statement and Command Changes .................................................. 15

Part 2  Software Features Overview
Chapter 2  Software Features Overview ................................. 27
  Software Features Overview ............................................. 27
    EX Series Switch Software Features Overview .................... 27
    EX Series Virtual Chassis Software Features Overview ........ 75
# Part 3 System Setup

## Chapter 3 Overview

- Software Overview ......................................................... 111
  - Understanding Software Infrastructure and Processes ........ 111
  - Routing Engine and Packet Forwarding Engine ................. 111
  - Junos OS Processes .................................................... 112

## Chapter 4 Configuration

- Initial Configuration .................................................... 115
  - Configuring the LCD Panel on EX Series Switches (CLI Procedure) 115
  - Disabling or Enabling Menus and Menu Options on the LCD Panel 115
  - Configuring a Custom Display Message ................................. 116
  - Configuring Date and Time for the EX Series Switch (J-Web Procedure) 117
  - Configuring System Identity for an EX Series Switch (J-Web Procedure) 118
- Configuration Statements ............................................... 119
  - `arp (System)` ............................................................ 120
  - `authentication-key` .................................................. 121
  - `auxiliary` .............................................................. 122
  - `boot-server (NTP)` .................................................... 123
  - `broadcast` ................................................................ 124
  - `broadcast-client` ........................................................ 125
  - `console (System Ports)` ................................................. 126
  - `default-address-selection` ............................................. 127
  - `domain-name` ............................................................ 128
  - `gre-path-mtu-discovery` .............................................. 128
  - `host-name` ............................................................... 129
  - `icmpv4-rate-limit` ....................................................... 129
  - `icmpv6-rate-limit` ....................................................... 130
  - `inet6-backup-router` .................................................... 131
  - `internet-options` ......................................................... 132
  - `ipip-path-mtu-discovery` ............................................. 133
  - `ipv6-duplicate-addr-detection-transmits` ......................... 133
  - `ipv6-path-mtu-discovery` ............................................. 134
  - `ipv6-path-mtu-discovery-timeout` .................................. 134
  - `ipv6-reject-zero-hop-limit` ......................................... 135
  - `lcd-menu` ................................................................ 136
  - `location (System)` ........................................................ 138
  - `menu-item` ............................................................... 140
  - `multicast-client` ......................................................... 143
  - `no-multicast-echo` .................................................... 144
  - `no-ping-record-route` .................................................. 145
  - `no-ping-time-stamp` .................................................... 145
  - `no-redirects (IPv4 Traffic)` .......................................... 146
  - `no-tcp-rfc1323-paws` ................................................ 147
  - `no-tcp-rfc1323` ......................................................... 147
  - `ntp` ..................................................................... 148
  - `path-mtu-discovery` .................................................... 148
  - `peer (NTP)` .............................................................. 149
  - `port-type` ............................................................... 150

---

Copyright © 2013, Juniper Networks, Inc.
## Chapter 5  Administration ................................................... 159

**Operational Commands** .................................................. 159
- clear chassis display message ........................................ 160
- clear system reboot .................................................. 163
- configure .......................................................... 167
- op .............................................................. 169
- request chassis pic ................................................... 171
- request chassis routing-engine master .................................. 175
- request system halt .................................................. 180
- request system logout .............................................. 186
- request system power-off ........................................... 187
- request system reboot ............................................... 191
- request system scripts convert ..................................... 198
- request system scripts refresh-from commit ....................... 200
- request system scripts refresh-from event ....................... 201
- request system scripts refresh-from op .......................... 202
- request system storage cleanup ................................... 203
- restart .......................................................... 213
- set chassis display message ....................................... 223
- set date ......................................................... 226
- show chassis fan ................................................... 227
- show chassis firmware .............................................. 240
- show chassis lcd ................................................... 251
- show configuration ................................................ 264
- show host ......................................................... 267
- show ntp associations .............................................. 268
- show ntp status .................................................. 270
- show system firmware ............................................. 273
- show system reboot ................................................. 275
- show system software ............................................. 278
- show system storage .............................................. 286
- show system switchover ........................................... 292
- show system uptime ................................................ 296
- show system users ................................................ 301
- show system virtual-memory ...................................... 305
- show task replication ............................................... 363
- show version ...................................................... 365
- show version fpc ................................................. 378

## Chapter 6  Troubleshooting Procedures ............................... 379

- Troubleshooting Loss of the Root Password .......................... 379
Table of Contents

Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure) ........................................... 419
Configuration Statements .................................................. 420
  allow-commands ..................................................... 420
  allow-configuration ................................................ 421
  announcement ....................................................... 422
  archive-sites ....................................................... 422
  authentication (Login) ............................................. 423
  authentication-order .............................................. 424
  change-type ......................................................... 425
  class (Assigning a Class to an Individual User) .............. 425
  class (Defining Login Classes) ................................... 426
  class-usage-profile ............................................... 427
  counters ............................................................ 428
  deny-commands .................................................... 428
  deny-configuration ............................................... 429
  destination-classes .............................................. 430
  fields (for Interface Profiles) ................................... 431
  file (Associating with a Profile) ................................ 432
  file (Configuring a Log File) .................................... 433
  files ...................................................................... 434
  filter-profile ........................................................ 435
  format .................................................................... 436
  full-name .............................................................. 436
  idle-timeout (System-Login) ....................................... 437
  interface-profile .................................................... 438
  interval (Accounting Options) .................................. 439
  login ...................................................................... 440
  login-alarms .......................................................... 441
  login-tip ................................................................. 441
  maximum-length ...................................................... 442
  message .................................................................. 443
  mib-profile ............................................................ 444
  minimum-changes .................................................... 445
  minimum-length ..................................................... 446
  object-names .......................................................... 447
  operation ............................................................... 447
  password (Login) ..................................................... 448
  permissions ............................................................ 449
  radius-options (edit system) ...................................... 450
  retry-options .......................................................... 451
  root-authentication ................................................. 452
  root-login .............................................................. 453
  routing-engine-profile ............................................. 454
  size ...................................................................... 455
  source-classes ........................................................ 455
  start-time (Log File Transfer) ..................................... 456
  tacplus-options ....................................................... 457
  tacplus-server ....................................................... 458
traceoptions (Address-Assignment Pool) ......................... 459
transfer-interval .................................................. 460
uid ................................................................. 461
user (Access) .................................................... 462

Chapter 12 Administration ............................................. 463
Routine Monitoring .................................................. 463
Managing Users (J-Web Procedure) .............................. 463
Operational Commands ............................................. 465
request message ................................................... 466
show subscribers ................................................... 467

Chapter 13 Troubleshooting Procedures ............................ 485
Troubleshooting Loss of the Root Password ...................... 485

Part 6 Configuration and File Management

Chapter 14 Overview .................................................. 491
Software Overview .................................................. 491
Understanding Software Infrastructure and Processes ....... 491
Routing Engine and Packet Forwarding Engine ............... 491
Junos OS Processes ............................................... 492
Configuration Files Overview ...................................... 493
Understanding Configuration Files for EX Series Switches .. 493
Using the CLI Viewer in the J-Web Interface to View Configuration Text ... 494
Using the CLI Editor in the J-Web Interface to Edit Configuration Text ... 494
Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text .................. 494
Understanding Automatic Refreshing of Scripts on EX Series Switches ... 496
Understanding Autoinstallation of Configuration Files ........ 497
Typical Uses for Autoinstallation ................................ 497
Autoinstallation Configuration Files and IP Addresses ....... 497
Typical Autoinstallation Process on a New Switch .......... 498
Configuration Files Terms ........................................ 499

Chapter 15 Configuration ............................................ 501
Configuration Tasks ................................................ 501
Uploading a Configuration File (CLI Procedure) ............... 501
Uploading a Configuration File (J-Web Procedure) .......... 503
Loading a Previous Configuration File (CLI Procedure) .... 503
Reverting to the Default Factory Configuration for the EX Series Switch ... 504
Reverting to the Factory-Default Configuration by Using the LCD Panel ............................................. 505
Reverting to the Factory-Default Configuration by Using the request system zeroize Command ................. 506
Reverting to the Factory-Default Configuration by Using the load factory-default Command .................. 506
Reverting to the Rescue Configuration for the EX Series Switch .......... 507
Setting or Deleting the Rescue Configuration (CLI Procedure) ........ 508
Setting or Deleting the Rescue Configuration (J-Web Procedure) .... 509
Table of Contents

Chapter 16 Administration ................................................... 523

Routine Monitoring .............................................................. 523

Managing Configuration Files Through the Configuration History (J-Web Procedure) .................................................. 523
Displaying Configuration History ............................................. 523
Displaying Users Editing the Configuration ................................ 524
Comparing Configuration Files with the J-Web Interface ................. 525
Downloading a Configuration File with the J-Web Interface ............. 525
Loading a Previous Configuration File with the J-Web Interface ........ 525
Verifying Autoinstallation Status ............................................. 526

Operational Commands ........................................................... 527

clear log .............................................................................. 528
clear system commit ............................................................. 529
file archive ......................................................................... 530
file checksum md5 ............................................................... 532
file checksum sha1 ............................................................... 533
file checksum sha-256 .......................................................... 534
file compare ................................................................. 535
file copy ........................................................................... 538
file delete ........................................................................... 540
file list .............................................................................. 541
file rename ......................................................................... 543
file show ............................................................................ 545
request system configuration rescue delete ......................... 547
request system configuration rescue save ............................ 548
request system scripts refresh-from commit ...................... 549
request system scripts refresh-from event ......................... 550
request system scripts refresh-from op ............................... 551
request system zeroize ......................................................... 552
show system commit ............................................................ 557
show system configuration archival .................................... 559
show system configuration rescue ....................................... 560
show system rollback .......................................................... 562
test configuration ............................................................... 564

Configuration Statements ......................................................... 513

archival ................................................................................. 513
archive-sites (Configuration File) ............................................. 514
autoinstallation ..................................................................... 516
synchronize (Commit configuration) ......................................... 517
configuration ..................................................................... 518
configuration-servers .......................................................... 519
interfaces ............................................................................ 520
transfer-interval (Configuration) ............................................. 521
transfer-on-commit ............................................................... 522

Configuring Autoinstallation of Configuration Files (CLI Procedure) ...... 509
Using the Commit Options to Commit Configuration Changes (J-Web Procedure) .................................................. 511

Copyright © 2013, Juniper Networks, Inc.
## Chapter 17 Troubleshooting Procedures

- Troubleshooting Loss of the Root Password

## Part 7 Software Installation

### Chapter 18 Overview

- Installation Overview
- Understanding Software Installation on EX Series Switches
- Overview of the Software Installation Process
- Software Package Security
- Installing Software on a Virtual Chassis
- Installing Software on Switches with Redundant Routing Engines
- Installing Software Using Automatic Software Download
- Troubleshooting Software Installation
- Understanding System Snapshot on EX Series Switches
- Understanding Resilient Dual-Root Partitions on Switches
- Resilient Dual-Root Partition Scheme (Junos OS Release 10.4R3 and Later)
- Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature
- Earlier Partition Scheme (Junos OS Release 10.4R2 and Earlier)
- Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases
- Junos OS Package Names

### Software Overview

- Understanding Software Infrastructure and Processes
- Routing Engine and Packet Forwarding Engine
- Junos OS Processes

### Licenses Overview

- Understanding Software Licenses for EX Series Switches
- Purchasing a Software Feature License
- Features Requiring a License on EX2200 Switches
- Features Requiring a License on EX3300 Switches
- Features Requiring a License on EX4300 Switches
- Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches
- License Warning Messages

## Chapter 19 Configuration

- Registering the Switch
- Registering the EX Series Switch with the J-Web Interface
- Booting the Switch
- Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive
- Creating a Snapshot and Using It to Boot an EX Series Switch
- Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch
- Creating a Snapshot on an Internal Flash Drive and Using It to Boot the Switch
Installation from the Boot Loader Generates ‘cannot open package’ Error ........................................ 659
Troubleshooting a Switch That Has Booted from the Backup Junos OS Image ........................................ 660
Resilient Dual-Root Partitions Frequently Asked Questions ........................................ 661
What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Enabled? ........................................ 661
What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Not Enabled? ........................................ 662
How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System? ........................................ 663

Part 8 System Monitoring
Chapter 22 Overview ........................................ 667
Software Overview ........................................ 667
Understanding Software Infrastructure and Processes ........................................ 667
Routing Engine and Packet Forwarding Engine ........................................ 667
Junos OS Processes ........................................ 668
Alarms Overview ........................................ 669
Understanding Alarm Types and Severity Levels on EX Series Switches ........................................ 669
Dashboard Overview ........................................ 670
Dashboard for EX Series Switches ........................................ 670
System Information Panel ........................................ 671
Health Status Panel ........................................ 673
Capacity Utilization Panel ........................................ 675
Alarms Panel ........................................ 675
File System Usage ........................................ 675
Chassis Viewer ........................................ 675
Hardware/CLI Terminology Mapping Overview ........................................ 686
EX4300 Switch Hardware and CLI Terminology Mapping ........................................ 686

Chapter 23 Configuration ........................................ 689
Configuration Statements ........................................ 689
facility-override ........................................ 689
file (System Logging) ........................................ 690
files ........................................ 691
host (System) ........................................ 692
interface (Accounting or Sampling) ........................................ 694
log-prefix (System) ........................................ 694
match ........................................ 695
size (System) ........................................ 696
structured-data ........................................ 697
syslog (System) ........................................ 698
time-format ........................................ 700
time-zone ........................................ 701
user (System Logging) ........................................ 703
world-readable (System) ........................................ 704
Part 9  System Services

Chapter 25  Overview .......................................................1189

Software Overview ......................................................1189
  Understanding Software Infrastructure and Processes .................1189
    Routing Engine and Packet Forwarding Engine .......................1189
    Junos OS Processes .................................................1190

DHCP Local Server .....................................................1191
  Extended DHCP Local Server Overview ................................1192
    Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools ...1192
    Providing DHCP Client Configuration Information .................1193
    Minimal Configuration for Clients ................................1194
    DHCP Local Server and Address-Assignment Pools ..................1194
    DHCP Liveness Detection ...........................................1195

DHCPv6 Local Server Overview .......................................1196

DHCP Local Server Handling of Client Information Request Messages ...........................................1197

DHCP Duplicate Client Differentiation Using Client Subinterface

  Overview ..............................................................1198

Group-Specific DHCP Local Server Options ................................1199

Understanding Dynamic Reconfiguration of Extended DHCP Local Server

  Clients ...............................................................1200
  Default Client/Server Interaction ..................................1200
  Dynamic Client/Server Interaction for DHCPv4 .......................1200
  Dynamic Client/Server Interaction for DHCPv6 ......................1201
  Dynamic Configuration Options ....................................1201

DHCP Snooping Support ................................................1203

DHCP Auto Logout Overview ...........................................1204
  Auto Logout Overview ................................................1204
  How DHCP Identifies and Releases Clients .........................1205
  Option 60 and Option 82 Requirements ................................1206

Address-Assignment Pools Overview ................................1206

show chassis led ......................................................1042
show chassis location .................................................1052
show chassis pic .......................................................1056
show chassis routing-engine ........................................1070
show log ...............................................................1091
show pfe next-hop ....................................................1094
show pfe route .........................................................1099
show pfe terse .........................................................1105
show system alarms ..................................................1107
show system audit .....................................................1109
show system buffers ..................................................1117
show system connections .............................................1124
show system core-dumps ..............................................1143
show system directory-usage .........................................1155
show system processes ..............................................1159
Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address ......................................................... 1207
Multiple Address Assignment for DHCPv6 Clients .................. 1208
Multiple Address Assignment Using Local Address Pools or RADIUS .... 1208
Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment ......................................................... 1208
Centrally Configured Opaque DHCP Options .......................... 1209
Data Flow for RADIUS-Sourced DHCP Options ...................... 1211
Multiple VSA 26-55 Instances Configuration .......................... 1212
DHCP Options That Cannot Be Centrally Configured .................. 1212
Port Number Requirements for DHCP Firewall Filters ............... 1213
DHCP Relay Agent .......................................................... 1214
Extended DHCP Relay Agent Overview ............................... 1215
Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers .......................................................... 1216
DHCP Liveness Detection ................................................... 1217
DHCP Relay Proxy Overview .............................................. 1218
Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers .......................................................... 1218
DHCPv6 Relay Agent Overview .......................................... 1220
DHCP Duplicate Client Differentiation Using Client Subinterface Overview .......................................................... 1221
Group-Specific DHCP Relay Options .................................... 1221
DHCP Snooping Support ..................................................... 1222
DHCP Auto Logout Overview .............................................. 1223
Auto Logout Overview ....................................................... 1223
How DHCP Identifies and Releases Clients ............................ 1224
Option 60 and Option 82 Requirements ................................ 1225
Public Key Cryptography Overview ...................................... 1225
Understanding Public Key Cryptography on Switches ................ 1226
Public Key Infrastructure (PKI) and Digital Certificates .............. 1226
Self-Signed Certificates Overview ....................................... 1227
Understanding Self-Signed Certificates on EX Series Switches .... 1227

Chapter 26 Configuration .................................................. 1229
DHCP Local Server Examples ............................................. 1229
Example: Minimum Extended DHCP Local Server Configuration .... 1229
Example: Extended DHCP Local Server Configuration with Optional Pool Matching .................................................. 1230
Example: Configuring Group Liveness Detection for DHCP Local Server Clients .................................................. 1231
DHCP Relay Agent Examples ............................................. 1234
Example: Minimum DHCP Relay Agent Configuration .............. 1234
Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings ....................... 1235
Example: Configuring DHCP Snooping Support for DHCP Relay Agent .... 1239

Copyright © 2013, Juniper Networks, Inc.

xv
Configuration Tasks ................................................................. 1240
Configuring DHCP Services (J-Web Procedure) ......................... 1241
  Configuring DHCP Services (J-Web Procedure) on EX Series
  Switches ........................................................................... 1241
  Configuring DHCP Services on EX4300 Switches (J-Web
  Procedure) ................................................................. 1243
  Configuring a DHCP SIP Server (CLI Procedure) ..................... 1248
  Configuring a DHCP Client (CLI Procedure) ......................... 1249
  Configuring a DHCP Server on Switches (CLI Procedure) ........ 1250
  Configuring an Extended DHCP Server on a Switch ................. 1250
  Configuring a Legacy DHCP Server on a Switch (CLI Procedure) .. 1251
  Configuring an Extended DHCP Relay Server on EX Series Switches (CLI
  Procedure) ................................................................ 1252
Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed
  Certificates (CLI Procedure) ................................................. 1253
Manually Generating Self-Signed Certificates on Switches (CLI
  Procedure) .................................................................. 1254
Generating a Public-Private Key Pair on Switches ....................... 1254
Generating Self-Signed Certificates on Switches ....................... 1254
Deleting Self-Signed Certificates (CLI Procedure) ...................... 1255
Configuration Tasks for DHCP Local Server ................................. 1255
  Using External AAA Authentication Services with DHCP ............ 1256
  Guidelines for Configuring Support for DHCP Duplicate Clients ... 1257
  Configuring DHCP Duplicate Client Support .......................... 1258
  Grouping Interfaces with Common DHCP Configurations .......... 1258
  Guidelines for Configuring Interface Ranges ........................... 1259
  Overriding Default DHCP Local Server Configuration Settings .... 1261
  Specifying the Maximum Number of DHCP Clients Per Interface 1262
  Disabling ARP Table Population ........................................... 1263
  Automatically Logging Out DHCP Clients ............................... 1264
  Enabling Processing of Client Information Requests ................ 1265
  Specifying the Delegated Address Pool for IPv6 Prefix Assignment . 1266
  Enabling DHCPv6 Rapid Commit Support ............................ 1267
  Deleting DHCP Local Server and DHCP Relay Override Settings .... 1267
  Configuring Extended DHCP Local Server Dynamic Client
      Reconfiguration ............................................................. 1268
  Configuring Dynamic Reconfiguration Attempts for DHCP Clients .... 1269
  Configuring Deletion of the Client When Dynamic Reconfiguration Fails .... 1270
  Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated
      Disconnect .................................................................. 1270
  Configuring a Token for DHCP Local Server Authentication .......... 1271
  Preventing Binding of Clients That Do Not Support Reconfigure
      Messages .................................................................... 1271
  Requesting DHCP Local Server to Initiate Reconfiguration of Client
      Bindings .................................................................... 1272
  Configuring Detection of DHCP Local Server Client Connectivity .... 1273
  Configuring DHCP Snooped Packets Forwarding Support for DHCP Local
      Server ....................................................................... 1274
  Configuring Passwords for Usernames .................................... 1276
username-include (DHCP Local Server) ................................. 1385
version (BFD) ............................................................. 1386
DHCP Relay Agent Configuration Statements ............................. 1386
[edit forwarding-options dhcp-relay] Hierarchy Level ................. 1386
  Supported Statements in the [edit forwarding-options dhcp-relay]
    Hierarchy Level .................................................. 1387
  Unsupported Statements in the [edit forwarding-options dhcp-relay]
    Hierarchy Level .................................................. 1387
access (Dynamic Access Routes) ........................................ 1392
access-internal (Dynamic Access-Internal Routes) ..................... 1393
active-server-group ................................................... 1394
allow-snooped-clients ................................................ 1395
always-write-giaddr ................................................... 1396
always-write-option-82 ................................................. 1397
authentication (DHCP Relay Agent) .................................... 1398
bfd ........................................................................... 1399
circuit-id (DHCP Relay Agent) ......................................... 1400
circuit-type (DHCP Relay Agent) ....................................... 1401
client-discover-match (DHCP Relay Agent) ............................. 1402
client-id (DHCP Relay Agent) .......................................... 1403
delimiter (DHCP Relay Agent) .......................................... 1404
detection-time ............................................................... 1405
dhcp-relay ................................................................. 1406
dhcpv6 (DHCP Relay Agent) ............................................. 1407
disable-relay .................................................................. 1408
domain-name (DHCP Relay Agent) ...................................... 1409
drop (DHCP Relay Agent Option) ....................................... 1410
duplicate-clients-on-interface (DHCP Relay Agent) .................. 1411
dynamic-profile (DHCP Relay Agent) ................................... 1412
failure-action ............................................................... 1413
forward-snooped-clients (DHCP Relay Agent) ......................... 1414
group (DHCP Relay Agent) .............................................. 1415
holddown-interval ........................................................ 1416
interface (DHCP Relay Agent) .......................................... 1417
interface-client-limit (DHCP Relay Agent) ............................ 1418
interface-delete (Subscriber Management or DHCP Client Management) ................................................... 1419
interface-name (DHCP Relay Agent) ................................... 1420
layer2-unicast-replies ................................................... 1421
liveness-detection ........................................................ 1422
local-server-group (DHCP Relay Agent Option) ....................... 1423
mac-address (DHCP Relay Agent) ...................................... 1424
method ...................................................................... 1425
minimum-interval ........................................................ 1426
minimum-receive-interval ............................................... 1427
multiplier ................................................................. 1428
next-hop (Dynamic Access-Internal Routes) ........................... 1429
no-adaptation ............................................................. 1430
no-allow-snooped-clients ............................................... 1431
no-bind-on-request (DHCP Relay Agent) ............................................. 1441
option-60 (DHCP Relay Agent) ..................................................... 1442
option-82 (DHCP Relay Agent) .................................................... 1443
option-number (DHCP Relay Agent Option) ...................................... 1444
overrides (DHCP Relay Agent) .................................................... 1445
password (DHCP Relay Agent) ..................................................... 1447
preference (Subscriber Management) ............................................. 1448
prefix (DHCP Relay Agent) .......................................................... 1449
proxy-mode .................................................................................. 1451
relay-agent-interface-id (DHCPv6 Relay Agent) ................................ 1452
relay-agent-remote-id (DHCPv6 Relay Agent) .................................... 1453
relay-option (DHCP Relay Agent) .................................................. 1454
relay-option-82 ............................................................................. 1455
relay-server-group (DHCP Relay Agent Option) ............................... 1456
replace-ip-source-with .................................................................. 1457
routing-instance-name (DHCP Relay Agent) .................................... 1458
send-release-on-delete (DHCP Relay Agent) .................................... 1459
server-group ............................................................................... 1460
service-profile (DHCP Relay Agent) ............................................. 1461
session-mode ............................................................................... 1462
threshold (detection-time) .............................................................. 1463
threshold (transmit-interval) .......................................................... 1464
trace (DHCP Relay Agent) ............................................................. 1465
transmit-interval ........................................................................... 1466
trust-option-82 ............................................................................. 1467
use-interface-description ............................................................... 1468
use-primary (DHCP Relay Agent) ................................................ 1470
user-prefix (DHCP Relay Agent) ................................................... 1471
username-include (DHCP Relay Agent) ........................................ 1472
version (BFD) ................................................................................ 1473
Other Configuration Statements .................................................. 1474
cache-size ..................................................................................... 1474
cache-timeout-negative ................................................................. 1475
certificates .................................................................................... 1476
certification-authority ................................................................. 1477
connection-limit .......................................................................... 1478
crl (Encryption Interface) .............................................................. 1479
domain-search ............................................................................. 1479
encoding ....................................................................................... 1480
enrollment-retry ........................................................................... 1480
enrollment-url ............................................................................ 1481
family (for EX Series switches) ..................................................... 1482
file ............................................................................................... 1485
ftp ................................................................................................. 1486
http ............................................................................................... 1487
https .............................................................................................. 1488
ldap-url .................................................................................... 1489
lease-time .................................................................................... 1490
load-key-file ................................................................................ 1491
Chapter 27 Administration ..................................................1527
Routine Monitoring ....................................................... 1527
Monitoring DHCP Services .............................................. 1527
Verifying and Managing DHCP Local Server Configurations ...... 1531
  Verifying and Managing DHCP Local Server Configuration ..... 1532
  Verifying and Managing DHCPv6 Local Server Configuration .. 1532
Verifying and Managing DHCP Relay Agent Configurations ...... 1532
  Verifying and Managing DHCP Relay Configuration .......... 1532
  Verifying and Managing DHCPv6 Relay Configuration ......... 1533
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Local Server Monitoring Commands</td>
<td>1533</td>
</tr>
<tr>
<td>clear dhcp server binding</td>
<td>1534</td>
</tr>
<tr>
<td>clear dhcp server statistics</td>
<td>1537</td>
</tr>
<tr>
<td>clear dhcpv6 server binding</td>
<td>1539</td>
</tr>
<tr>
<td>clear dhcpv6 server statistics</td>
<td>1541</td>
</tr>
<tr>
<td>request dhcp server reconfigure</td>
<td>1542</td>
</tr>
<tr>
<td>request dhcpv6 server reconfigure</td>
<td>1544</td>
</tr>
<tr>
<td>request system reboot</td>
<td>1546</td>
</tr>
<tr>
<td>show dhcp server binding</td>
<td>1551</td>
</tr>
<tr>
<td>show dhcp server statistics</td>
<td>1556</td>
</tr>
<tr>
<td>show dhcpv6 server binding</td>
<td>1559</td>
</tr>
<tr>
<td>show dhcpv6 server statistics</td>
<td>1565</td>
</tr>
<tr>
<td>DHCP Relay Agent Monitoring Commands</td>
<td>1567</td>
</tr>
<tr>
<td>clear dhcp relay binding</td>
<td>1568</td>
</tr>
<tr>
<td>clear dhcp relay statistics</td>
<td>1570</td>
</tr>
<tr>
<td>clear dhcpv6 relay binding</td>
<td>1573</td>
</tr>
<tr>
<td>clear dhcpv6 relay statistics</td>
<td>1576</td>
</tr>
<tr>
<td>show dhcp relay binding</td>
<td>1578</td>
</tr>
<tr>
<td>show dhcp relay statistics</td>
<td>1583</td>
</tr>
<tr>
<td>show dhcpv6 relay binding</td>
<td>1586</td>
</tr>
<tr>
<td>show dhcpv6 relay statistics</td>
<td>1591</td>
</tr>
<tr>
<td>show route extensive</td>
<td>1594</td>
</tr>
<tr>
<td>show route protocol</td>
<td>1610</td>
</tr>
<tr>
<td>Other Operational Commands</td>
<td>1621</td>
</tr>
<tr>
<td>clear security pki local-certificate</td>
<td>1622</td>
</tr>
<tr>
<td>clear system services dhcp binding</td>
<td>1623</td>
</tr>
<tr>
<td>clear system services dhcp conflict</td>
<td>1624</td>
</tr>
<tr>
<td>clear system services dhcp statistics</td>
<td>1625</td>
</tr>
<tr>
<td>request ipsec switch</td>
<td>1626</td>
</tr>
<tr>
<td>request security certificate (signed)</td>
<td>1627</td>
</tr>
<tr>
<td>request security certificate (unsigned)</td>
<td>1629</td>
</tr>
<tr>
<td>request security key-pair</td>
<td>1630</td>
</tr>
<tr>
<td>request security pki generate-key-pair</td>
<td>1631</td>
</tr>
<tr>
<td>request security pki local-certificate generate-self-signed</td>
<td>1632</td>
</tr>
<tr>
<td>show security pki local-certificate</td>
<td>1633</td>
</tr>
<tr>
<td>show system services dhcp binding</td>
<td>1636</td>
</tr>
<tr>
<td>show system services dhcp conflict</td>
<td>1639</td>
</tr>
<tr>
<td>show system services dhcp global</td>
<td>1640</td>
</tr>
<tr>
<td>show system services dhcp pool</td>
<td>1642</td>
</tr>
<tr>
<td>show system services dhcp statistics</td>
<td>1644</td>
</tr>
<tr>
<td>show system services service-deployment</td>
<td>1647</td>
</tr>
<tr>
<td>ssh</td>
<td>1648</td>
</tr>
<tr>
<td>telnet</td>
<td>1650</td>
</tr>
</tbody>
</table>
Part 10  Access Control

Chapter 28  Overview

Access Control Overview ....................................................... 1655
802.1X for EX Series Switches Overview ................................. 1655
How 802.1X Authentication Works ......................................... 1655
802.1X Features Overview .................................................... 1656
Supported Features Related to 802.1X Authentication ............... 1657
Understanding Authentication on EX Series Switches .......... 1658
Sample Basic Authentication Topology .................................... 1658
802.1X Authentication .......................................................... 1659
MAC RADIUS Authentication .................................................. 1661
Captive Portal Authentication .................................................. 1661
Static MAC Bypass of Authentication ....................................... 1662
Fallback of Authentication Methods ................................中央........... 1662
Understanding Guest VLANs for 802.1X on EX Series Switches . 1664
Understanding 802.1X and RADIUS Accounting on EX Series Switches . 1664
Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches . 1665
Understanding 802.1X and VoIP on EX Series Switches ................. 1668
Understanding 802.1X and VSAs on EX Series Switches .......... 1670
Understanding Dynamic VLANs for 802.1X on EX Series Switches ...... 1670
Understanding Server Fail Fallback and Authentication on EX Series Switches .................................................. 1671
Authentication Process Flow for EX Series Switches .................. 1672
Understanding Authentication Session Timeout ....................... 1673

Chapter 29  Configuration .................................................... 1675

Configuration Examples .......................................................... 1675
Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch .................................................. 1675
Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch .................................................. 1679
Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch .................................................. 1684
Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch .................................................. 1690
Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication .................................................. 1698
Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch .................................................. 1704
Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch .................................................. 1707
Example: Configuring MAC RADIUS Authentication on an EX Series Switch .................................................. 1713
Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch .................................................. 1719
Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication .................................................. 1725
Example: Setting Up Captive Portal Authentication on an EX Series Switch .................................................. 1730
Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS
Authentication and Odyssey Access Clients ........................................... 1735
Configuration Tasks ................................................................. 1739
Configuring 802.1X Interface Settings (CLI Procedure) ...................... 1740
Configuring 802.1X RADIUS Accounting (CLI Procedure) .................. 1741
Filtering 802.1X Supplicants Using RADIUS Server Attributes .......... 1742
  Configuring Match Statements on the RADIUS Server ................. 1743
  Applying a Port Firewall Filter from the RADIUS Server ........... 1745
Configuring LLDP (CLI Procedure) ............................................. 1745
  Enabling LLDP on Interfaces .............................................. 1746
  Adjusting LLDP Advertisement Settings ................................ 1746
  Adjusting SNMP Notification Settings of LLDP Changes ............ 1747
  Specifying a Management Address for the LLDP Management TLV . 1747
Configuring LLDP Power Negotiation .......................................... 1747
Configuring LLDP-MED (CLI Procedure) ..................................... 1748
  Enabling LLDP-MED on Interfaces ..................................... 1748
  Configuring Location Information Advertised by the Switch ........ 1748
  Configuring for Fast Start .............................................. 1749
VSA Match Conditions and Actions ............................................. 1749
Configuring Server Fail Fallback (CLI Procedure) ......................... 1752
Configuring MAC RADIUS Authentication (CLI Procedure) ............. 1754
Configuring Static MAC Bypass of Authentication (CLI Procedure) .... 1755
Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure) ................................................................. 1756
Configure Captive Portal Authentication (CLI Procedure) ................ 1757
  Configuring Secure Access for Captive Portal ....................... 1757
  Enabling an Interface for Captive Portal ............................. 1758
  Configuring Bypass of Captive Portal Authentication ............ 1758
Designing a Captive Portal Authentication Login Page on an EX Series Switch ............................................................... 1759
Controlling Authentication Session Timeouts (CLI Procedure) ........... 1761
Configuration Statements ......................................................... 1762
[edit access] Configuration Statement Hierarchy on EX Series Switches ................................................................. 1762
  Supported Statements in the [edit access] Hierarchy Level ........ 1763
  Unsupported Statements in the [edit access] Hierarchy Level ...... 1767
[edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches ................................................................. 1769
  Supported Statements in the [edit protocols dot1x] Hierarchy Level ... 1769
  Unsupported Statements in the [edit protocols dot1x] Hierarchy Level ................................................................. 1770
accounting (Access Profile) .................................................... 1771
accounting-order ................................................................. 1772
accounting-port ................................................................. 1772
address-assignment (Address-Assignment Pools) .......................... 1773
address-protection .............................................................. 1774
authorization-order ............................................................. 1775
authentication-order ........................................................... 1776
authentication-whitelist ......................................................... 1777
client-accounting-algorithm ................................................... 1777
client-authentication-algorithm ........................................ 1778
coa-dynamic-variable-validation ..................................... 1778
destination-host (Gx-Plus) ............................................. 1778
destination-realm (Gx-Plus) ............................................ 1779
diameter-instance (Gx-Plus) ........................................... 1780
domain (Domain Map) ................................................... 1781
domain-name-server (Routing Instances and Access Profiles) .... 1782
domain-name-server-inet (Routing Instances and Access Profiles) . 1783
domain-name-server-inet6 (Routing Instances and Access Profiles) . 1784
ethernet-port-type-virtual ............................................. 1784
global (Gx-Plus) ......................................................... 1785
gx-plus (Gx-Plus) ....................................................... 1785
ignore ........................................................................... 1786
include-ipv6 (Gx-Plus) .................................................. 1787
interface (Static MAC Bypass) ......................................... 1787
interface (VoIP) ........................................................... 1789
interface-description-format ........................................... 1790
juniper-dsl-attributes ................................................... 1791
max-outstanding-requests (Gx-Plus) .................................. 1792
nas-identifier ............................................................... 1792
nas-port-extended-format (Access Profile) ............................ 1793
nas-port-id-delimiter (Subscriber Management) ..................... 1794
nas-port-id-format (Subscriber Management) ........................ 1795
nas-port-type (Subscriber Management) ............................... 1796
options (Access Profile) .................................................. 1797
partition (Gx-Plus) ....................................................... 1799
port ............................................................................. 1800
provisioning-order ......................................................... 1801
radius (Access Profile) .................................................... 1802
retry ............................................................................. 1804
revert-interval ............................................................... 1805
routing-instance ............................................................ 1805
secret ........................................................................... 1806
send-acct-status-on-config-change (Access Profile) ............... 1806
service (Service Accounting) ............................................ 1807
source-address ............................................................... 1807
time-out (RADIUS) ........................................................ 1808
vlan-assignment ............................................................. 1809
vlan-nas-port-stacked-format .......................................... 1810
voip ............................................................................. 1810
wait-for-acct-on-ack (Access Profile) .................................. 1811

Chapter 30 Administration .................................................. 1813
Routine Monitoring ............................................................ 1813
Monitoring 802.1X Authentication ...................................... 1813
Verifying 802.1X Authentication ......................................... 1814
Operational Commands ..................................................... 1815
clear captive-portal ......................................................... 1816
clear dot1x ................................................................. 1818

Copyright © 2013, Juniper Networks, Inc.
Chapter 32 Configuration

Configuration Examples .............................................. 1895
Example: Configuring CoS on EX Series Switches ................. 1895
Configuration Tasks ................................................. 1919
Configuring CoS (J-Web Procedure) ................................ 1920
Defining CoS Code-Point Aliases (CLI Procedure) ................ 1921
Defining CoS Code-Point Aliases (J-Web Procedure) .............. 1921
Defining CoS Classifiers (CLI Procedure) .......................... 1923
Defining CoS Classifiers (J-Web Procedure) ....................... 1925
Defining CoS Forwarding Classes (CLI Procedure) ................. 1927
Defining CoS Forwarding Classes (J-Web Procedure) .......... 1927
Defining CoS Schedulers and Scheduler Maps (CLI Procedure) . 1929
Configuring a Scheduler and a Scheduler Map ..................... 1929
Assigning a Scheduler Map to Interfaces .......................... 1930
Assigning Scheduler Maps to Interfaces on EX8200 Line Cards That Include Oversubscribed Ports ................. 1930
Defining CoS Schedulers (J-Web Procedure) ....................... 1931
Defining CoS Scheduler Maps (J-Web Procedure) ................. 1934
Configuring CoS Congestion Management (CLI Procedure) ....... 1935
Configuring a Weighted Tail Drop Profile ........ ................ 1936
Configuring a Weighted Random Early Detection Drop Profile .... 1936
Defining CoS Drop Profiles (J-Web Procedure) .................... 1938
Defining CoS Rewrite Rules (CLI Procedure) ...................... 1939
Defining CoS Rewrite Rules (J-Web Procedure) .................. 1940
Assigning CoS Components to Interfaces (CLI Procedure) ....... 1942
Assigning CoS Components to Interfaces (J-Web Procedure) .... 1942
Configuring Junos OS EZQoS for CoS (CLI Procedure) ........... 1944
Configuring CoS Traffic Classification for Ingress Queueing on Oversubscribed Ports on EX8200 Line Cards (CLI Procedure) ........ 1945
Configuration Statements ............................. 1946
[edit class-of-service] Configuration Statement Hierarchy on EX Series Switches ............................. 1946
Supported Statements in the [edit class-of-service] Hierarchy Level ........................................ 1946
Unsupported Statements in the [edit class-of-service] Hierarchy Level ........................................ 1948
broadcast ............................................. 1949
buffer-size ......................................... 1950
classifiers ........................................... 1951
code-point-aliases .................................. 1952
code-points ......................................... 1952
drop-profile-map ...................................... 1953
dscp .................................................. 1954
dscp-ipv6 ........................................... 1955
ethernet (CoS for Multidestination Traffic) ............. 1956
excess-rate (Schedulers) ................................ 1956
family ................................................... 1957
forwarding-class ..................................... 1958
forwarding-classes .................................. 1959
ieee-802.1 ........................................... 1960
import .................................................. 1961
inet-precedence ...................................... 1962
interfaces ............................................. 1963
loss-priority (Classifiers and Rewrite Rules) ............... 1964
policing ............................................. 1965
priority (Schedulers) .................................. 1966
protocol (Drop Profiles) ................................ 1966
rewrite-rules ......................................... 1967
scheduler-map ......................................... 1968
scheduler-maps ....................................... 1969
schedulers (CoS) ...................................... 1970
shaping-rate .......................................... 1971
transmit-rate (EX Series Switches) ......................... 1972
unit ..................................................... 1973

Chapter 33 Administrative Commands .......................... 1975
Routine Monitoring .................................... 1975
Monitoring CoS Classifiers ................................ 1975
Monitoring CoS Forwarding Classes ......................... 1976
Monitoring Interfaces That Have CoS Components ........... 1978
Monitoring CoS Rewrite Rules ............................ 1979
Monitoring CoS Scheduler Maps ............................ 1980
Monitoring CoS Value Aliases ............................. 1981
Monitoring CoS Drop Profiles ............................. 1982
Operational Commands .................................. 1983
show class-of-service .................................. 1984
show class-of-service classifier ............................ 1989
show class-of-service code-point-aliases .................... 1991
Chapter 37 Administration .................................................2043
Routine Monitoring .....................................................2043
Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface ..................................................2043
Operational Commands ..................................................2044
clear ethernet-switching recovery-timeout ..........................2045

Part 13 Ethernet Switching ..................................................2049
Overview .............................................................................2049
Bridging and VLANs ..........................................................2049
Understanding Bridging and VLANs on EX Series Switches ...................................................................................2049
  History of VLANs ................................................................2050
  How Bridging of VLAN Traffic Works ................................2050
  Packets Are Either Tagged or Untagged ..............................2051
  Switch Interface Modes—Access, Trunk, or Tagged Access ...................................................................................2052
  Additional Advantages of Using VLANs ..............................2054
  Maximum VLANs and VLAN Members Per Switch ..............2054
  A Default VLAN Is Configured on Most Switches ..............2055
  Assigning Traffic to VLANs ..............................................2055
  Forwarding VLAN Traffic ................................................2056
  VLANs Communicate with Integrated Routing and Bridging Interfaces or Routed VLAN Interfaces ......................2056
Understanding Integrated Routing and Bridging Interfaces and Routed VLAN Interfaces on EX Series Switches ...................................................................................2058
  When Should I Use an IRB Interface or RVI? ......................2059
  How Does an IRB Interface or RVI Work? ............................2059
  Creating an IRB Interface or RVI .......................................2060
  Viewing IRB Interface and RVI Statistics ............................2061
  IRB Interfaces and RVI Functions and Other Technologies ...................................................................................2061
Understanding Virtual Routing Instances on EX Series Switches ...................................................................................2062
Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches ..................................................2063
  How MVRP Updates, Creates, and Deletes VLANs on the Switches .................................................................2063
  MVRP Is Disabled by Default on the Switches ....................2063
  MRP Timers Control MVRP Updates ..................................2064
  MVRP Uses MRP Messages to Transmit Switch and VLAN States .................................................................2064
  Compatibility Issues with Junos OS Releases of MVRP ........2065
Understanding MAC Address Aging .......................................2066
Redundant Trunk Groups .....................................................2068
Understanding Redundant Trunk Links on EX Series Switches ...................................................................................2068
Proxy ARP .............................................................................2070
Understanding Proxy ARP on EX Series Switches .................2070
  What Is ARP? ....................................................................2070
  Proxy ARP Overview .......................................................2070
[edit vlans] Configuration Statement Hierarchy on EX Series Switches ... 2136
  Supported Statements in the [edit vlans] Hierarchy Level ... 2137
  Unsupported Statements in the [edit vlans] Hierarchy Level ... 2139
  address ........................................... 2140
description (Interfaces) .................................. 2141
description (VLANs) ................................... 2142
  filter (VLANs) ..................................... 2143
global-mac-table-aging-time .......................... 2144
global-no-mac-learning .................. 2144
  interface (MVRP) .................................. 2145
  interface-mac-limit .............................. 2146
  interface-mode .................................. 2148
  join-timer (MVRP) ................................ 2149
  l3-interface (VLANs) ............................ 2150
  leaveall-timer (MVRP) ............................ 2151
  leave-timer (MVRP) ............................... 2152
  mac (Static MAC-Based VLANs) .................. 2153
  mac-table-size ................................. 2154
  members ........................................ 2156
  mvrp ............................................. 2158
  native-vlan-id .................................. 2159
  no-attribute-length-in-pdu ....................... 2160
  no-dynamic-vlan ................................. 2161
  no-gratuitous-arp-request ......................... 2162
  no-mac-learning ................................ 2163
  packet-action .................................. 2165
  proxy-arp ..................................... 2168
  redundant-trunk-group ............................. 2169
  registration ................................... 2170
  vlan (802.1Q Tagging) ............................ 2171
  vlan-id (802.1Q Tagging) .......................... 2172
  vlan-id-list ................................... 2173
  vlans ........................................... 2174

Chapter 40  Administration ........................................... 2177
  Routine Monitoring .................................. 2177
    Verifying That Virtual Routing Instances Are Working .... 2177
    Verifying Integrated Routing and Bridging Interface Status and Statistics ... 2178
    Verifying That MVRP Is Working Correctly ................ 2180
    Verifying That Proxy ARP Is Working Correctly .......... 2181
  Operational Commands ................................ 2182
    show ethernet-switching interface .................. 2183
    show ethernet-switching table ..................... 2185
    show interfaces irb ................................ 2192
    show mvrp ..................................... 2198
    show mvrp dynamic-vlan-memberships ............... 2200
    show mvrp statistics ............................ 2201
    show redundant-trunk-group ....................... 2203
    show system statistics trunk-group ............... 2205
show vlans ................................................................. 2206

Part 14 High Availability
Chapter 41 Overview ..................................................... 2211
High Availability Features Overview ..................................... 2211
High Availability Features for EX4300 Switches Overview ............... 2211
Redundant Routing Engines ............................................ 2211
Virtual Chassis ......................................................... 2212
VRRP ................................................................. 2212
Graceful Routing Engine Switchover .................................... 2212
Link Aggregation ....................................................... 2213
Power Management Overview ......................................... 2213
Understanding Power Management on EX Series Switches .............. 2213
Power Priority of Line Cards ........................................... 2215
Power Supply Redundancy ............................................. 2218
VRRP Overview .......................................................... 2219
Understanding VRRP on EX Series Switches ............................. 2220
Overview of VRRP on EX Series Switches ............................... 2220
Examples of VRRP Topologies .......................................... 2221

Chapter 42 Configuration .................................................. 2223
Configuration Tasks ..................................................... 2223
Configuring Power Supply Redundancy (CLI Procedure) ................. 2223
Configuring VRRP for IPv6 (CLI Procedure) ............................ 2224
Configuration Statements ............................................... 2225
[edit chassis] Configuration Statement Hierarchy on EX Series Switches . 2225
Supported Statements in the [edit chassis] Hierarchy Level .............. 2226
[edit interfaces] Configuration Statement Hierarchy on EX Series Switches . 2227
[edit protocols vrrp] Hierarchy Level .................................. 2228
chassis .............................................................. 2229
synchronize .......................................................... 2231
failover (Chassis) .................................................... 2232
fpc ................................................................. 2233
graceful-switchover .................................................. 2234
hold-time .......................................................... 2235
inet6-advertise-interval .................................................. 2235
keepalive-time ....................................................... 2236
n-plus-n (Power Management) ......................................... 2237
preempt ............................................................. 2237
priority ............................................................. 2238
psu ................................................................. 2239
redundancy (Graceful Switchover) ..................................... 2240
redundancy (Power Management) ...................................... 2241
traceoptions (Routing Options) ......................................... 2242
virtual-inet6-address ............................................... 2244
virtual-link-local-address ............................................. 2245
vrrp-inet6-group ..................................................... 2246

Copyright © 2013, Juniper Networks, Inc. xxxiii
Chapter 43  Administration .......................................................... 2247
  Verification Tasks .............................................................. 2247
  Verifying Power Configuration and Use .................................... 2247
  Operational Commands ........................................................ 2249
    show chassis power-budget-statistics ................................... 2250
    show vrrp ................................................................. 2254

Part 15  Interfaces
  Chapter 44  Overview .......................................................... 2267
  Interfaces Overview .......................................................... 2267
    EX Series Switches Interfaces Overview ................................ 2267
      Network Interfaces ...................................................... 2267
      Special Interfaces ..................................................... 2268
    Understanding Interface Naming Conventions on EX Series Switches ... 2270
      Physical Part of an Interface Name ................................... 2270
      Logical Part of an Interface Name .................................... 2272
     Wildcard Characters in Interface Names ................................ 2272
    Understanding Aggregated Ethernet Interfaces and LACP ............... 2272
      Link Aggregation Group (LAG) ........................................... 2273
      Link Aggregation Control Protocol (LACP) ............................ 2274
    Understanding Layer 3 Subinterfaces ................................... 2275
    Understanding Unicast RPF for EX Series Switches ....................... 2276
      Unicast RPF for EX Series Switches Overview ......................... 2276
      When to Enable Unicast RPF .......................................... 2277
      When Not to Enable Unicast RPF ...................................... 2278
      Limitations of the Unicast RPF Implementation on EX3200, EX4200,
      and EX4300 Switches .................................................. 2279
    Understanding IP Directed Broadcast for EX Series Switches ............ 2280
      IP Directed Broadcast for EX Series Switches Overview ............... 2280
      When to Enable IP Directed Broadcast ................................ 2281
      When Not to Enable IP Directed Broadcast ............................ 2281
    Understanding Interface Ranges on EX Series Switches .................. 2281
    802.1Q VLANs Overview .................................................. 2283

Chapter 45  Configuration .......................................................... 2285
  Configuration Tasks ........................................................... 2285
    Configuring Gigabit Ethernet Interfaces (CLI Procedure) ............... 2286
      Configuring VLAN Options and Interface Mode ......................... 2286
      Configuring the Link Settings ....................................... 2287
      Configuring the IP Options .......................................... 2288
    Configuring Gigabit Ethernet Interfaces (J-Web Procedure) ............ 2289
    Port Role Configuration with the J-Web Interface (with CLI References) . 2295
    Adding a Logical Unit Description to the Configuration ................. 2299
    Disabling a Physical Interface .......................................... 2299
    Example: Disabling a Physical Interface ................................ 2300
    Disabling a Logical Interface .......................................... 2301
Configuring Aggregated Ethernet LACP (CLI Procedure) ........................................ 2339
Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) ................................................................. 2340
Configuring LACP Link Protection at the Global Level ........................................ 2341
Configuring LACP Link Protection at the Aggregated Interface Level ................. 2341
Configuring Aggregated Ethernet Link Protection .................................................. 2342
Configuring Link Protection for Aggregated Ethernet Interfaces ....................... 2342
Configuring Primary and Backup Links for Link Aggregated Ethernet Interfaces ........................................ 2342
Reverting Traffic to a Primary Link When Traffic is Passing Through a Backup Link ................................................................. 2343
Disabling Link Protection for Aggregated Ethernet Interfaces .......................... 2343
Configuring Aggregated Ethernet Link Speed .................................................... 2343
Configuring Aggregated Ethernet Minimum Links ............................................. 2345
Configuring Tagged Aggregated Ethernet Interfaces ........................................... 2346
Configuring a Layer 3 Subinterface (CLI Procedure) ..................................... 2346
Configuring Unicast RPF (CLI Procedure) .................................................... 2347
Disabling Unicast RPF (CLI Procedure) .................................................... 2348
Configuring IP Directed Broadcast (CLI Procedure) ...................................... 2349
Tracing Operations of an Individual Router or Switch Interface ....................... 2350
Tracing Operations of the Interface Process .................................................... 2351
Configuration Statements .................................................................................. 2351
[edit chassis] Configuration Statement Hierarchy on EX Series Switches .............. 2352
  Supported Statements in the [edit chassis] Hierarchy Level ......................... 2352
[edit interfaces] Configuration Statement Hierarchy on EX Series Switches .......... 2354
[edit interfaces ae] Configuration Statement Hierarchy on EX Series Switches .......... 2354
  Supported Statements in the [edit interfaces ae] Hierarchy Level ............... 2355
  Unsupported Statements in the [edit interfaces ae] Hierarchy Level ............... 2358
[edit interfaces et] Configuration Statement Hierarchy on EX Series Switches .......... 2360
  Supported Statements in the [edit interfaces et] Hierarchy Level ............... 2360
  Unsupported Statements in the [edit interfaces et] Hierarchy Level ............... 2363
[edit interfaces ge] Configuration Statement Hierarchy on EX Series Switches .......... 2365
  Supported Statements in the [edit interfaces ge] Hierarchy Level ............... 2365
  Unsupported Statements in the [edit interfaces ge] Hierarchy Level ............... 2369
[edit interfaces interface-range] Configuration Statement Hierarchy on EX Series Switches .... 2371
  Supported Statements in the [edit interfaces interface-range] Hierarchy Level ............... 2371
  Unsupported Statements in the [edit interfaces interface-range] Hierarchy Level ............... 2374
[edit interfaces irb] Configuration Statement Hierarchy on EX Series Switches .......... 2379
  Supported Statements in the [edit interfaces irb] Hierarchy Level ............... 2379
  Unsupported Statements in the [edit interfaces irb] Hierarchy Level ............... 2382
[edit interfaces lo] Configuration Statement Hierarchy on EX Series
Switches ...................................................... 2383
Supported Statements in the [edit interfaces lo] Hierarchy Level ........................................... 2383
Unsupported Statements in the [edit interfaces lo] Hierarchy Level ........................................... 2385

[edit interfaces me] Configuration Statement Hierarchy on EX Series
Switches ...................................................... 2386
Supported Statements in the [edit interfaces me] Hierarchy Level ........................................... 2386
Unsupported Statements in the [edit interfaces me] Hierarchy Level ........................................... 2388

[edit interfaces vme] Configuration Statement Hierarchy on EX Series
Switches ...................................................... 2389
Supported Statements in the [edit interfaces vme] Hierarchy Level ........................................... 2390
Unsupported Statements in the [edit interfaces vme] Hierarchy Level ........................................... 2392

[edit interfaces xe] Configuration Statement Hierarchy on EX Series
Switches ...................................................... 2393
Supported Statements in the [edit interfaces xe] Hierarchy Level ........................................... 2393
Unsupported Statements in the [edit interfaces xe] Hierarchy Level ........................................... 2396

[edit protocols lacp] Configuration Statement Hierarchy on EX Series
Switches ...................................................... 2398
Supported Statements in the [edit protocols lacp] Hierarchy Level ........................................... 2398
Unsupported Statements in the [edit protocols lacp] Hierarchy Level ........................................... 2399

802.3ad .......................................................... 2400
accounting-profile ........................................ 2401
address ....................................................... 2402
aggregated-devices ........................................ 2404
aggregated-ether-options ................................ 2405
arp (Interfaces) .............................................. 2406
auto-negotiation ............................................. 2407
broadcast ..................................................... 2409
chassis ....................................................... 2410
description (Interfaces) .................................. 2413
device-count ................................................ 2414
disable (Interface) ......................................... 2415
eui-64 ........................................................ 2416
ether-options .............................................. 2417
ethernet (Aggregated Devices) .......................... 2418
family ....................................................... 2419
filter ........................................................ 2425
flow-control ............................................... 2426
force-up .................................................... 2427
gratuitous-arp-reply ....................................... 2427
hold-time (Physical Interface) .......................... 2428
interface-mode ............................................ 2429
interface-range ............................................ 2430
lacp (Aggregated Ethernet) .............................. 2432
lacp (802.3ad) ............................................... 2434
Chapter 46  Administration .................................................2463

Routine Monitoring ...................................................2463

Monitoring Interface Status and Traffic .............................2463
Verifying the Status of a LAG Interface .......................2465
Verifying That LACP Is Configured Correctly and Bundle Members Are
    Exchanging LACP Protocol Packets ..............................2465
    Verifying the LACP Setup .........................................2465
    Verifying That LACP Packets Are Being Exchanged ..........2466
Verifying That Layer 3 Subinterfaces Are Working ................2466
Verifying Unicast RPF Status ..........................................2467
Verifying IP Directed Broadcast Status ............................2469

Operational Commands ...............................................2470
monitor interface ...................................................2471
request diagnostics tdr ............................................2479
show diagnostics tdr ..................................................2481
show interfaces diagnostics optics .................................2486
show interfaces ge- ................................................2493
show interfaces irb ..................................................2505
show interfaces me0 ..................................................2511
show interfaces queue ...............................................2518
show interfaces xe- ..................................................2524
show lACP interfaces ..................................................2538
test interface restart-auto-negotiation ..........................2543
Chapter 47 Troubleshooting Procedures ..................................... 2545

Troubleshooting an Aggregated Ethernet Interface ..................... 2545
Show Interfaces Command Shows the LAG is Down .................... 2545
Logical Interface Statistics Do Not Reflect All Traffic ............... 2545
IPv6 Interface Traffic Statistics Are Not Supported .................. 2546
Troubleshooting Interface Configuration and Cable Faults .......... 2546
Interface Configuration or Connectivity Is Not Working ............. 2546
Troubleshooting Unicast RPF .............................................. 2547
Legitimate Packets Are Discarded ..................................... 2547
Diagnosing a Faulty Twisted-Pair Cable (CLI Procedure) .......... 2547

Part 16 BGP

Chapter 48 Overview ............................................................ 2553
Layer 3 Protocols .................................................................. 2553
Layer 3 Protocols Supported on EX Series Switches .................. 2553
Layer 3 Protocols Not Supported on EX Series Switches .......... 2554

Chapter 49 Configuration ....................................................... 2557
Configuration Tasks ............................................................. 2557
Configuring BGP Sessions (J-Web Procedure) ......................... 2557
Configuration Statements ..................................................... 2562
accept-remote-next-hop ................................................... 2562
advertise-external ............................................................ 2563
advertise-inactive ............................................................. 2565
advertise-peer-as .............................................................. 2566
aggregate-label .................................................................. 2567
allow .............................................................................. 2568
as-override ....................................................................... 2569
authentication-algorithm ................................................... 2570
authentication-key (Protocols BGP) ....................................... 2571
authentication-key-chain (Protocols BGP) ............................... 2572
autonomous-system ............................................................ 2573
bfd-liveness-detection (Protocols BGP) .................................... 2576
bgp ............................................................................... 2580
bgp-orf-cisco-mode .......................................................... 2581
cluster ............................................................................. 2583
damping (Protocols BGP) ..................................................... 2585
description (Protocols BGP) ................................................ 2587
disable (Protocols BGP) ...................................................... 2588
explicit-null (Protocols BGP) .............................................. 2589
export (Protocols BGP) ...................................................... 2591
family (Protocols BGP) ...................................................... 2592
graceful-restart (Protocols BGP) .......................................... 2596
group (Protocols BGP) ....................................................... 2598
hold-time (Protocols BGP) .................................................. 2601
idle-after-switch-over ....................................................... 2603
import (Protocols BGP) ..................................................... 2604
include-mp-next-hop ........................................................ 2606
keep ................................................................. 2607
labeled-unicast (Protocols BGP) ......................... 2609
local-address (Protocols BGP) ............................ 2611
local-as .......................................................... 2613
local-interface (IPv6) ........................................... 2615
local-preference ............................................... 2616
log-updown (Protocols BGP) ............................... 2617
metric-out (Protocols BGP) ................................. 2618
mtu-discovery .................................................. 2620
multihop .......................................................... 2622
multipath (Protocols BGP) ................................. 2624
neighbor (Protocols BGP) ................................. 2625
no-aggregator-id ............................................... 2628
no-client-reflect .............................................. 2629
no-validate ....................................................... 2630
out-delay ......................................................... 2632
outbound-route-filter ....................................... 2634
passive (Protocols BGP) ..................................... 2635
peer-as (Protocols BGP) ..................................... 2636
preference (Protocols BGP) ............................... 2638
prefix-limit ..................................................... 2639
remove-private ............................................... 2641
rib-group (Protocols BGP) ................................. 2643
tcp-mss (Protocols BGP) ..................................... 2644
traceoptions (Protocols BGP) ............................. 2645
type (Protocols BGP) .......................................... 2648

Chapter 50 Administration ................................................. 2649
Routine Monitoring .............................................. 2649
Monitoring BGP Routing Information ..................... 2649
Operational Commands ...................................... 2651
clear bgp damping ............................................. 2652
clear bgp neighbor ............................................ 2653
clear bgp table .................................................. 2655
show bgp bmp ..................................................... 2657
show bgp group .................................................. 2659
show bgp neighbor ............................................. 2666
show bgp summary ............................................. 2680
show policy damping ......................................... 2685

Part 17 IS-IS
Chapter 51 Overview ...................................................... 2689
Layer 3 Protocols .................................................. 2689
Layer 3 Protocols Supported on EX Series Switches .... 2689
Layer 3 Protocols Not Supported on EX Series Switches 2690
# Chapter 52 Configuration

## Configuration Statements

- `authentication-key` (Protocols IS-IS) ........................................... 2694
- `authentication-type` (Protocols IS-IS) ...................................... 2695
- `bfd-liveness-detection` (Protocols IS-IS) .................................... 2696
- `checksum` (Protocols IS-IS) ...................................................... 2698
- `csnp-interval` ............................................................................ 2699
- `disable` (Protocols IS-IS) ............................................................ 2700
- `export` (Protocols IS-IS) .............................................................. 2701
- `external-preference` (Protocols IS-IS) ........................................... 2702
- `graceful-restart` (Protocols IS-IS) .............................................. 2703
- `hello-authentication-key` .............................................................. 2704
- `hello-authentication-type` .............................................................. 2705
- `hello-interval` (Protocols IS-IS) ................................................ 2706
- `hello-padding` .............................................................................. 2707
- `hold-time` (Protocols IS-IS) ......................................................... 2709
- `ignore-attached-bit` ..................................................................... 2710
- `interface` (Protocols IS-IS) .......................................................... 2711
- `ipv4-multicast` ............................................................................ 2713
- `ipv4-multicast-metric` ................................................................. 2714
- `ipv6-multicast` ............................................................................ 2714
- `ipv6-multicast-metric` ................................................................. 2715
- `ipv6-unicast` .............................................................................. 2716
- `ipv6-unicast-metric` ................................................................. 2717
- `isis` .......................................................................................... 2718
- `level` (Global IS-IS) ................................................................. 2719
- `link-protection` (Protocols IS-IS) .............................................. 2720
- `loose-authentication-check` ....................................................... 2720
- `lsp-interval` .............................................................................. 2721
- `lsp-lifetime` .............................................................................. 2722
- `max-areas` .................................................................................. 2723
- `mesh-group` (Protocols IS-IS) .................................................. 2724
- `metric` (Protocols IS-IS) ............................................................... 2725
- `no-adjacency-holdown` .............................................................. 2726
- `no-authentication-check` .............................................................. 2727
- `no-csnp-authentication` ............................................................... 2727
- `no-eligible-backup` (Protocols IS-IS) ......................................... 2728
- `no-hello-authentication` .............................................................. 2728
- `no-ipv4-multicast` ................................................................. 2729
- `no-ipv4-routing` ................................................................. 2730
- `no-ipv6-multicast` ................................................................. 2731
- `no-ipv6-routing` ................................................................. 2732
- `no-ipv6-unicast` ................................................................. 2733
- `no-psnp-authentication` ............................................................. 2733
- `no-unicast-topology` ............................................................... 2734
- `node-link-protection` (Protocols IS-IS) ................................... 2734
- `overload` (Protocols IS-IS) .......................................................... 2735
- `passive` (Protocols IS-IS) ............................................................ 2738
- `point-to-point` ........................................................................... 2739
Chapter 53 Administration .................................................. 2751

Operational Commands .................................................... 2751
  clear isis adjacency ................................................. 2752
  clear isis database ................................................ 2754
  clear isis overload ................................................ 2756
  clear isis statistics ............................................... 2758
  show isis adjacency .............................................. 2760
  show isis authentication ...................................... 2764
  show isis backup coverage .................................... 2766
  show isis backup label-switched-path ....................... 2768
  show isis backup spf results .................................. 2770
  show isis database ............................................... 2774
  show isis hostname .............................................. 2781
  show isis interface ............................................. 2782
  show isis overview .............................................. 2786
  show isis route .................................................. 2789
  show isis spf ..................................................... 2793
  show isis statistics ............................................. 2798

Part 18 OSPF

Chapter 54 Overview ...................................................... 2803

Layer 3 Protocols ........................................................ 2803
  Layer 3 Protocols Supported on EX Series Switches .......... 2803
  Layer 3 Protocols Not Supported on EX Series Switches .... 2804
OSPF Overview .......................................................... 2806
  Understanding IPsec Authentication for OSPF Packets on EX Series Switches ........................................... 2807
  Authentication Algorithms ...................................... 2807
  Encryption Algorithms .......................................... 2808
  IPsec Protocols ................................................... 2808
  Security Associations ............................................ 2808
  IPsec Modes ........................................................ 2809

preference (Protocols IS-IS) ........................................... 2740
prefix-export-limit (Protocols IS-IS) ............................. 2741
priority (Protocols IS-IS) ............................................. 2742
reference-bandwidth (Protocols IS-IS) ........................... 2743
rib-group (Protocols IS-IS) .......................................... 2744
spf-options (Protocols IS-IS) ....................................... 2745
topologies (Protocols IS-IS) ......................................... 2746
traceoptions (Protocols IS-IS) ...................................... 2747
wide-metrics-only ..................................................... 2750
Chapter 55 Configuration ................................................... 2811

Configuration Tasks .................................................... 2811
Configuring an OSPF Network (J-Web Procedure) ................. 2811
Using IPsec to Secure OSPFv3 Networks (CLI Procedure) ....... 2815
Configuring Security Associations ..................................... 2815
Securing OSPFv3 Networks ............................................. 2816

Configuration Statements .............................................. 2817
area ............................................................................ 2818
area-range .................................................................... 2820
bandwidth-based-metrics .................................................. 2822
bfd-liveness-detection (Protocols OSPF) .............................. 2824
dead-interval ................................................................ 2828
default-lsa .................................................................... 2829
default-metric ................................................................ 2830
disable (OSPF) ................................................................. 2832
domain-id ...................................................................... 2833
domain-vpn-tag ................................................................. 2834
export (Protocols OSPF) ................................................... 2835
external-preference (Protocols OSPF) ................................. 2836
graceful-restart (Protocols OSPF) ...................................... 2837
hello-interval (Protocols OSPF) ......................................... 2839
ignore-lsp-metrics ............................................................ 2840
import (Protocols OSPF) .................................................... 2841
inter-area-prefix-export ................................................... 2842
inter-area-prefix-import ................................................... 2843
interface (Protocols OSPF) ............................................... 2844
interface-type (Protocols OSPF) ......................................... 2847
lsp-metric-into-summary .................................................. 2848
metric (Protocols OSPF Interface) ...................................... 2849
metric-type .................................................................... 2851
no-nssa-abr .................................................................. 2852
no-rfc-1583 ................................................................... 2853
nssa .............................................................................. 2854
ospf .............................................................................. 2855
ospf3 ............................................................................. 2856
overload (Protocols OSPF) ............................................... 2857
passive (Protocols OSPF) .................................................. 2859
preference (Protocols OSPF) ............................................. 2860
prefix-export-limit (Protocols OSPF) ................................. 2861
priority (Protocols OSPF) ............................................... 2862
realm ........................................................................... 2863
reference-bandwidth (Protocols OSPF) ............................... 2864
retransmit-interval (OSPF) .............................................. 2865
rib-group (Protocols OSPF) ............................................. 2866
route-type-community ..................................................... 2867
shortcuts (Protocols OSPF) .............................................. 2868
spf-options (Protocols OSPF) .......................................... 2869
stub .............................................................................. 2871
summaries .................................................................... 2872
Chapter 56 Administration .................................................. 2881
Routine Monitoring ............................................................. 2881
Monitoring OSPF Routing Information .................................... 2881
Operational Commands ...................................................... 2883
  clear (ospf | ospf3) database .............................................. 2884
  clear (ospf | ospf3) io-statistics ...................................... 2887
  clear (ospf | ospf3) neighbor ........................................... 2888
  clear (ospf | ospf3) statistics ......................................... 2890
  clear (ospf | ospf3) overload ........................................... 2892
  show (ospf | ospf3) interface .......................................... 2893
  show (ospf | ospf3) io-statistics ..................................... 2899
  show (ospf | ospf3) log .................................................. 2901
  show (ospf | ospf3) neighbor .......................................... 2904
  show (ospf | ospf3) overview ......................................... 2910
  show (ospf | ospf3) route .............................................. 2915
  show (ospf | ospf3) statistics ......................................... 2921
  show ospf database .................................................... 2925
  show ospf3 database ................................................... 2933

Part 19 RIP
Chapter 57 Overview .......................................................... 2947
Layer 3 Protocols .............................................................. 2947
  Layer 3 Protocols Supported on EX Series Switches ............. 2947
  Layer 3 Protocols Not Supported on EX Series Switches ....... 2948
Chapter 58 Configuration ..................................................... 2951
Configuration Tasks ........................................................... 2951
  Configuring a RIP Network (J-Web Procedure) ..................... 2951
Configuration Statements: RIP ............................................. 2955
  any-sender ............................................................... 2955
  authentication-key (Protocols RIP) ................................ 2956
  authentication-type (Protocols RIP) ................................ 2957
  bfd-liveness-detection (Protocols RIP) ............................ 2958
  check-zero ............................................................... 2961
  export (Protocols RIP) ................................................. 2962
  graceful-restart (Protocols RIP) .................................... 2963
  group (Protocols RIP) .................................................. 2964
  holddown (Protocols RIP) ............................................. 2966
  import (Protocols RIP) ................................................ 2967
  message-size ............................................................ 2968
  metric-in (Protocols RIP) ............................................. 2969
  metric-out (Protocols RIP) .......................................... 2970
  neighbor (Protocols RIP) ............................................. 2971
<table>
<thead>
<tr>
<th>Configuration Statements: RIPng</th>
<th>2981</th>
</tr>
</thead>
<tbody>
<tr>
<td>export (Protocols RIPng)</td>
<td>2981</td>
</tr>
<tr>
<td>graceful-restart (Protocols RIPng)</td>
<td>2982</td>
</tr>
<tr>
<td>group (Protocols RIPng)</td>
<td>2983</td>
</tr>
<tr>
<td>holddown (Protocols RIPng)</td>
<td>2984</td>
</tr>
<tr>
<td>import (Protocols RIPng)</td>
<td>2985</td>
</tr>
<tr>
<td>metric-in (Protocols RIPng)</td>
<td>2986</td>
</tr>
<tr>
<td>metric-out (Protocols RIPng)</td>
<td>2987</td>
</tr>
<tr>
<td>neighbor (Protocols RIPng)</td>
<td>2988</td>
</tr>
<tr>
<td>preference (Protocols RIPng)</td>
<td>2989</td>
</tr>
<tr>
<td>receive (Protocols RIPng)</td>
<td>2990</td>
</tr>
<tr>
<td>ripng</td>
<td>2991</td>
</tr>
<tr>
<td>route-timeout (Protocols RIPng)</td>
<td>2991</td>
</tr>
<tr>
<td>send (Protocols RIPng)</td>
<td>2992</td>
</tr>
<tr>
<td>traceoptions (Protocols RIPng)</td>
<td>2993</td>
</tr>
<tr>
<td>update-interval (Protocols RIPng)</td>
<td>2995</td>
</tr>
</tbody>
</table>

Chapter 59

**Administration** ................................................. 2997

Routine Monitoring ................................................. 2997

Monitoring RIP Routing Information ................................. 2997

Operational Commands: RIP ........................................ 2998

clear rip general-statistics ..................................... 2999

clear rip statistics ............................................. 3000

show rip general-statistics ...................................... 3001

show rip neighbor .................................................. 3003

show rip statistics ............................................... 3005

Operational Commands: RIPng ...................................... 3007

clear ripng general-statistics ................................. 3008

clear ripng statistics ........................................... 3009

show ripng general-statistics ................................. 3010

show ripng neighbor .............................................. 3011

show ripng statistics ............................................ 3013

Part 20

**Routing Options** .................................................. 3017

Chapter 60

**Overview** .......................................................... 3017

Layer 3 Protocols .................................................... 3017

Layer 3 Protocols Supported on EX Series Switches .......... 3017

Layer 3 Protocols Not Supported on EX Series Switches .... 3018

Routing Options Overview .......................................... 3020

Understanding Distributed Periodic Packet Management on EX Series Switches ........................................... 3020
# Configuration

Chapter 61 Configuration .................................................. 3023

- **Configuration Tasks** .............................................. 3023

  - Configuring Static Routing (CLI Procedure) .................... 3024
  - Configuring Static Routing (J-Web Procedure) .................. 3024

  - Configuring Distributed Periodic Packet Management on an EX Series Switch
    - (CLI Procedure) .................................................. 3026
  - Disabling or Enabling Distributed Periodic Packet Management Globally ........................................ 3027
  - Disabling or Enabling Distributed Periodic Packet Management for LACP Packets ..................................... 3027

- **Configuration Statements** ......................................... 3028

  - active ........................................................................... 3029
  - aggregate (Routing) ................................................... 3030
  - as-path (Routing Options) ............................................ 3032
  - asm-override-ssm .................................................... 3034
  - authentication-key-chains .......................................... 3035
  - autonomous-system .................................................. 3036
  - backup-pe-group ............................................................ 3038
  - backups ....................................................................... 3039
  - bandwidth (Multicast Flow Map) ..................................... 3040
  - bfd-liveness-detection (Routing Options Static Route) ........ 3041
  - bgp-orf-cisco-mode ............................................................ 3045
  - bmp ............................................................................. 3046
  - brief ............................................................................. 3047
  - centralized ................................................................. 3048
  - community (Routing Options) ......................................... 3049
  - confederation ............................................................. 3051
  - disable (Routing Options) .................................................. 3052
  - discard ........................................................................ 3053
  - export (Routing Options) ................................................. 3054
  - export-rib .................................................................... 3055
  - fate-sharing ............................................................... 3056
  - flow ............................................................................. 3057
  - flow-map ...................................................................... 3058
  - forwarding-cache (Flow Maps) ....................................... 3059
  - forwarding-cache (Multicast) .......................................... 3060
  - forwarding-table .......................................................... 3061
  - generate ...................................................................... 3062
  - import (Routing Options) ............................................... 3063
  - import-policy .............................................................. 3064
  - import-rib .................................................................... 3065
  - indirect-next-hop .......................................................... 3066
  - install (Routing Options) ................................................ 3067
  - instance-export ............................................................ 3068
  - instance-import ............................................................. 3068
  - interface (Multicast Static Routes) .................................... 3069
  - interface (Routing Options) ............................................. 3070
  - interface-routes ............................................................ 3071
  - local-address (Routing Options) ...................................... 3072
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>martians</td>
<td>3073</td>
</tr>
<tr>
<td>maximum-bandwidth (Routing Options)</td>
<td>3074</td>
</tr>
<tr>
<td>maximum-paths</td>
<td>3075</td>
</tr>
<tr>
<td>maximum-prefixes</td>
<td>3077</td>
</tr>
<tr>
<td>med-igp-update-interval</td>
<td>3078</td>
</tr>
<tr>
<td>metric (Aggregate, Generated, or Static Route)</td>
<td>3079</td>
</tr>
<tr>
<td>multicast (Routing Options)</td>
<td>3080</td>
</tr>
<tr>
<td>no-qos-adjust</td>
<td>3081</td>
</tr>
<tr>
<td>options (Routing Options)</td>
<td>3082</td>
</tr>
<tr>
<td>pim-to-igmp-proxy</td>
<td>3083</td>
</tr>
<tr>
<td>pim-to-mld-proxy</td>
<td>3084</td>
</tr>
<tr>
<td>policy (Aggregate and Generated Routes)</td>
<td>3085</td>
</tr>
<tr>
<td>policy (Flow Maps)</td>
<td>3086</td>
</tr>
<tr>
<td>policy (SSM Maps)</td>
<td>3087</td>
</tr>
<tr>
<td>ppm</td>
<td>3088</td>
</tr>
<tr>
<td>ppm (Ethernet Switching)</td>
<td>3089</td>
</tr>
<tr>
<td>preference (Routing Options)</td>
<td>3090</td>
</tr>
<tr>
<td>prefix</td>
<td>3091</td>
</tr>
<tr>
<td>qualified-next-hop (Static Routes)</td>
<td>3092</td>
</tr>
<tr>
<td>readvertise</td>
<td>3094</td>
</tr>
<tr>
<td>redundant-sources</td>
<td>3095</td>
</tr>
<tr>
<td>resolution</td>
<td>3096</td>
</tr>
<tr>
<td>resolution-ribs</td>
<td>3097</td>
</tr>
<tr>
<td>resolve</td>
<td>3098</td>
</tr>
<tr>
<td>restart-duration (Routing Options)</td>
<td>3099</td>
</tr>
<tr>
<td>retain</td>
<td>3100</td>
</tr>
<tr>
<td>reverse-of-mapping</td>
<td>3101</td>
</tr>
<tr>
<td>rpf-check-policy (Routing Options RPF)</td>
<td>3102</td>
</tr>
<tr>
<td>rib (General)</td>
<td>3103</td>
</tr>
<tr>
<td>rib (Route Resolution)</td>
<td>3105</td>
</tr>
<tr>
<td>rib-group (Routing Options)</td>
<td>3106</td>
</tr>
<tr>
<td>rib-groups</td>
<td>3107</td>
</tr>
<tr>
<td>route-distinguisher-id</td>
<td>3109</td>
</tr>
<tr>
<td>route-record</td>
<td>3110</td>
</tr>
<tr>
<td>router-id</td>
<td>3111</td>
</tr>
<tr>
<td>routing-options</td>
<td>3112</td>
</tr>
<tr>
<td>scope</td>
<td>3112</td>
</tr>
<tr>
<td>scope-policy</td>
<td>3113</td>
</tr>
<tr>
<td>source (Source-Specific Multicast)</td>
<td>3114</td>
</tr>
<tr>
<td>source-routing</td>
<td>3115</td>
</tr>
<tr>
<td>ssm-groups</td>
<td>3116</td>
</tr>
<tr>
<td>ssm-map (Routing Options Multicast)</td>
<td>3117</td>
</tr>
<tr>
<td>static (Routing Options)</td>
<td>3118</td>
</tr>
<tr>
<td>subscriber-leave-timer</td>
<td>3124</td>
</tr>
<tr>
<td>tag (Routing Options)</td>
<td>3125</td>
</tr>
<tr>
<td>threshold (Multicast Forwarding Cache)</td>
<td>3126</td>
</tr>
<tr>
<td>timeout (Flow Maps)</td>
<td>3127</td>
</tr>
<tr>
<td>timeout (Multicast)</td>
<td>3128</td>
</tr>
<tr>
<td>traceoptions (Routing Options)</td>
<td>3129</td>
</tr>
<tr>
<td>Chapter 64</td>
<td>Configuration Examples ................................................. 3315</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Example: Configuring IGMP Snooping .................................. 3315</td>
</tr>
<tr>
<td></td>
<td>Configuration Tasks ...................................................... 3318</td>
</tr>
<tr>
<td></td>
<td>Configuring IGMP Snooping (CLI Procedure) .......................... 3318</td>
</tr>
<tr>
<td></td>
<td>Enabling IGMP Snooping on VLANs ...................................... 3319</td>
</tr>
<tr>
<td></td>
<td>Enabling Immediate Leave .............................................. 3319</td>
</tr>
<tr>
<td></td>
<td>Configuring an Interface as a Multicast-Router Interface .......... 3320</td>
</tr>
<tr>
<td></td>
<td>Configuring Static Group Membership on an Interface ............... 3321</td>
</tr>
<tr>
<td></td>
<td>Changing the Timer and Counter Values ................................ 3322</td>
</tr>
<tr>
<td></td>
<td>Configuring IGMP Snooping (J-Web Procedure) ......................... 3323</td>
</tr>
<tr>
<td></td>
<td>Configuring IGMP Snooping Tracing Operations (CLI Procedure) ...... 3325</td>
</tr>
<tr>
<td></td>
<td>Configuring Tracing Operations ....................................... 3326</td>
</tr>
<tr>
<td></td>
<td>Viewing, Stopping, and Restarting Tracing Operations ............... 3327</td>
</tr>
<tr>
<td></td>
<td>Configuration Statements .............................................. 3327</td>
</tr>
<tr>
<td></td>
<td>[edit protocols] Configuration Statement Hierarchy on EX Series</td>
</tr>
<tr>
<td></td>
<td>Switches ........................................................................ 3327</td>
</tr>
<tr>
<td></td>
<td>[edit protocols igmp-snooping] Configuration Statement Hierarchy .. 3329</td>
</tr>
<tr>
<td></td>
<td>Supported Statements in the [edit protocols igmp-snooping] Hierarchy Level ......................................................................................... 3329</td>
</tr>
<tr>
<td></td>
<td>Unsupported Statements in the [edit protocols igmp-snooping] Hierarchy Level ......................................................................................... 3330</td>
</tr>
<tr>
<td></td>
<td>accounting (Protocols IGMP Interface) .................................. 3330</td>
</tr>
<tr>
<td></td>
<td>accounting (Protocols IGMP) .............................................. 3331</td>
</tr>
<tr>
<td></td>
<td>address (Anycast RPs) ..................................................... 3331</td>
</tr>
<tr>
<td></td>
<td>address (Local RPs) ......................................................... 3332</td>
</tr>
<tr>
<td></td>
<td>anycast-pim ...................................................................... 3332</td>
</tr>
<tr>
<td></td>
<td>assert-timeout .................................................................. 3333</td>
</tr>
<tr>
<td></td>
<td>auto-rp ........................................................................... 3334</td>
</tr>
<tr>
<td></td>
<td>bootstrap ........................................................................ 3335</td>
</tr>
<tr>
<td></td>
<td>bootstrap-export ................................................................ 3336</td>
</tr>
<tr>
<td></td>
<td>bootstrap-import ................................................................ 3337</td>
</tr>
<tr>
<td></td>
<td>bootstrap.priority ............................................................ 3338</td>
</tr>
<tr>
<td></td>
<td>data-forwarding .............................................................. 3339</td>
</tr>
<tr>
<td></td>
<td>dense-groups .................................................................... 3340</td>
</tr>
<tr>
<td></td>
<td>disable (IGMP Snooping) .................................................... 3340</td>
</tr>
<tr>
<td></td>
<td>disable (Protocols IGMP) .................................................... 3341</td>
</tr>
<tr>
<td></td>
<td>disable (PIM) .................................................................... 3342</td>
</tr>
<tr>
<td></td>
<td>dr-election-on-p2p ........................................................... 3343</td>
</tr>
<tr>
<td></td>
<td>dr-register-policy ............................................................ 3343</td>
</tr>
<tr>
<td></td>
<td>embedded-rp ..................................................................... 3344</td>
</tr>
<tr>
<td></td>
<td>export (Protocols PIM Bootstrap) .......................................... 3345</td>
</tr>
<tr>
<td></td>
<td>family (Bootstrap) ............................................................. 3346</td>
</tr>
</tbody>
</table>
family (Local RP) .................................................. 3347
graceful-restart (Protocols PIM) .............................. 3348
group (IGMP Snooping) ......................................... 3348
group (Protocols IGMP) ........................................ 3349
group-ranges ...................................................... 3350
hello-interval (Protocols PIM) ............................... 3351
hold-time (Protocols PIM) ...................................... 3352
igmp-snooping ................................................... 3353
immediate-leave (Protocols IGMP) ............................ 3354
immediate-leave (IGMP Snooping) ............................. 3355
import (Protocols PIM Bootstrap) ............................ 3356
import (Protocols PIM) ......................................... 3357
infinity ............................................................ 3358
interface (IGMP Snooping) ...................................... 3359
interface (Protocols PIM) ....................................... 3360
interface (Protocols IGMP) ..................................... 3362
join-load-balance ............................................... 3363
local ............................................................ 3364
local-address (Protocols PIM) ............................... 3365
mapping-agent-election ....................................... 3366
maximum-rps .................................................... 3367
mode (Protocols PIM) .......................................... 3368
multicast-router-interface (IGMP Snooping) .................. 3369
neighbor-policy ................................................ 3370
pim ............................................................. 3371
priority (PIM Interfaces) ....................................... 3375
priority (Bootstrap) ............................................. 3376
priority (PIM RPs) ............................................. 3377
query-interval (Protocols IGMP) .............................. 3378
query-last-member-interval (Protocols IGMP) ............... 3379
query-response-interval (Protocols IGMP) ................... 3380
receiver .......................................................... 3381
restart-duration (Protocols PIM) ............................. 3382
rib-group (Protocols PIM) ..................................... 3383
robust-count (IGMP Snooping) ................................ 3384
robust-count (Protocols IGMP) ............................... 3384
rp ............................................................... 3385
rp-register-policy .............................................. 3387
rp-set ........................................................... 3388
source (Protocols IGMP) ....................................... 3389
source-vlans .................................................... 3390
spt-threshold .................................................... 3391
ssm-map (Protocols IGMP) ..................................... 3392
static (IGMP Snooping) ........................................ 3392
static (Protocols PIM) ......................................... 3393
static (Protocols IGMP) ....................................... 3394
traceoptions (Protocols PIM) ................................. 3395
traceoptions (Protocols IGMP) ............................... 3395
traceoptions (IGMP Snooping) ............................... 3401
Chapter 65\hfill Administration \hfill 3407

Routine Monitoring \hfill 3407
  Monitoring IGMP Snooping \hfill 3407
  Verifying IGMP Snooping (CLI Procedure) \hfill 3410
    Verifying IGMP Snooping Memberships \hfill 3410
    Viewing IGMP Snooping Statistics \hfill 3411
    Viewing IGMP Snooping Routing Information \hfill 3411

Operational Commands \hfill 3412
  clear igmp membership \hfill 3413
  clear igmp statistics \hfill 3416
  clear igmp-snooping membership \hfill 3418
  clear igmp-snooping statistics \hfill 3419
  clear multicast bandwidth-admission \hfill 3420
  clear multicast scope \hfill 3422
  clear multicast sessions \hfill 3423
  clear multicast statistics \hfill 3424
  clear pim join \hfill 3425
  clear pim register \hfill 3427
  clear pim statistics \hfill 3429
  mtrace \hfill 3431
  mtrace from-source \hfill 3434
  mtrace monitor \hfill 3437
  mtrace to-gateway \hfill 3439
  show igmp group \hfill 3442
  show igmp interface \hfill 3446
  show igmp statistics \hfill 3450
  show igmp-snooping membership \hfill 3453
  show igmp-snooping route \hfill 3456
  show igmp-snooping statistics \hfill 3458
  show multicast flow-map \hfill 3460
  show multicast interface \hfill 3462
  show multicast mrinfo \hfill 3464
  show multicast next-hops \hfill 3466
  show multicast pim-to-igmp-proxy \hfill 3469
  show multicast pim-to-mld-proxy \hfill 3471
  show multicast route \hfill 3473
  show multicast rpf \hfill 3479
  show multicast scope \hfill 3483
  show multicast sessions \hfill 3485
  show multicast usage \hfill 3488
  show pim bootstrap \hfill 3491
  show pim interfaces \hfill 3493
  show pim join \hfill 3496
  show pim neighbors \hfill 3510
show pim rps ................................................................. 3514
show pim source ......................................................... 3521
show pim statistics ....................................................... 3524

Part 22  Network Management and Monitoring

Chapter 66  Overview ..................................................3539

Real-Time Performance Monitoring ........................................3539
Understanding Real-Time Performance Monitoring on EX Series
Switches ................................................................. 3540
RPM Packet Collection .................................................. 3540
Tests and Probe Types .................................................... 3540
Hardware Timestamps ..................................................... 3541
Limitations of RPM on EX Series Switches ............................... 3543

Analyzers and Port Mirroring ............................................3543
Understanding Port Mirroring and Analyzers on EX4300 Switches .. 3544
Port Mirroring Overview .................................................. 3544
Analyzer Overview ........................................................ 3545
Port Mirroring and Analyzer Terminologies ............................... 3545
Configuration Guidelines for Port Mirroring and Analyzers on EX4300
Switches ................................................................. 3546

sFlow Monitoring Technology ............................................3548
Understanding How to Use sFlow Technology for Network Monitoring on
an EX Series Switch .................................................... 3549
Sampling Mechanism and Architecture of sFlow Technology on EX
Series Switches .......................................................... 3549
Adaptive Sampling ........................................................ 3550
sFlow Agent Address Assignment ........................................ 3551

Ethernet OAM Link Fault Management and Connectivity Fault Management .. 3551
Understanding Ethernet OAM Link Fault Management for an EX Series
Switch ................................................................. 3551
Understanding Ethernet OAM Connectivity Fault Management for an EX
Series Switch .......................................................... 3553
Understanding Ethernet Frame Delay Measurements on Switches .... 3554
Ethernet Frame Delay Measurements .................................... 3554
Types of Ethernet Frame Delay Measurements .......................... 3555
Limitations ................................................................. 3556

Uplink Failure Detection ..................................................3556
Understanding Uplink Failure Detection .................................. 3556
Uplink Failure Detection Overview ....................................... 3557
Failure Detection Pair ...................................................... 3558

Chapter 67  Configuration ..................................................3559

Configuration Examples .....................................................3559
Example: Configuring sFlow Technology to Monitor Network Traffic on EX
Series Switches .......................................................... 3559
Example: Configuring Mirroring for Local Monitoring of Employee Resource
Use on EX4300 Switches ................................................ 3564
Example: Configuring Mirroring for Remote Monitoring of Employee Resource
Use on EX4300 Switches ................................................ 3570
Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches ...................................... 3580
Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches .......................................................... 3587
Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches .......................................................... 3591
Configuration Tasks .......................................................... 3593
Configuring SNMP (J-Web Procedure) ........................................ 3594
Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) .......................................................... 3597
Configuring an Analyzer for Local Traffic Analysis ......................... 3598
Configuring an Analyzer for Remote Traffic Analysis ...................... 3598
Configuring Port Mirroring ................................................... 3599
Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) .... 3601
Configuring sFlow Technology for Network Monitoring (CLI Procedure) .......................................................... 3603
Configuring Real-Time Performance Monitoring (J-Web Procedure) .. 3604
Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure) ........................................ 3611
Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) .......................................................... 3612
Creating the Maintenance Domain ........................................... 3612
Configuring the Maintenance Domain MIP Half Function ................ 3613
Creating a Maintenance Association .......................................... 3613
Configuring the Continuity Check Protocol .................................. 3614
Configuring a Maintenance Association End Point ......................... 3614
Configuring a Connectivity Fault Management Action Profile .......... 3615
Configuring the Linktrace Protocol ......................................... 3615
Configuring Ethernet OAM Link Fault Management (CLI Procedure) .......................................................... 3616
Configuring Interfaces for Uplink Failure Detection (CLI Procedure) .......................................................... 3618
Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) ........................................ 3619
Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) .......................................................... 3620
Configuring an Iterator Profile on a Switch (CLI Procedure) .......... 3621
Triggering an Ethernet Frame Delay Measurement Session on a Switch .......................................................... 3622
Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) .......................................................... 3623
Configuration Statements: SNMP ........................................... 3623
[edit snmp] Configuration Statement Hierarchy on EX Series Switches .......................................................... 3623
Supported Statements in the [edit snmp] Hierarchy Level ................ 3624
Unsupported Statements in the [edit snmp] Hierarchy Level .............. 3628
address (SNMP) .......................................................... 3631
address-mask .......................................................... 3632
agent-address .......................................................... 3632
alarm (SNMP RMON) ................................................... 3633
authorization .......................................................... 3634
bucket-size .......................................................... 3634
categories .......................................................... 3635
client-list .......................................................... 3635
routing-instance (SNMPv3) ........................................ 3670
sample-type ................................................... 3670
security-level (Defining Access Privileges) ................. 3671
security-level (Generating SNMP Notifications) .......... 3672
security-model (Access Privileges) ......................... 3673
security-model (Group) ....................................... 3674
security-model (SNMP Notifications) ....................... 3675
security-name (Security Group) ........... 3676
security-name (Community String) ......................... 3677
security-name (SNMP Notifications) ....................... 3678
security-to-group ............................................ 3679
snmp ......................................................... 3679
snmp-community ............................................. 3680
source-address (SNMP) ....................................... 3682
startup-alarm ............................................... 3683
syslog-subtag ............................................... 3683
tag (SNMPv3) ............................................... 3684
tag-list ...................................................... 3684
target-address ............................................... 3685
target-parameters .......................................... 3686
targets ......................................................... 3687
traceoptions (SNMP) ......................................... 3688
trap-group .................................................... 3690
trap-options ................................................ 3691
type (SNMP RMON) ........................................... 3692
type (SNMPv3) ............................................... 3693
v3 .......................................................... 3694
vacm .......................................................... 3696
variable ....................................................... 3697
version (SNMP) ............................................... 3697
view (Associating a MIB View with a Community) ....... 3698
view (Configuring a MIB View) ............................ 3699
write-view .................................................. 3700
Configuration Statements: Analyzers and Port Mirroring .... 3700
[edit forwarding-options port-mirroring] Hierarchy Level .. 3700
[edit forwarding-options analyzer] Hierarchy Level ........ 3701
egress ........................................................ 3702
egress (Analyzer) ........................................... 3702
ingress (vlans) ................................................ 3703
ingress (Analyzer) ........................................... 3703
input (Analyzer) ............................................. 3704
interface ...................................................... 3705
no-tag ........................................................ 3706
output (Mirroring) ........................................... 3706
vlan (Mirroring) ............................................. 3707
Configuration Statements: sFlow Technology ........................... 3707
  [edit protocols] Configuration Statement Hierarchy on EX4300 Switches .................................. 3707
  [edit protocols sflow] Configuration Statement Hierarchy on EX Series Switches .................. 3707
  Supported Statements in the [edit protocols sflow] Hierarchy Level .................................. 3708
  Unsupported Statements in the [edit sflow] Hierarchy Level ............................................. 3708
  agent-id ................................................................. 3710
  collector ............................................................... 3710
  disable (sFlow Monitoring Technology) ....................................................... 3711
  interfaces (sFlow Monitoring Technology) .................................................. 3712
  polling-interval ...................................................... 3713
  sample-rate .......................................................... 3714
  sflow ................................................................. 3715
  source-ip .............................................................. 3716
  udp-port ............................................................... 3716

Configuration Statements: Ethernet OAM Connectivity Fault Management .......................... 3717
  action-profile (Applying to OAM CFM, for EX Series Switch Only) .................................. 3717
  age (EX Series Switch Only) ............................................ 3718
  auto-discovery (EX Series Switch Only) .................................. 3718
  calculation-weight .................................................... 3719
  connectivity-fault-management (EX Series Switch Only) .............................................. 3720
  continuity-check (EX Series Switch Only) ................................................. 3720
  cycle-time ............................................................. 3721
  delay ................................................................. 3722
  delay-variation ....................................................... 3723
  direction (EX Series Switch Only) ........................................ 3724
  hold-interval (OAM CFM, for EX Series Switch Only) .............................................. 3725
  interface (OAM CFM, for EX Series Switch Only) ................................................. 3725
  interval (EX Series Switch Only) ........................................ 3726
  iteration-period ...................................................... 3727
  level (EX Series Switch Only) .......................................... 3728
  linktrace (EX Series Switch Only) .......................................... 3729
  loss-threshold (EX Series Switch Only) ......................................... 3729
  maintenance-association (EX Series Switch Only) .............................................. 3730
  maintenance-domain (EX Series Switch Only) .............................................. 3730
  measurement-type (OAM LFM) ............................................. 3731
  mep (EX Series Switch Only) ............................................. 3732
  mep-half-function (EX Series Switch Only) ........................................... 3733
  name-format (EX Series Switch Only) ........................................... 3734
  path-database-size (EX Series Switch Only) .............................................. 3735
  performance-monitoring (OAM LFM) .............................................. 3735
  remote-mep (EX Series Switch Only) ............................................. 3736
  sla-iterator-profiles (OAM LFM) ............................................. 3737

Configuration Statements: Ethernet OAM Link Fault Management ................................. 3739
  action (OAM LFM) .......................................................... 3739
  action-profile .......................................................... 3740
  allow-remote-loopback ................................................... 3741
  ethernet (OAM LFM) .......................................................... 3742
link-to-monitor ........................................ 3779
traceoptions (Uplink Failure Detection) ............... 3780
uplink-failure-detection ................................ 3781

Chapter 68  Administration  .................................................. 3783

Routine Monitoring ................................................... 3783
Monitoring Hosts Using the J-Web Ping Host Tool ........ 3783
Monitoring Network Traffic Using Traceroute ............ 3785
Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches ................. 3786
Viewing Real-Time Performance Monitoring Information .......... 3787
Verifying That Uplink Failure Detection Is Working Correctly ........ 3788

Operational Commands: General ....................... 3789
monitor traffic .................................................. 3790
ping ............................................................. 3800
show pfe statistics bridge .................................. 3804
traceroute ...................................................... 3809

Operational Commands: RPM .............................. 3812
show services rpm active-servers ...................... 3813
show services rpm history-results .................... 3814
show services rpm probe-results ..................... 3817

Operational Commands: SNMP ............................. 3822
clear snmp rmon history .................................. 3823
clear snmp statistics ....................................... 3824
request snmp spoof-trap .................................. 3826
show snmp health-monitor ................................ 3832
show snmp inform-statistics ......................... 3839
show snmp mib ................................................. 3841
show snmp rmon ............................................. 3844
show snmp rmon history .................................. 3848
show snmp statistics ..................................... 3852
show snmp v3 .................................................. 3856

Operational Commands: Analyzers and Port Mirroring ....... 3858
show forwarding-options port-mirroring ............... 3859
show forwarding-options analyzer .................... 3861

Operational Commands: sFlow ..................................... 3862
show sflow ................................................... 3863
show sflow interface ...................................... 3865
show sflow collector ...................................... 3867
clear sflow collectors statistics ..................... 3868

Operational Commands: Ethernet OAM Connectivity Fault Management ................. 3868
clear oam ethernet connectivity-fault-management delay-statistics 3869
clear oam ethernet connectivity-fault-management sla-iterator-statistics .................. 3871
clear oam ethernet connectivity-fault-management statistics 3872
monitor ethernet delay-measurement .................. 3873
show oam ethernet connectivity-fault-management delay-statistics 3878
show oam ethernet connectivity-fault-management forwarding-state 3882
show oam ethernet connectivity-fault-management interfaces 3886
Part 25 Routing Policy and Packet Filtering

Chapter 77 Overview ...................................................... 4085

Security Features Overview ........................................... 4085
Security Features for EX Series Switches Overview .......... 4085
Firewall Filters Overview .............................................. 4087
Firewall Filters for EX Series Switches Overview .......... 4088
Firewall Filter Types .................................................. 4088
Firewall Filter Components .......................................... 4089
Firewall Filter Processing ............................................ 4090
Understanding Planning of Firewall Filters ..................... 4091
Understanding Firewall Filter Processing Points for Bridged and Routed
Packets on EX Series Switches ..................................... 4094
Understanding How Firewall Filters Control Packet Flows .... 4095
Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series
Switches .................................................................. 4096
Firewall Filter Elements .............................................. 4097
Match Conditions Supported on Switches ....................... 4097
Actions for Firewall Filters ........................................... 4104
Action Modifiers for Firewall Filters .............................. 4105
Support for Match Conditions and Actions for Loopback Firewall Filters on
Switches .................................................................. 4107
Platform Support for Firewall Filter Match Conditions, Actions, and Action
Modifiers on EX Series Switches ................................. 4111
Firewall Filter Types and Their Bind Points ..................... 4111
Support for IPv4 and IPv6 Firewall Filters on Switches ...... 4112
Platform Support for Match Conditions for IPv4 Traffic .... 4112
Platform Support for Match Conditions for IPv6 Traffic .... 4125
Platform Support for Match Conditions for Non-IP Traffic .. 4133
Platform Support for Actions for IPv4 Traffic ................. 4133
Platform Support for Actions for IPv6 Traffic ................. 4136
Platform Support for Action Modifiers for IPv4 Traffic ..... 4138
Platform Support for Action Modifiers for IPv6 Traffic ..... 4144
Understanding How Firewall Filters Are Evaluated .......... 4149
Understanding Firewall Filter Match Conditions .............. 4151
Filter Match Conditions .............................................. 4151
Numeric Filter Match Conditions ................................. 4151
Interface Filter Match Conditions .................................. 4152
IP Address Filter Match Conditions .............................. 4152
MAC Address Filter Match Conditions ......................... 4153
Bit-Field Filter Match Conditions ................................. 4153
Understanding How Firewall Filters Test a Packet's Protocol .. 4155
Understanding the Use of Policers in Firewall Filters ........ 4155
Policers Overview ...................................................... 4155
Policer Types .......................................................... 4156
Policer Actions ........................................................ 4157
Policer Levels .......................................................... 4157
Color Modes ............................................................. 4158
Naming Conventions for Policers ................................. 4158
Chapter 78 Configuration ................................................... 4161

Configuration Examples ................................................. 4161
Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches .............. 4161
Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch .................. 4179
Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches .................. 4183
Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication .................. 4186

Configuration Tasks ...................................................... 4191
Configuring Firewall Filters (CLI Procedure) ...................... 4192
Configuring a Firewall Filter ........................................ 4192
Configuring a Term Specifically for IPv4 or IPv6 Traffic ........ 4196
Applying a Firewall Filter to a Port on a Switch ................ 4197
Applying a Firewall Filter to a Management Interface on a Switch ................ 4198
Applying a Firewall Filter to a VLAN on a Network .......... 4199
Applying a Firewall Filter to a Layer 3 (Routed) Interface .... 4200
Configuring Firewall Filters (J-Web Procedure) .................. 4201
Configuring Policers to Control Traffic Rates (CLI Procedure) .... 4206
Configuring Policers ................................................. 4207
Specifying Policers in a Firewall Filter Configuration ........... 4208
Applying a Firewall Filter That Is Configured with a Policier .... 4208
Assigning Multifield Classifiers in Firewall Filters to Specify
Packet-Forwarding Behavior (CLI Procedure) .................... 4209
Configuring Routing Policies (J-Web Procedure) .................. 4210
Configuring Tricolor Marking Policers ......................... 4215
Configuring a Tricolor Marking Policier ..................... 4216
Applying Tricolor Marking Policers to Firewall Filters ......... 4216

Configuration Statements ............................................ 4217
[edit firewall] Configuration Statement Hierarchy on EX Series Switches ........................................ 4217
Supported Statements in the [edit firewall] Hierarchy Level .... 4218
Unsupported Statements in the [edit firewall] Hierarchy Level .... 4219
Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches .......... 4219
action (TCM Policers) .................................................. 4222
apply-path .............................................................. 4222
as-path (Policy Options) ............................................ 4223
as-path-group .......................................................... 4224
bandwidth-limit ........................................................ 4225
burst-size-limit .......................................................... 4226
color-aware .............................................................. 4227
color-blind .............................................................. 4227
committed-burst-size .................................................. 4228
committed-information-rate ......................................... 4229
community (Policy Options) .......................................... 4230
Spanning-Tree Protocols

Overview ...................................................... 4297

Spanning Trees Overview ................................ 4297
Understanding MSTP for EX Series Switches .......... 4298
MSTP Maps Multiple VLANs ................................ 4298
Configuring MSTP Regions ................................. 4299
Selecting a Spanning-Tree Protocol ..................... 4299
Understanding RSTP for EX Series Switches .......... 4300
Spanning-Tree Protocols Help Prevent Broadcast Storms 4300
RSTP is an Enhancement of the Original STP .......... 4301
Port Roles Determine Participation in The Spanning-Tree 4301
Port States Determine How a Port Processes a Frame 4301
Edge Ports Connect to Devices That Cannot Be Part of a Spanning-Tree 4302
BPDUs Maintain the Spanning-Tree ....................... 4302
When an RSTP Root Bridge Fails ......................... 4303
Switches Must Relearn MAC Addresses After a Link Failure 4303
Selecting a Spanning-Tree Protocol ..................... 4303
Understanding STP for EX Series Switches ............ 4304
Selecting a Spanning-Tree Protocol ..................... 4305
RSTP or VSTP Forced to Run as IEEE 802.1D STP ....... 4306
Understanding VSTP for EX Series Switches .......... 4306
Selecting a Spanning-Tree Protocol ..................... 4307
Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches ............................. 4308
Different Kinds of BPDUs ................................ 4308
Protecting Switches From Incompatible BPDUs ....... 4308
Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches ......................... 4310
Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches ......................... 4311

Configuration .................................................. 4313

Configuration Examples .................................. 4313
Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches ............. 4313
Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches ......................... 4330
Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches ................................. 4352
Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches ................................. 4357
Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches ................................. 4363
Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches .......................... 4367
Configuration Tasks ....................................................... 4372
Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure) ... 4372
Configuring Spanning-Tree Protocols (J-Web Procedure) ................. 4373
Configuring VSTP (CLI Procedure) ..................................... 4378
Unblocking an Interface That Receives BPDUs in Error (CLI Procedure) 4380
Operational Tasks ......................................................... 4380
Reverting to RSTP or VSTP from Forced IEEE 802.1D STP ............... 4381
Configuration Statements .................................................. 4381
[edit protocols] Configuration Statement Hierarchy on EX Series

Switches ................................................................. 4382
block (Spanning Trees) .................................................. 4384
bpdus-block ............................................................ 4385
bpdus-block-on-edge .................................................. 4386
bpdus-timeout-action (Spanning Trees) ................................ 4387
bridge-priority (Spanning Trees) ...................................... 4388
configuration-name (Spanning Trees) .................................. 4389
cost (Spanning Trees) ................................................... 4390
disable (Spanning Trees) ............................................... 4391
disable-timeout (Spanning Trees) ...................................... 4392
disabled (Spanning Trees) .............................................. 4393
force-version (IEEE 802.1D STP) ...................................... 4394
forward-delay (Spanning Trees) ........................................ 4395
hello-time (Spanning Trees) ............................................ 4396
interface (BPDU Block) ............................................... 4397
interface (Spanning Trees) ............................................. 4398
log (Spanning Trees) ................................................... 4399
max-age (Spanning Trees) ............................................... 4400
max-hops (Spanning Trees) ............................................. 4401
mode (Spanning Trees) ................................................... 4402
msti (Spanning Trees) ................................................... 4403
mstp (Spanning Trees) ................................................... 4404
no-root-port (Spanning Trees) ......................................... 4405
priority (Spanning Trees) ............................................... 4406
revision-level (Spanning Trees) ....................................... 4407
rstp (Spanning Trees) ................................................... 4408
stp (Spanning Trees) .................................................... 4410
traceoptions (Spanning Trees) ......................................... 4412
vlan (Spanning Trees) ................................................... 4415
vlan (VSTP) ............................................................ 4417
vstp ................................................................. 4419
Administration ............................................................. 4421
Routine Monitoring ....................................................... 4421
Monitoring Spanning-Tree Protocols .................................... 4421
Operational Commands .................................................. 4423
clear ethernet-switching bpdu-error ................................... 4424
clear spanning-tree protocol-migration ................................. 4425

Chapter 83 Administration .................................................. 4421
Routine Monitoring ....................................................... 4421
Monitoring Spanning-Tree Protocols .................................... 4421
Operational Commands .................................................. 4423
clear ethernet-switching bpdu-error ................................... 4424
clear spanning-tree protocol-migration ................................. 4425
clear spanning-tree statistics ........................................ 4426
clear spanning-tree statistics ........................................ 4427
show spanning-tree bridge ........................................... 4428
show spanning-tree bridge ........................................... 4433
show spanning-tree interface ........................................ 4438
show spanning-tree interface ........................................ 4442
show spanning-tree mstp configuration ............................ 4448
show spanning-tree mstp configuration ............................ 4450
show spanning-tree statistics ........................................ 4452
show spanning-tree statistics ........................................ 4454

**Part 27** Virtual Chassis

**Chapter 84** Overview ............................................. 4459

Virtual Chassis Overview ............................................. 4459
Understanding EX4300 Virtual Chassis ............................. 4459
Understanding EX Series Virtual Chassis Components ............ 4460
  Maximum Number of Switches per Virtual Chassis .............. 4461
  Virtual Chassis Ports (VCPs) ....................................... 4462
  Master Role .......................................................... 4463
  Backup Role .......................................................... 4463
  Linecard Role ......................................................... 4464
  Member Switch and Member ID ..................................... 4464
  Mastership Priority .................................................. 4465
  Mixed Virtual Chassis .............................................. 4465
  Virtual Chassis Identifier (VCID) ................................. 4466
Understanding How the Master in an EX Series Virtual Chassis Is Elected ......................................................... 4467
Understanding Software Upgrade in an EX Series Virtual Chassis ................................................................. 4468
Understanding Global Management of an EX Series Virtual Chassis ............................................................... 4469
  Nonvolatile Memory Features ....................................... 4472
Understanding EX Series Virtual Chassis Port Link Aggregation .............................................................. 4472
Understanding EX Series Virtual Chassis Configuration ........ 4475
Understanding Split and Merge in an EX Series Virtual Chassis .............................................................. 4476
  What Happens When a Virtual Chassis Configuration Splits ...... 4477
  Merging Virtual Chassis Configurations .......................... 4478
Understanding Automatic Software Update on EX Series Virtual Chassis .............................................................. 4479
  Member Switches ....................................................... 4479
  Automatic Software Update Basics ................................ 4480
  Automatic Software Update Restrictions ........................ 4480
Understanding MAC Address Assignment on a Virtual Chassis .......................................................... 4482
Understanding High Availability on an EX Series Virtual Chassis .......................................................... 4483
Chapter 86  Administration ................................................. 4529

Routine Monitoring ................................................. 4529

Command Forwarding Usage with an EX Series Virtual Chassis .... 4529

Verifying the Member ID, Role, and Neighbor Member Connections of an EX Series Virtual Chassis Member ............ 4534

Verifying That Virtual Chassis Ports on an EX Series Switch Are Operational ............................................. 4535

Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis ........................................... 4537

Verifying That Graceful Routing Engine Switchover Is Working in the Virtual Chassis ........................................ 4538

Operational Commands ................................................. 4540

clear virtual-chassis vc-port statistics ................................... 4541

request session member .................................................. 4543

request virtual-chassis recycle .......................................... 4544

request virtual-chassis renumber ...................................... 4545

request virtual-chassis vc-port ......................................... 4546

request virtual-chassis vc-port diagnostics optics .................. 4548

show system uptime ...................................................... 4549

show virtual-chassis active-topology ................................ 4551

show virtual-chassis device-topology .................................. 4554

show virtual-chassis login .............................................. 4557

show virtual-chassis protocol adjacency .............................. 4558

show virtual-chassis protocol database .............................. 4562

show virtual-chassis protocol interface ................................ 4566

show virtual-chassis protocol route .................................... 4568

show virtual-chassis protocol statistics ............................. 4571

show virtual-chassis .................................................... 4574

show virtual-chassis vc-path .......................................... 4577

show virtual-chassis vc-port .......................................... 4579

show virtual-chassis vc-port diagnostics optics .................. 4583

show virtual-chassis vc-port statistics ............................ 4597

Chapter 87  Troubleshooting ................................................. 4605

Troubleshooting Procedures ........................................... 4605

Troubleshooting an EX Series Virtual Chassis ...................... 4605

A Disconnected Member Switch’s ID Is Not Available for
Reassignment .............................................................. 4605

Load Factory Default Does Not Commit on a Multimember Virtual Chassis ...................................................... 4605
Table of Contents

The Member ID Persists When a Member Switch Is Disconnected From a Virtual Chassis ........................................ 4606
A Member Switch Is Not Participating in a Mixed Virtual Chassis . . . 4606
# List of Figures

<table>
<thead>
<tr>
<th>Part 3</th>
<th>System Setup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 6</td>
<td>Troubleshooting Procedures</td>
</tr>
<tr>
<td>Figure 1: Connecting to the Console Port on the EX Series Switch</td>
<td>379</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 5</th>
<th>Access and User Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 13</td>
<td>Troubleshooting Procedures</td>
</tr>
<tr>
<td>Figure 2: Connecting to the Console Port on the EX Series Switch</td>
<td>485</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 6</th>
<th>Configuration and File Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 15</td>
<td>Configuration</td>
</tr>
<tr>
<td>Figure 3: EX Series Switch LCD Panel</td>
<td>505</td>
</tr>
<tr>
<td>Chapter 17</td>
<td>Troubleshooting Procedures</td>
</tr>
<tr>
<td>Figure 4: Connecting to the Console Port on the EX Series Switch</td>
<td>565</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 9</th>
<th>System Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 25</td>
<td>Overview</td>
</tr>
<tr>
<td>Figure 5: DHCP Options Data Flow</td>
<td>1211</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 10</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 28</td>
<td>Overview</td>
</tr>
<tr>
<td>Figure 6: Example Authentication Topology</td>
<td>1659</td>
</tr>
<tr>
<td>Figure 7: VoIP Multiple Supplicant Topology</td>
<td>1668</td>
</tr>
<tr>
<td>Figure 8: VoIP Single Supplicant Topology</td>
<td>1669</td>
</tr>
<tr>
<td>Figure 9: Authentication Process Flow for an EX Series Switch</td>
<td>1672</td>
</tr>
<tr>
<td>Chapter 29</td>
<td>Configuration</td>
</tr>
<tr>
<td>Figure 10: Topology for Configuration</td>
<td>1677</td>
</tr>
<tr>
<td>Figure 11: Topology for Guest VLAN Example</td>
<td>1681</td>
</tr>
<tr>
<td>Figure 12: Topology for Configuring Supplicant Modes</td>
<td>1686</td>
</tr>
<tr>
<td>Figure 13: VoIP Topology</td>
<td>1692</td>
</tr>
<tr>
<td>Figure 14: Topology for Static MAC Authentication Configuration</td>
<td>1705</td>
</tr>
<tr>
<td>Figure 15: Topology for Configuration</td>
<td>1709</td>
</tr>
<tr>
<td>Figure 16: Topology for MAC RADIUS Authentication Configuration</td>
<td>1715</td>
</tr>
<tr>
<td>Figure 17: Topology for Firewall Filter and RADIUS Server Attributes Configuration</td>
<td>1721</td>
</tr>
<tr>
<td>Figure 18: Conceptual Model: Dynamic Filter Updated for Each New User</td>
<td>1727</td>
</tr>
</tbody>
</table>
Part 11 Class of Service

Chapter 31 Overview .......................................................1861

Figure 22: Packet Flow Across the Network .........................1863
Figure 23: Graphical Representation of a Segmented Drop Profile .... 1877
Figure 24: Graphical Representation of an Interpolated Drop Profile on EX Series Switches Except EX4300 Switches ...............1878
Figure 25: Tail-Drop Profile Packet Drop on EX4300 Switches ........1879

Chapter 32 Configuration ..................................................1895

Figure 26: Topology for Configuring CoS .............................1896

Part 13 Ethernet Switching

Chapter 38 Overview ......................................................2049

Figure 27: An IRB Interface or RVI on a Switch Providing Routing Between Two Access Switches .................................2059
Figure 28: Creating an IRB Interface or RVI ...........................2060
Figure 29: Redundant Trunk Group, Link 1 Active ....................2069
Figure 30: Redundant Trunk Group, Link 2 Active ....................2069

Chapter 39 Configuration ..................................................2073

Figure 31: Sample Access Switch-Distribution Switch Topology ........2085
Figure 32: MVRP Configured on Two Access Switches and One Distribution Switch for Automatic VLAN Administration ..........2098
Figure 33: Topology for Configuring the Redundant Trunk Links ........2111

Part 14 High Availability

Chapter 41 Overview .......................................................2211

Figure 34: Basic VRRP on EX Series Switches .........................2221
Figure 35: VRRP on Virtual Chassis Switches .........................2221

Part 15 Interfaces

Chapter 44 Overview .......................................................2267

Figure 36: Symmetrically Routed Interfaces ..........................2278
Figure 37: Asymmetrically Routed Interfaces .........................2279

Part 21 Multicast

Chapter 63 Overview .......................................................3305

Figure 38: Multicast Traffic Flow with IGMP Snooping Enabled ........3306
Figure 39: Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts ..........................3310
Figure 40: Scenario 2: Switch Forwarding Multicast Traffic to Another Switch . 3311
Figure 41: Scenario 3: Switch Connected to Hosts Only (No IGMP Querier) . . 3312
Figure 42: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic
Between VLANs .......................................................... 3313

Chapter 64 Configuration ...................................................3315
Figure 43: IGMP Snooping Topology Sample Topology .................. 3316

Part 22 Network Management and Monitoring
Chapter 66 Overview ......................................................3539
Figure 44: RPM Timestamps .............................................. 3542
Figure 45: Relationship Among MEPs, MIPs, and Maintenance Domain Levels . 3554
Figure 46: Uplink Failure Detection Configuration on Switches ........... 3557

Chapter 67 Configuration ..................................................3559
Figure 47: sFlow Technology Monitoring System ....................... 3561
Figure 48: Network Topology for Local Mirroring Example ............. 3566
Figure 49: Remote Mirroring Network Topology Example .............. 3572
Figure 50: Remote Mirroring Through a Transit Switch Network—Sample
Topoogy ................................................................. 3581

Part 24 Port Security
Chapter 74 Overview ......................................................3995
Figure 51: DHCP Clients, Switch, and DHCP Server Are All on Same VLAN . 4002
Figure 52: Switch Acting as an Extended Relay Server .................. 4003
Figure 53: DHCP Server Connected Directly to Switch .................. 4007
Figure 54: DHCP Server Connected Directly to Switch 2, with Switch 2 Connected
to Switch 1 Through a Trusted Trunk Port .......................... 4007
Figure 55: Switch Is the DHCP Server . ................................. 4008
Figure 56: Switch Acting as Relay Agent Through Router to DHCP Server . 4009

Chapter 75 Configuration ...................................................4017
Figure 57: Network Topology for Basic Port Security .................. 4019

Part 25 Routing Policy and Packet Filtering
Chapter 77 Overview ......................................................4085
Figure 58: Firewall Filter Processing Points in the Packet Forwarding Path . 4094
Figure 59: Application of Firewall Filters to Control Packet Flow ........ 4096
Figure 60: Evaluation of Terms Within a Firewall Filter ................ 4150

Chapter 78 Configuration ..................................................4161
Figure 61: Application of Port, VLAN, and Layer 3 Routed Firewall Filters . . 4163
Figure 62: SSH Connection From a Management PC to an EX Series Switch . 4180
Figure 63: Conceptual Model: Dynamic Filter Updated for Each New User . 4188
Figure 64: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to
a File Server ............................................................ 4189
Part 26  Spanning-Tree Protocols
Chapter 82  Configuration ................................................. 4313
Figure 65: Network Topology for RSTP .................................. 4315
Figure 66: Network Topology for MSTP ............................... 4332
Figure 67: BPDU Protection Topology ................................. 4354
Figure 68: BPDU Protection Topology ......................... 4359
Figure 69: Network Topology for Loop Protection .............. 4364
Figure 70: Network Topology for Root Protection ................. 4369

Part 27  Virtual Chassis
Chapter 84  Overview .................................................. 4459
Figure 71: Console Session Redirection (EX4200 Virtual Chassis Pictured) 4470
Figure 72: Management Ethernet Port Redirection to the VME Interface ........ 4471
List of Tables

About the Documentation ................................................. xcv
Table 1: Notice Icons ......................................................... xcvii
Table 2: Text and Syntax Conventions .................................... xcvii

Part 1 Getting Started with ELS
Chapter 1 Getting Started with ELS ....................................... 3
Table 3: Enhanced Layer 2 CLI Changes ................................. 7
Table 4: Enhanced Layer 2 CLI Changes ................................. 15

Part 2 Software Features Overview
Chapter 2 Software Features Overview .................................. 27
Table 5: First Junos OS Release for Each EX Series Switch ............ 28
Table 6: Access Control Features on Switches by Junos OS Release ... 29
Table 7: Administration Features on Switches by Junos OS Release .... 30
Table 8: Class-of-Service (CoS) Features on Switches by Junos OS Release .... 31
Table 9: Class-of-Service (CoS) Features on EX9200 Switches by Junos OS Release .......... 32
Table 10: Converged Networks (LAN and SAN) Features on Switches by Junos OS Release ............ 34
Table 11: Device Security Features on Switches by Junos OS Release ........ 34
Table 12: High Availability and Resiliency Features on Switches by Junos OS Release ............... 35
Table 13: High Availability and Resiliency Features on EX9200 Switches by Junos OS Release .......... 37
Table 14: Interfaces Features on Switches by Junos OS Release ........... 39
Table 15: Interfaces Features on EX9200 Switches by Junos OS Release ................. 40
Table 16: IP Address Management Features on Switches by Junos OS Release ....................... 41
Table 17: IP Address Management Features on EX9200 Switches by Junos OS Release ..................... 41
Table 18: IPv6 Features on Switches by Junos OS Release .................. 42
Table 19: Layer 2 Network Protocols Features on Switches by Junos OS Release ...................... 45
Table 20: Layer 2 Networking Features on EX9200 Switches by Junos OS Release ...................... 46
Table 21: Layer 3 Protocols Features on Switches by Junos OS Release ...................... 48
Table 22: Layer 3 Protocols Features on EX9200 Switches by Junos OS Release ...................... 50
Table 23: Logical Systems Features on EX9200 Switches by Junos OS Release ........................................ 53
Table 24: MPLS Features on Switches by Junos OS Release ................................................................. 53
Table 25: MPLS Features on EX9200 Switches by Junos OS Release .............................................. 56
Table 26: Multicast Features on Switches by Junos OS Release ........................................................... 58
Table 27: Multicast Features on EX9200 Switches by Junos OS Release ........................................... 59
Table 28: Network Management and Monitoring Features on Switches by Junos OS Release ............ 61
Table 29: Network Management and Monitoring Features on EX9200 Switches by Junos OS Release .................................................................................................................. 63
Table 30: Port Security Features on Switches by Junos OS Release ..................................................... 64
Table 31: Power over Ethernet (PoE) Features on Switches by Junos OS Release ................................. 66
Table 32: Routing Policy and Packet Filtering Features on Switches by Junos OS Release ................. 67
Table 33: Routing Policy and Firewall Filters on EX9200 Switches by Junos OS Release .................. 67
Table 34: Spanning-Tree Protocols Features on Switches by Junos OS Release ................................. 69
Table 35: Spanning-Tree Protocols Features on EX9200 Switches by Junos OS Release .................... 70
Table 36: System Management Features on Switches by Junos OS Release ........................................ 71
Table 37: System Management Features on EX9200 Switches by Junos OS Release ............................ 71
Table 38: User Interface and Configuration Features on EX9200 Switches by Junos OS Release ........ 72
Table 39: VPN Features on EX9200 Switches by Junos OS Release ..................................................... 72
Table 40: First Junos OS Release for Each EX Series Virtual Chassis ................................................... 76
Table 41: Access Control Features by Junos OS Release .......................................................................... 76
Table 42: Administration Features by Junos OS Release ........................................................................ 76
Table 43: Class-of-Service (CoS) Features by Junos OS Release ............................................................. 78
Table 44: Converged Networks (LAN and SAN) Features by Junos OS Release ................................. 78
Table 45: Device Security Features by Junos OS Release ........................................................................ 80
Table 46: High Availability and Resiliency Features by Junos OS Release ........................................... 80
Table 47: Interfaces Features by Junos OS Release ................................................................................... 81
Table 48: IP Address Management Features by Junos OS Release ......................................................... 83
Table 49: IPv6 Features by Junos OS Release ........................................................................................... 85
Table 50: Layer 2 Network Protocols Features by Junos OS Release ..................................................... 87
Table 51: Layer 3 Protocols Features by Junos OS Release ..................................................................... 89
Table 52: MPLS Features by Junos OS Release ....................................................................................... 91
Table 53: Multicast Features by Junos OS Release .................................................................................. 95
Table 54: Network Management and Monitoring Features by Junos OS Release ............................... 95
Table 55: Port Security Features by Junos OS Release .......................................................................... 96
Table 56: Power over Ethernet (PoE) Features by Junos OS Release ................................................... 99
Table 57: Routing Policy and Packet Filtering Features by Junos OS Release ....................................... 100
Table 58: Spanning-Tree Protocols Features by Junos OS Release ....................................................... 101
Table 59: System Management Features by Junos OS Release ............................................................... 103
List of Tables

Table 60: Virtual Chassis Features ...................................................... 104

Part 3  System Setup

Chapter 3  Overview ........................................................................... 111
Table 61: Junos OS Processes ............................................................... 112

Chapter 4  Configuration ................................................................. 115
Table 62: Date and Time Settings ......................................................... 117
Table 63: System Identity Configuration Summary ................................. 118
Table 64: Menu Options of the LCD Menus Supported on the Switches ....... 141

Chapter 5  Administration ................................................................. 159
Table 65: request system storage cleanup Output Fields ....................... 205
Table 66: show chassis fan Output Fields .............................................. 229
Table 67: show chassis firmware Output Fields .................................... 242
Table 68: show chassis lcd Output Fields ............................................. 253
Table 69: show ntp associations Output Fields ...................................... 268
Table 70: show ntp status Output Fields .............................................. 270
Table 71: show system firmware Output Fields ..................................... 273
Table 72: show system storage Output Fields ........................................ 288
Table 73: show system switchover Output Fields ................................... 294
Table 74: show system uptime Output Fields ....................................... 298
Table 75: show system users Output Fields ......................................... 303
Table 76: show system virtual-memory Output Fields ........................... 308
Table 77: show system users Output Fields ............................. 303
Table 78: show system virtual-memory Output Fields ........................... 308
Table 79: show system users Output Fields ............................. 303
Table 77: show system virtual-memory Output Fields ........................... 308

Part 4  User Interfaces

Chapter 7  Overview ........................................................................... 385
Table 78: Junos OS Processes ............................................................... 386
Table 79: J-Web Interface .................................................................... 390
Table 80: Switching Platform Configuration Interfaces ............................ 393

Part 5  Access and User Management

Chapter 10  Overview ........................................................................ 411
Table 81: Junos OS Processes ............................................................... 412

Chapter 11  Configuration ................................................................. 415
Table 82: Secure Management Access Configuration Summary ............... 416

Chapter 12  Administration ............................................................... 463
Table 83: User Management Configuration Page Summary ...................... 464
Table 84: Add an Authentication Server .............................................. 465
Table 85: show subscribers Output Fields ........................................... 470

Part 6  Configuration and File Management

Chapter 14  Overview ........................................................................ 491
Table 86: Junos OS Processes ............................................................... 492
Table 87: J-Web Edit Point & Click Configuration Links .......................... 495
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 15</td>
<td>Configuration</td>
<td>501</td>
</tr>
<tr>
<td></td>
<td>Table 88: J-Web Edit Point &amp; Click Configuration Icons</td>
<td>495</td>
</tr>
<tr>
<td></td>
<td>Table 89: J-Web Edit Point &amp; Click Configuration Buttons</td>
<td>496</td>
</tr>
<tr>
<td></td>
<td>Table 90: Configuration File Terms</td>
<td>499</td>
</tr>
<tr>
<td></td>
<td>Table 91: Options for the load command</td>
<td>502</td>
</tr>
<tr>
<td></td>
<td>Table 92: Commit Options</td>
<td>512</td>
</tr>
<tr>
<td></td>
<td>Table 93: Commit Preference Options</td>
<td>512</td>
</tr>
<tr>
<td>Chapter 16</td>
<td>Administration</td>
<td>523</td>
</tr>
<tr>
<td></td>
<td>Table 94: J-Web Configuration History Summary</td>
<td>524</td>
</tr>
<tr>
<td></td>
<td>Table 95: J-Web Configuration Database Information Summary</td>
<td>524</td>
</tr>
<tr>
<td></td>
<td>Table 96: show system commit Database Information Summary</td>
<td>557</td>
</tr>
<tr>
<td>Part 7</td>
<td>Software Installation</td>
<td></td>
</tr>
<tr>
<td>Chapter 18</td>
<td>Overview</td>
<td>571</td>
</tr>
<tr>
<td></td>
<td>Table 97: Resilient Dual-Root Partition Scheme</td>
<td>575</td>
</tr>
<tr>
<td></td>
<td>Table 98: Earlier Partition Scheme</td>
<td>577</td>
</tr>
<tr>
<td></td>
<td>Table 99: Junos OS Processes</td>
<td>580</td>
</tr>
<tr>
<td></td>
<td>Table 100: Junos OS EFL Part Number on EX2200 Switches</td>
<td>582</td>
</tr>
<tr>
<td></td>
<td>Table 101: Junos OS EFL Part Number on EX3300 Switches</td>
<td>583</td>
</tr>
<tr>
<td></td>
<td>Table 102: Junos OS AFL Part Number on EX3300 Switches</td>
<td>584</td>
</tr>
<tr>
<td></td>
<td>Table 103: Junos OS AFL Part Number on EX4300 Switches</td>
<td>584</td>
</tr>
<tr>
<td></td>
<td>Table 104: Junos OS AFL Part Number on EX4300 Switches</td>
<td>585</td>
</tr>
<tr>
<td></td>
<td>Table 105: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches</td>
<td>586</td>
</tr>
<tr>
<td>Chapter 20</td>
<td>Administration</td>
<td>597</td>
</tr>
<tr>
<td></td>
<td>Table 106: show system auto-snapshot status Output Fields</td>
<td>640</td>
</tr>
<tr>
<td></td>
<td>Table 107: show system license Output Fields</td>
<td>649</td>
</tr>
<tr>
<td></td>
<td>Table 108: show system snapshot Output Fields</td>
<td>653</td>
</tr>
<tr>
<td></td>
<td>Table 109: show system storage partitions Output Fields</td>
<td>655</td>
</tr>
<tr>
<td>Chapter 21</td>
<td>Troubleshooting Procedures</td>
<td>657</td>
</tr>
<tr>
<td></td>
<td>Table 110: Actions If Corrupt Files Are Found and Automatic Snapshot is Enabled</td>
<td>662</td>
</tr>
<tr>
<td></td>
<td>Table 111: Actions If Corrupt Files Are Found</td>
<td>662</td>
</tr>
<tr>
<td>Part 8</td>
<td>System Monitoring</td>
<td></td>
</tr>
<tr>
<td>Chapter 22</td>
<td>Overview</td>
<td>667</td>
</tr>
<tr>
<td></td>
<td>Table 112: Junos OS Processes</td>
<td>668</td>
</tr>
<tr>
<td></td>
<td>Table 113: Alarm Terms</td>
<td>669</td>
</tr>
<tr>
<td></td>
<td>Table 114: System Information</td>
<td>671</td>
</tr>
<tr>
<td></td>
<td>Table 115: Health Status</td>
<td>673</td>
</tr>
<tr>
<td></td>
<td>Table 116: Capacity Utilization</td>
<td>675</td>
</tr>
<tr>
<td></td>
<td>Table 117: Chassis Viewer for EX2200 Switches</td>
<td>676</td>
</tr>
<tr>
<td></td>
<td>Table 118: Chassis Viewer for EX2200-C Switches</td>
<td>676</td>
</tr>
<tr>
<td></td>
<td>Table 119: Chassis Viewer for EX3200, EX3300, and EX4200 Switches</td>
<td>677</td>
</tr>
<tr>
<td></td>
<td>Table 120: Chassis Viewer for EX4300 Switches</td>
<td>678</td>
</tr>
</tbody>
</table>
Chapter 24: Administration .................................................. 705
Table 128: Filtering System Log Messages ......................... 706
Table 129: Viewing System Log Messages ......................... 707
Table 130: Summary of Key Alarm Output Fields ............... 708
Table 131: Chassis Alarms for EX8200 Switches ............... 709
Table 132: Packet Capture Field Summary ....................... 712
Table 133: Summary of Key System Properties Output Fields 714
Table 134: Summary of the Key Output Fields for Chassis Information 716
Table 135: Summary of System Process Information Output Fields 718
Table 136: monitor list Output Fields ......................... 740
Table 137: monitor start Output Fields ......................... 741
Table 138: show chassis alarms Output Fields ............... 764
Table 139: show chassis environment Output Fields ....... 776
Table 140: show chassis environment cb Output Fields .... 826
Table 141: show chassis environment fpc Output Fields .... 845
Table 142: show chassis environment routing-engine Output Fields 869
Table 143: show chassis ethernet-switch Output Fields ...... 875
Table 144: show chassis fabric fpcs Output Fields .......... 918
Table 145: show chassis fabric map Output Fields .......... 954
Table 146: show chassis fabric plane Output Fields .......... 962
Table 147: show chassis fabric plane-location Output Fields 1003
Table 148: show chassis fabric summary Output Fields ...... 1006
Table 149: show chassis fabric fpc Output Fields .......... 1018
Table 150: show chassis led Output Fields .................... 1043
Table 151: show chassis location Output Fields ........... 1054
Table 152: show chassis pic Output Fields .................... 1059
Table 153: show chassis routing-engine Output Fields ..... 1072
Table 154: show system buffers Output Fields ............... 1120
Table 155: show system connections Output Fields .......... 1126
Table 156: show system core-dumps Output Fields .......... 1145
Table 157: show system directory-usage Output Fields ...... 1157
Table 158: show system processes Output Fields ........... 1166

Part 9: System Services

Chapter 25: Overview ...................................................... 1189
Table 159: Junos OS Processes ........................................ 1190
Table 160: Information in Authentication Grant ................ 1194
Table 161: RADIUS Attributes and VSAs for DHCPv6 Local Server 1196
Table 162: Action Taken for Events That Occur During a Reconfiguration 1203
Table 163: Unsupported Opaque DHCP Options ............... 1213
Chapter 26  Configuration ................................................... 1229
Table 164: DHCP Service Configuration Pages Summary ..................... 1241
Table 165: DHCP Service Configuration Pages Summary for EX4300 Switches ................................................... 1244
Table 166: DHCP Client Settings ........................................... 1249
Table 167: ARP Table in Trusted Environment ................................ 1263
Table 168: ARP Table in Distrusted Environment ................................ 1263
Table 169: Actions for DHCP Local Server Snooped Packets ............... 1275
Table 170: ARP Table in Trusted Environment ................................ 1289
Table 171: ARP Table in Distrusted Environment ................................ 1290
Table 172: DHCP Relay Agent Option 82 Value for Auto Logout ............ 1292
Table 173: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled ................................................... 1299
Table 174: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled ................................................... 1300
Table 175: Actions for Snooped BOOTREPLY Packets ...................... 1300
Table 176: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches ................................................... 1391
Table 177: Protocol Families and Supported Interface Types .................. 1484
Chapter 27  Administration ................................................... 1527
Table 178: Summary of DHCP Output Fields ................................... 1528
Table 179: Summary of DHCP Output Fields for EX4300 Switches .......... 1530
Table 180: Summary of the DHCP Statistics Information Output for EX4300 Switches ................................................... 1531
Table 181: show dhcp server binding Output Fields ............................ 1552
Table 182: show dhcp server statistics Output Fields .......................... 1557
Table 183: show dhcpv6 server binding Output Fields ........................ 1560
Table 184: show dhcpv6 server statistics Output Fields ........................ 1566
Table 185: clear dhcp relay statistics Output Fields ............................ 1571
Table 186: show dhcp relay binding Output Fields ............................. 1579
Table 187: show dhcp relay statistics Output Fields ............................ 1584
Table 188: show dhcpv6 relay binding Output Fields .......................... 1587
Table 189: show dhcpv6 relay statistics Output Fields ........................ 1591
Table 190: show route extensive Output Fields .................................. 1594
Table 191: show security pki local-certificate Output Fields .................. 1633
Table 192: show system services dhcp binding Output Fields ................. 1636
Table 193: show system services dhcp conflict Output Fields ................. 1639
Table 194: show system services dhcp global Output Fields ................. 1640
Table 195: show system services dhcp pool Output Fields .................... 1642
Table 196: show system services dhcp statistics Output Fields ............... 1644
Table 197: show system services service-deployment Output Fields ........ 1647

Part 10  Access Control

Chapter 29  Configuration ................................................... 1675
Table 198: Components of the Topology ....................................... 1677
Table 199: Components of the Guest VLAN Topology ......................... 1681
Table 200: Components of the Supplicant Mode Configuration Topology . . . 1686
Table 201: Components of the VoIP Configuration Topology ........................................ 1692
Table 202: Components of the Static MAC Authentication Configuration
  Topology ........................................................................... 1705
Table 203: Components of the Topology ............................................ 1709
Table 204: Components of the MAC RADIUS Authentication Configuration
  Topology ........................................................................... 1715
Table 205: Components of the Firewall Filter and RADIUS Server Attributes
  Topology ........................................................................... 1721
Table 206: Components of the OAC Deployment .............................. 1737
Table 207: Match Conditions ...................................................... 1750
Table 208: Actions for VSAs ...................................................... 1751
Table 209: Configurable Elements of a Captive Portal Login Page .......... 1759
Table 210: Unsupported [edit access] Configuration Statements on EX Series
  Switches ........................................................................... 1767
Chapter 30 Administration ........................................................ 1813
Table 211: clear captive-portal interface Output Fields ...................... 1816
Table 212: show captive-portal authentication-failed-users Output Fields . 1822
Table 213: show captive-portal interface Output Fields ...................... 1825
Table 214: show dot1x Output Fields ........................................... 1828
Table 215: show dot1x authentication-failed-users Output Fields .......... 1833
Table 216: show dot1x static-mac-address Output Fields .................... 1835
Table 217: show lldp Output Fields .............................................. 1838
Table 218: show lldp local-information Output Fields ....................... 1842
Table 219: show lldp neighbors Output Fields .................................. 1844
Table 220: show lldp remote-global-statistics Output Fields ............... 1851
Table 221: show lldp statistics Output Fields ................................... 1853
Table 222: show network-access aaa statistics accounting Output Fields ... 1855
Table 223: show network-access aaa statistics authentication Output Fields ... 1856
Table 224: show network-access aaa statistics dynamic-requests Output Fields .................. 1858
Part 11 Class of Service
Chapter 31 Overview .................................................................. 1861
Table 225: Default Code-Point Aliases .......................................... 1866
Table 226: Default BA Classification ............................................ 1870
Table 227: Allowed BA Classification .......................................... 1870
Table 228: Default Forwarding Classes for Unicast Traffic ................. 1873
Table 229: Default Forwarding Classes for Multicast Traffic ............... 1873
Table 230: Support for Scheduler Maps on Switches and Line Cards .......... 1883
Table 231: Default Packet Header Rewrite Mappings .......................... 1889
Table 232: EX8200 Line Cards That Include Oversubscribed Ports ........ 1892
Chapter 32 Configuration .......................................................... 1895
Table 233: Configuration Components: VLANs ............................ 1897
Table 234: Configuration Components: Switch Ports on a 48-Port All-PoE
  Switch ............................................................................... 1897
Table 235: CoS Value Aliases Configuration Fields .......................... 1922
Table 236: BA-classifier Loss Priority Assignments ............................ 1923
Part 17  IS-IS

Chapter 51  Overview

Table 336: Supported Junos OS Layer 3 Protocol Statements and Features 2689
Table 337: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported 2690

Chapter 52  Configuration

Table 338: Default Metric Values for Routes Exported into IS-IS 2725

Chapter 53  Administration

Table 339: show isis adjacency Output Fields 2760
Table 340: show isis authentication Output Fields 2764
Table 341: show isis backup coverage Output Fields 2766
Table 342: show isis backup label-switched-path Output Fields 2768
Table 343: show isis backup spf results Output Fields 2771
Table 344: show isis database Output Fields 2775
Table 345: show isis hostname Output Fields 2781
Table 346: show isis interface Output Fields 2783
Table 347: show isis overview Output Fields 2786
Table 348: show isis route Output Fields 2789
Table 349: show isis spf Output Fields 2793
Table 350: show isis statistics Output Fields 2799

Part 18  OSPF

Chapter 54  Overview

Table 351: Supported Junos OS Layer 3 Protocol Statements and Features 2803
Table 352: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported 2804

Chapter 55  Configuration

Table 353: OSPF Routing Configuration Summary 2812
Table 354: Edit OSPF Global Settings 2813

Chapter 56  Administration

Table 355: Summary of Key OSPF Routing Output Fields 2881
Table 356: show (ospf | ospf3) interface Output Fields 2894
Table 357: show (ospf | ospf3) iostatistics Output Fields 2899
Table 358: show (ospf | ospf3) log Output Fields 2901
Table 359: show (ospf | ospf3) neighbor Output Fields 2905
Table 360: show ospf overview Output Fields 2910
Table 361: show (ospf | ospf3) route Output Fields 2916
Table 362: show (ospf | ospf3) statistics Output Fields 2921
Table 363: show ospf database Output Fields 2926
Table 364: show ospf3 database Output Fields ........................................ 2934

**Part 19**

**Chapter 57**

**Overview** ................................................................. 2947

Table 365: Supported Junos OS Layer 3 Protocol Statements and Features ... 2947
Table 366: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported .............................................................. 2948

**Chapter 58**

**Configuration** ............................................................ 2951

Table 367: RIP Routing Configuration Summary ................................ 2952
Table 368: Edit RIP Global Settings ........................................ 2952

**Chapter 59**

**Administration** ............................................................ 2997

Table 369: Summary of Key RIP Routing Output Fields .................... 2997
Table 370: show rip general-statistics Output Fields ..................... 3001
Table 371: show rip neighbor Output Fields ................................ 3003
Table 372: show rip statistics Output Fields ............................... 3006
Table 373: show ripng general-statistics Output Fields ................. 3010
Table 374: show ripng neighbor Output Fields ............................ 3011
Table 375: show ripng statistics Output Fields ............................ 3013

**Part 20**

**Chapter 60**

**Overview** ................................................................. 3017

Table 376: Supported Junos OS Layer 3 Protocol Statements and Features ... 3017
Table 377: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported .............................................................. 3018

**Chapter 61**

**Configuration** ............................................................ 3023

Table 378: Static Routing Configuration Summary ......................... 3025

**Chapter 62**

**Administration** ............................................................ 3133

Table 379: Filtering Route Messages ...................................... 3133
Table 380: Summary of Key Routing Information Output Fields .......... 3134
Table 381: show as-path Output Fields .................................... 3137
Table 382: show as-path domain Output Fields ........................... 3141
Table 383: show as-path summary Output Fields ......................... 3143
Table 384: show ipv6 neighbors Output Fields ............................ 3145
Table 385: show route Output Fields ..................................... 3148
Table 386: show route damping Output Fields ............................ 3170
Table 387: show route detail Output Fields ............................... 3175
Table 388: Next-hop Types Output Field Values ........................... 3179
Table 389: State Output Field Values ..................................... 3181
Table 390: Communities Output Field Values ............................. 3183
Table 391: show route export Output Fields .............................. 3193
Table 392: show route extensive Output Fields .......................... 3196
Table 393: show route flow validation Output Fields .................... 3212
Table 394: show route instance Output Fields ............................ 3219
Table 395: show route martians Output Fields ............................ 3230
Table 396: show route receive-protocol Output Fields .................. 3257
Table 397: show route resolution Output Fields .......................... 3266
Table 398: show route summary Output Fields .......................... 3282
Table 399: show route terse Output Fields .............................. 3299

Part 21 Multicast

Chapter 64 Configuration .................................................. 3315
Table 400: IGMP Snooping Configuration Fields ....................... 3324
Table 401: Supported Tracing Operations for IGMP Snooping .......... 3325

Chapter 65 Administration ................................................. 3407
Table 402: Summary of IGMP Snooping Output Fields ................. 3408
Table 403: mtrace Output Fields ........................................ 3410
Table 404: mtrace from-source Output Fields ......................... 3435
Table 405: mtrace monitor Output Fields .............................. 3437
Table 406: mtrace to-gateway Output Fields ......................... 3440
Table 407: show igmp group Output Fields ............................ 3442
Table 408: show igmp interface Output Fields ......................... 3446
Table 409: show igmp statistics Output Fields ....................... 3450
Table 410: show igmp-snooping membership Output Fields ......... 3453
Table 411: show igmp-snooping route Output Fields ................. 3456
Table 412: show igmp-snooping statistics Output Fields ............ 3458
Table 413: show multicast flow-map Output Fields .................. 3460
Table 414: show multicast interface Output Fields .................. 3462
Table 415: show multicast mrinfo Output Fields ..................... 3464
Table 416: show multicast next-hops Output Fields ................. 3467
Table 417: show multicast pim-to-igmp-proxy Output Fields ....... 3469
Table 418: show multicast pim-to-mld-proxy Output Fields ......... 3471
Table 419: show multicast route Output Fields ....................... 3474
Table 420: show multicast rpf Output Fields .......................... 3480
Table 421: show multicast scope Output Fields ...................... 3483
Table 422: show multicast sessions Output Fields ................. 3485
Table 423: show multicast usage Output Fields ...................... 3488
Table 424: show pim bootstrap Output Fields ......................... 3491
Table 425: show pim interfaces Output Fields ....................... 3493
Table 426: show pim join Output Fields ............................... 3497
Table 427: show pim neighbors Output Fields ....................... 3511
Table 428: show pim rps Output Fields ................................ 3515
Table 429: show pim source Output Fields ............................ 3522
Table 430: show pim statistics Output Fields ......................... 3525

Part 22 Network Management and Monitoring

Chapter 66 Overview .......................................................... 3539
Table 431: Mirroring Terminologies ..................................... 3545
Table 432: Configuration Guidelines for Port Mirroring and Analyzers on EX4300 Switches ........................................ 3547

Chapter 67 Configuration .................................................. 3559
Table 433: SNMP Configuration Page ................................. 3594
Table 434: Port Mirroring Configuration Settings ................................................. 3602
Table 435: RPM Probe Owner, Concurrent Probes, and Probe Servers
  Configuration Fields .................................................................................. 3606
Table 436: Performance Probe Tests Configuration Fields .......................... 3607
Table 437: Unsupported [edit snmp] Configuration Statements on EX Series
  Switches ..................................................................................... 3629

Administration ....................................................................................... 3783
Table 438: J-Web Ping Host Field Summary ............................................. 3784
Table 439: Traceroute field summary ......................................................... 3786
Table 440: Match Conditions for the monitor traffic Command .............. 3792
Table 441: Logical Operators for the monitor traffic Command .............. 3793
Table 442: Arithmetic and Relational Operators for the monitor traffic
  Command .................................................................................. 3795
Table 443: show pfe statistics bridge Output Fields ................................. 3804
Table 444: traceroute Output Fields .......................................................... 3811
Table 445: show services rpm active-servers Output Fields ................... 3813
Table 446: show services rpm history-results Output Fields .................. 3814
Table 447: show services rpm probe-results Output Fields .................... 3817
Table 448: show snmp health-monitor Output Fields ............................... 3832
Table 449: show snmp inform-statistics Output Fields .............................. 3839
Table 450: show snmp mib Output Fields .................................................. 3842
Table 451: show snmp rmon Output Fields .............................................. 3844
Table 452: show snmp rmon history Output Fields ................................. 3848
Table 453: show snmp statistics Fields ..................................................... 3852
Table 454: show snmp v3 Output Fields .................................................... 3857
Table 455: show forwarding-options port-mirroring Output Fields ......... 3859
Table 456: show forwarding-options analyzer Output Fields ................. 3861
Table 457: show sflow Output Fields ...................................................... 3863
Table 458: show sflow interface Output Fields ........................................ 3865
Table 459: show sflow collector Output Fields ....................................... 3867
Table 460: monitor ethernet delay-measurement one-way Output Fields . 3875
Table 461: monitor ethernet delay-measurement two-way Output Fields ... 3875
Table 462: show oam ethernet connectivity-fault-management delay-statistics
  and mep-statistics Output Fields ......................................................... 3879
Table 463: show oam ethernet connectivity-fault-management forwarding-state
  Output Fields .................................................................................. 3882
Table 464: show oam ethernet connectivity-fault-management interfaces
  Output Fields .................................................................................. 3886
Table 465: show oam ethernet connectivity-fault-management linktrace
  path-database Output Fields .............................................................. 3892
Table 466: show oam ethernet connectivity-fault-management mep-database
  Output Fields .................................................................................. 3895
Table 467: show oam ethernet connectivity-fault-management mip Output
  Fields ........................................................................................... 3901
Table 468: show oam ethernet connectivity-fault-management
  sla-iterator-statistics Output Fields .................................................... 3902
Table 469: show oam ethernet link-fault-management Output Fields ....... 3907
Table 470: show uplink-failure-detection Output Fields ......................... 3912
Part 26  Spanning-Tree Protocols

Chapter 81  Overview ...................................................... 4297
Table 534: Selecting a Spanning-Tree Protocol ........................................... 4299
Table 535: Selecting a Spanning-Tree Protocol ................................................ 4303
Table 536: Selecting a Spanning-Tree Protocol ................................................ 4305
Table 537: Selecting a Spanning-Tree Protocol ................................................ 4307

Chapter 82  Configuration ................................................... 4313
Table 538: Components of the Topology for Configuring RSTP ................................................... 4315
Table 539: Components of the Topology for Configuring MSTP on EX Series Switches ................................................... 4332
Table 540: Components of the Topology for Configuring BPDU Protection on EX Series Switches ................................................... 4354
Table 541: Components of the Topology for Configuring BPDU Protection on EX Series Switches ................................................... 4359
Table 542: Components of the Topology for Configuring Loop Protection on EX Series Switches ................................................... 4364
Table 543: Components of the Topology for Configuring Root Protection on EX Series Switches ................................................... 4369
Table 544: Spanning-Tree Protocol Configuration Parameters ................................................... 4374

Chapter 83  Administration .................................................. 4421
Table 545: Summary of Spanning-Tree Protocols Output Fields ................................................... 4421
Table 546: show spanning-tree bridge Output Fields ................................................... 4428
Table 547: show spanning-tree bridge Output Fields ................................................... 4433
Table 548: show spanning-tree interface Output Fields ................................................... 4439
Table 549: show spanning-tree interface Output Fields ................................................... 4442
Table 550: show spanning-tree mstp configuration Output Fields ................................................... 4448
Table 551: show spanning-tree mstp configuration Output Fields ................................................... 4450
Table 552: show spanning-tree statistics Output Fields ................................................... 4452
Table 553: show spanning-tree statistics Output Fields ................................................... 4454

Part 27  Virtual Chassis

Chapter 84  Overview ...................................................... 4459
Table 554: Maximum Member Switch Support for Virtual Chassis by Junos OS Release ................................................... 4461
Table 555: Maximum Member Links in LAGs Over Optical Interface VCPs . . . . . . . . . . 4473
Table 556: Automatic Software Update Support ................................................... 4481
Table 557: Effects of a Routing Engine Switchover ................................................... 4484

Chapter 86  Administration .................................................. 4529
Table 558: Commands That Can be Run on All or Specific Members of the Virtual Chassis Configuration ................................................... 4530
Table 559: show system uptime Output Fields ................................................... 4549
Table 560: show virtual-chassis active-topology Output Fields ................................................... 4551
Table 561: show virtual-chassis device-topology Output Fields ................................................... 4554
Table 562: show virtual-chassis protocol adjacency Output Fields ................................................... 4558
Table 563: show virtual-chassis protocol database Output Fields ................................................... 4562
Table 564: show virtual-chassis protocol interface Output Fields ................................................... 4566
Table 565: show virtual-chassis protocol route Output Fields ............... 4568
Table 566: show virtual-chassis protocol statistics Output Fields .......... 4571
Table 567: show virtual-chassis Output Fields ............................. 4574
Table 568: show virtual-chassis vc-path Output Fields ...................... 4577
Table 569: show virtual-chassis vc-port Output Fields ..................... 4579
Table 570: show virtual-chassis vc-port diagnostics optics Output Fields . 4584
Table 571: show virtual-chassis vc-port statistics Output Fields .......... 4598
About the Documentation

- Documentation and Release Notes on page xcv
- Supported Platforms on page xcv
- Using the Examples in This Manual on page xcv
- Documentation Conventions on page xcvii
- Documentation Feedback on page xcviii
- Requesting Technical Support on page xcix

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- EX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the `load merge` or the `load merge relative` command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a full example. In this case, use the `load merge` command.
If the example configuration does not start at the top level of the hierarchy, the example is a snippet. In this case, use the load merge relative command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file ex-script.conf. Copy the ex-script.conf file to the /var/tmp directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the load merge configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file ex-script-snippet.conf. Copy the ex-script-snippet.conf file to the /var/tmp directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:
3. Merge the contents of the file into your routing platform configuration by issuing the `load merge relative` configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the `load` command, see the *CLI User Guide*.

**Documentation Conventions**

*Table 1 on page xcvii* defines notice icons used in this guide.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![i]</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![!]</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>![!]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>![!]</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>

*Table 2 on page xcvii* defines the text and syntax conventions used in this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the <code>configure</code> command: <code>user@host&gt; configure</code></td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td><code>user@host&gt; show chassis alarms</code>&lt;br&gt;<code>No alarms currently active</code></td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td></td>
<td>• A policy term is a named structure that defines match conditions and actions.&lt;br&gt;• <em>Junos OS CLI User Guide</em>&lt;br&gt;• RFC 1997, <em>BGP Communities Attribute</em></td>
</tr>
</tbody>
</table>
### Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italic text like this</em></td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine's domain name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[edit]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root@# set system domain-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>domain-name</td>
</tr>
<tr>
<td><strong>Text like this</strong></td>
<td>Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.</td>
<td>• To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The console port is labeled CONSOLE.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code> (angle brackets)</td>
<td>Enclose optional keywords or variables.</td>
<td>stub &lt;default-metric metric&gt;;</td>
</tr>
<tr>
<td></td>
<td>(pipe symbol)</td>
<td>Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(string1</td>
</tr>
<tr>
<td><code>#</code> (pound sign)</td>
<td>Indicates a comment specified on the same line as the configuration statement to which it applies.</td>
<td>rsvp [ # Required for dynamic MPLS only</td>
</tr>
<tr>
<td><code>[ ]</code> (square brackets)</td>
<td>Enclose a variable for which you can substitute one or more values.</td>
<td>community name members [community-ids]</td>
</tr>
<tr>
<td>Indention and braces ({ })</td>
<td>Identify a level in the configuration hierarchy.</td>
<td>[edit]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>routing-options { static { route default { nexthop address; retain; } } }</td>
</tr>
<tr>
<td><code>:</code> (semicolon)</td>
<td>Identifies a leaf statement at a configuration hierarchy level.</td>
<td></td>
</tr>
<tr>
<td><strong>GUI Conventions</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Bold text like this</em></td>
<td>Represents graphical user interface (GUI) items you click or select.</td>
<td>• In the Logical Interfaces box, select All Interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To cancel the configuration, click Cancel.</td>
</tr>
<tr>
<td>&gt; (bold right angle bracket)</td>
<td>Separates levels in a hierarchy of menu selections.</td>
<td>In the configuration editor hierarchy, select Protocols&gt;Ospf.</td>
</tr>
</tbody>
</table>

### Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at
https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

### Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/
Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.
PART 1

Getting Started with ELS

• Getting Started with ELS on page 3
CHAPTER 1

Getting Started with ELS

- Getting Started on page 3

Getting Started

- Getting Started with Enhanced Layer 2 Software on page 3
- Enhanced Layer 2 CLI Configuration Statement and Command Changes on page 15

Getting Started with Enhanced Layer 2 Software

- Using the ELS Translator Tool on page 3
- Configuring a VLAN on page 4
- Configuring the Native VLAN Identifier on page 4
- Configuring Layer 2 Interfaces on page 4
- Configuring Layer 3 Interfaces on page 5
- Configuring an IRB Interface on page 5
- Configuring an Aggregated Ethernet Interface and Configuring LACP on That Interface on page 6
- Enhanced Layer 2 CLI Configuration Statement and Command Changes on page 7

Using the ELS Translator Tool

The ELS Translator is a web-based tool that converts Junos OS Layer 2 configurations to Enhanced Layer 2 Software (ELS) configurations used in Junos OS Release 12.3R2 and later. This conversion tool supports all Juniper Networks EX Series and MX Series platforms with ELS installed. The ELS Translator is hosted on Juniper’s Customer Support website for EX Series switches and MX Series Universal Edge routers, and is available to registered users, internal users, partners, and premium service contract customers. You need to login using your Juniper Networks user name and password to access the ELS Translator tool.

NOTE: It is possible a script might not translate correctly, so review translated scripts carefully before loading the converted configuration on your switch or other device.

Copyright © 2013, Juniper Networks, Inc.
Click to access the ELS translator tool.

**Configuring a VLAN**

You can configure one or more VLANs to perform Layer 2 bridging. The Layer 2 bridging functions include integrated routing and bridging (IRB) for support for Layer 2 bridging and Layer 3 IP routing on the same interface. EX Series switches can function as Layer 2 switches, each with multiple bridging, or broadcast, domains that participate in the same Layer 2 network. You can also configure Layer 3 routing support for a VLAN.

To configure a VLAN:

1. Create the VLAN by setting the unique VLAN name and configuring the VLAN ID:
   ```
   [edit]
   user@host# set vlans vlan-name vlan-id vlan-id-number
   ```
2. Assign at least one interface to the VLAN:
   ```
   [edit]
   user@host# set interface interface-name family ethernet-switching vlan members vlan-name
   ```

**Configuring the Native VLAN Identifier**

EX Series switches support receiving and forwarding routed or bridged Ethernet frames with 802.1Q VLAN tags. Typically, trunk ports, which connect switches to each other, accept untagged control packets but do not accept untagged data packets. You can enable a trunk port to accept untagged data packets by configuring a native VLAN ID on the interface on which you want the untagged data packets to be received.

To configure the native VLAN ID:

1. On the interface on which you want untagged data packets to be received, set the interface mode to trunk, which specifies that the interface is in multiple VLANs and can multiplex traffic between different VLANs.
   ```
   [edit interfaces]
   user@host# set interface-name unit logical-unit-number family ethernet-switching interface-mode trunk
   ```
2. Configure the native VLAN ID:
   ```
   [edit interfaces]
   user@host# set interface-name native-vlan-id number
   ```
3. Assign the interface to the native VLAN ID:
   ```
   [edit interfaces]
   user@host# set interface-name unit logical-unit-number family ethernet-switching vlan members native-vlan-id-number
   ```

**Configuring Layer 2 Interfaces**

To ensure that your high-traffic network is tuned for optimal performance, explicitly configure some settings on the switch’s network interfaces.

To configure a Gigabit Ethernet interface or 10-Gigabit Ethernet interface for trunk interface mode:

```
To configure a Gigabit Ethernet interface or 10-Gigabit Ethernet interface for access interface mode:

```
[edit]
user@host# set interfaces interface-name unit logical-unit-number family ethernet-switching interface-mode trunk
```

Configuring Layer 3 Interfaces

To configure a Layer 3 interface, you must assign an IP address to the interface. You assign an address to an interface by specifying the address when configuring the protocol family. For the inet or inet6 family, configure the interface IP address.

You can configure interfaces with a 32-bit IP version 4 (IPv4) address and optionally with a destination prefix, sometimes called a subnet mask. An IPv4 address utilizes a 4-octet dotted decimal address syntax (for example, 192.168.1.1). An IPv4 address with destination prefix utilizes a 4-octet dotted decimal address syntax with a destination prefix appended (for example, 192.168.1.1/30).

To specify an IP address for the logical unit using IPv4:

```
[edit]
user@host# set interfaces interface-name unit logical-unit-number family inet address ip-address
```

You represent IP version 6 (IPv6) addresses in hexadecimal notation using a colon-separated list of 16-bit values. You assign a 128-bit IPv6 address to an interface.

To specify an IP address for the logical unit using IPv6:

```
[edit]
user@host# set interfaces interface-name unit logical-unit-number family inet6 address ip-address
```

Configuring an IRB Interface

Integrated routing and bridging (IRB) provides support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route packets to another routed interface or to another VLAN that has a Layer 3 protocol configured. IRBs allow the device to recognize packets that are being sent to local addresses so that they are bridged (switched) whenever possible and are routed only when necessary. Whenever packets can be switched instead of routed, several layers of processing are eliminated. An interface named irb functions as a logical router on which you can configure a Layer 3 logical interface for VLAN. For redundancy, you can combine an IRB interface with implementations of the Virtual Router Redundancy Protocol (VRRP) in both bridging and virtual private LAN service (VPLS) environments.

To configure an IRB interface:

1. Create a Layer 2 VLAN by assigning it a name and a VLAN ID:

```
[edit]
user@host# set vlans vlan-name vlan-id vlan-id
```

2. Create an IRB logical interface:

```
[edit]
user@host# set interface irb unit logical-unit-number family inet address ip-address
```
3. Associate the IRB interface with the VLAN:

```
[edit]
user@host# set vlans vlan-name l3-interface irb.logical-unit-number
```

### Configuring an Aggregated Ethernet Interface and Configuring LACP on That Interface

Use the link aggregation feature to aggregate one or more links to form a virtual link or link aggregation group (LAG). The MAC client can treat this virtual link as if it were a single link to increase bandwidth, provide graceful degradation as failure occurs, and increase availability.

To configure an aggregated Ethernet interface:

1. Specify the number of aggregated Ethernet interfaces to be created:

```
[edit chassis]
user@host# set aggregated-devices ethernet device-count number
```

2. Specify the name of the link aggregation group interface:

```
[edit interfaces]
user@host# set interfaces ae
```

3. Specify the minimum number of links for the aggregated Ethernet interface (aex), that is, the defined bundle, to be labeled “up”:

```
[edit interfaces]
user@host# set ae x aggregated-ether-options minimum-links number
```

4. Specify the link speed for the aggregated Ethernet bundle:

```
[edit interfaces]
user@host# set ae x aggregated-ether-options link-speed link-speed
```

5. Specify the members to be included within the aggregated Ethernet bundle:

```
[edit interfaces]
user@host# set interface-name ether-options 802.3ad aex
user@host# set interface-name ether-options 802.3ad aex
```

6. Specify an interface family for the aggregated Ethernet bundle:

```
[edit interfaces]
user@host# set ae x unit 0 family inet address ip-address
```

For aggregated Ethernet interfaces on the device, you can configure the Link Aggregation Control Protocol (LACP). LACP bundles several physical interfaces to form one logical interface. You can configure aggregated Ethernet with or without LACP enabled.

When LACP is enabled, the local and remote sides of the aggregated Ethernet links exchange protocol data units (PDUs), containing information about the state of the link. You can configure Ethernet links to actively transmit PDUs, or you can configure the links to passively transmit them, sending out LACP PDUs only when they receive them from another link. One side of the link must be configured as active for the link to be up.

To configure LACP:

1. Enable one side of the aggregated Ethernet link as active:

```
[edit interfaces]
user@host# set ae x aggregated-ether-options lacp active
```

2. Specify the interval at which the interfaces send LACP packets:
Enhanced Layer 2 CLI Configuration Statement and Command Changes

The enhanced Layer 2 Command Line Interface (CLI) feature is introduced in Junos OS Release 12.3R2. The enhanced Layer 2 CLI feature changes the CLI for some Layer 2 features on EX Series switches. This enhanced CLI will be used to configure Layer 2 features on future EX Series hardware platforms, and also to configure Layer 2 features on other Juniper Networks products.

The following tables provide a list of existing commands that were moved to new hierarchies or changed on EX Series switches as part of this CLI enhancement effort. The table is provided as a high-level reference only. For detailed information about these commands, use the links to the configuration statements provided in the table or see the technical documentation.

Table 3: Enhanced Layer 2 CLI Changes

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-switching-options {</td>
<td>forwarding-options {</td>
<td>Statements moved to different hierarchy.</td>
</tr>
<tr>
<td>analyzer {</td>
<td>analyzer {</td>
<td></td>
</tr>
<tr>
<td>name {</td>
<td>name {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>switch-options {</td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td>authentication-whitelist [</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>protocols {</td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td>bpdu-block {</td>
<td>layer2-control {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>bpdu-block {</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td></td>
<td>Statements deleted.</td>
</tr>
<tr>
<td>dot1q-tunneling {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ether-type (0x8100</td>
<td>0x88a8</td>
<td>0x9100);</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>switch-options {</td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td>interfaces interface-name {</td>
<td>interfaces interface-name {</td>
<td></td>
</tr>
<tr>
<td>no-mac-learning;</td>
<td>no-mac-learning;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-switching-options {</td>
<td>--</td>
<td>Statements deleted.</td>
</tr>
<tr>
<td>mac-notification {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>notification-interval seconds;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>protocols {</td>
<td>Statement replaced with new statement and moved to different hierarchy.</td>
</tr>
<tr>
<td>mac-table-aging-time seconds;</td>
<td>l2-learning {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>global-mac-table-aging-time seconds;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>interfaces interface-name family ethernet-switching {</td>
<td>Statement replaced with a new statement.</td>
</tr>
<tr>
<td>port-error-disable {</td>
<td>recovery-timeout seconds;</td>
<td></td>
</tr>
<tr>
<td>disable-timeout timeout;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>switch-options {</td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td>redundant-trunk-group {</td>
<td>redundant-trunk-group {</td>
<td></td>
</tr>
<tr>
<td>group name {</td>
<td>group name {</td>
<td></td>
</tr>
<tr>
<td>description;</td>
<td>description;</td>
<td></td>
</tr>
<tr>
<td>interface interface-name {</td>
<td>interface interface-name {</td>
<td></td>
</tr>
<tr>
<td>primary;</td>
<td>primary;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>preempt-cutover-timer seconds;</td>
<td>preempt-cutover-timer seconds;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-switching-options { secure-access-port { interface (all</td>
<td>interface-name) { (dhcp-trusted</td>
<td>no-dhcp-trusted); static-ip ip-address { mac mac-address; vlan vlan-name; } } vlan (all</td>
</tr>
</tbody>
</table>

NOTE: The statement examine-dhcp does not exist in the changed hierarchy. Instead, DHCP snooping is enabled automatically when other DHCP security features are enabled on a VLAN. See “Configuring Port Security (CLI Procedure)” on page 4023 for additional information.

| ethernet-switching-options { secure-access-port { dhcp-snooping-file [ location local_pathname | remote_URL; timeout seconds; write-interval seconds; } } | system { processes [ dhcp-service dhcp-snooping-file local_pathname | remote_URL; write-interval interval; ] } | Statement moved to different hierarchy. |

| ethernet-switching-options { secure-access-port vlan (all | vlan-name{ mac-move-limit } | vlans vlan-name switch-options { mac-move-limit } | Statement moved to different hierarchy. |
Table 3: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
</table>
| ethernet-switching-options {  
  static {  
  vlan vlan-id {  
  mac mac-address next-hop  
  interface interface-name;  
  }  
  }  
} | vlans {  
  vlan-name {  
  switch-options {  
  interface interface-name {  
  static mac mac-address;  
  }  
  }  
  }  
} | Statement replaced with new statement and moved to different hierarchy. |
| ethernet-switching-options {  
  storm-control {  
  (...)
  }  
} | forwarding-options {  
  storm-control-profiles profile-name {  
  (...)
  }  
} | Storm control configuration is done in two steps. The first step is to create a storm control profile at the [edit forwarding-options] hierarchy, and the second step is to bind the profile to a logical interface at the [edit interfaces] hierarchy. See “Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches” on page 2019 for additional information. |
| ethernet-switching-options {  
  traceoptions {  
  file filename <files number> <no-stamp>  
  <replace> <size size> <world-readable  
  | no-world-readable>;  
  flag flag <disable>;  
  }  
} | — | Statements removed. |
| ethernet-switching-options {  
  unknown-unicast-forwarding {  
  (...)
  }  
} | switch-options on page 2027 {  
  unknown-unicast-forwarding {  
  (...)
  }  
} | Hierarchy renamed. |
Table 3: Enhanced Layer 2 CLI Changes *(continued)*

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ethernet-switching-options {</code></td>
<td><code>switch-options {</code></td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td><code>  voip</code>{</td>
<td><code>  voip</code>{</td>
<td></td>
</tr>
<tr>
<td>`      interface (all</td>
<td>[interface-name</td>
<td>`</td>
</tr>
<tr>
<td>`         access-ports</td>
<td>)<code> {</code></td>
<td>`         access-ports</td>
</tr>
<tr>
<td>`             forwarding-class (assured-forwarding</td>
<td>`</td>
<td>`             forwarding-class (assured-forwarding</td>
</tr>
<tr>
<td>`                 best-effort</td>
<td>expedited-forwarding</td>
<td>`</td>
</tr>
<tr>
<td><code>                     network-control);</code></td>
<td><code>                     network-control);</code></td>
<td></td>
</tr>
<tr>
<td><code>              vlan vlan-name;</code></td>
<td><code>              vlan vlan-name;</code></td>
<td></td>
</tr>
<tr>
<td><code>      ...</code></td>
<td><code>      ...</code></td>
<td></td>
</tr>
<tr>
<td><code>   }</code></td>
<td><code>   }</code></td>
<td></td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>}</code></td>
<td></td>
</tr>
<tr>
<td><code>interfaces interface-name {</code></td>
<td><code>interfaces interface-name {</code></td>
<td>Statements moved to different hierarchy.</td>
</tr>
<tr>
<td><code>   ether-options {</code></td>
<td><code>   link-mode mode;</code></td>
<td></td>
</tr>
<tr>
<td><code>      link-mode mode;</code></td>
<td>`      speed (auto-negotiation</td>
<td>speed)</td>
</tr>
<tr>
<td>`      speed (auto-negotiation</td>
<td>speed)</td>
<td>`   speed speed)</td>
</tr>
<tr>
<td><code>   }</code></td>
<td><code>   }</code></td>
<td></td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>}</code></td>
<td></td>
</tr>
<tr>
<td><code>interfaces interface-name {</code></td>
<td><code>interfaces interface-name {</code></td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td><code>   unit logical-unit-number {</code></td>
<td><code>   native-vlan-id vlan-id</code></td>
<td></td>
</tr>
<tr>
<td><code>      family ethernet-switching {</code></td>
<td><code>      native-vlan-id vlan-id</code></td>
<td></td>
</tr>
<tr>
<td><code>       native-vlan-id vlan-id</code></td>
<td><code> </code></td>
<td></td>
</tr>
<tr>
<td><code>   }</code></td>
<td><code>   }</code></td>
<td></td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>}</code></td>
<td></td>
</tr>
<tr>
<td><code>interfaces interface-name {</code></td>
<td><code>interfaces interface-name {</code></td>
<td>Statement replaced with a new statement.</td>
</tr>
<tr>
<td><code>   unit logical-unit-number {</code></td>
<td><code>   unit logical-unit-number {</code></td>
<td></td>
</tr>
<tr>
<td><code>      family ethernet-switching {</code></td>
<td><code>      family ethernet-switching {</code></td>
<td></td>
</tr>
<tr>
<td><code>         port-mode mode</code></td>
<td><code>         interface-mode mode</code></td>
<td></td>
</tr>
<tr>
<td><code>   }</code></td>
<td><code>   }</code></td>
<td></td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>}</code></td>
<td></td>
</tr>
<tr>
<td><code>interfaces vlan</code></td>
<td><code>interfaces irb</code></td>
<td>Statement replaced with a new statement.</td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>}</code></td>
<td></td>
</tr>
</tbody>
</table>
### Table 3: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protocols</strong> {</td>
<td><strong>protocols</strong> {</td>
<td>IGMP snooping is configured on a VLAN.</td>
</tr>
<tr>
<td>igmp-snooping {</td>
<td>igmp-snooping {</td>
<td></td>
</tr>
<tr>
<td>trace-options {</td>
<td>vlan vlan-name {</td>
<td></td>
</tr>
<tr>
<td>file filename &lt;files number&gt; &lt;no-stamp&gt; &lt;replace&gt;</td>
<td>immediate-leave;</td>
<td></td>
</tr>
<tr>
<td>&lt;size maximum-file-size&gt; &lt;world-readable&gt; &lt;no-world-readable&gt;</td>
<td>interface interface-name {</td>
<td></td>
</tr>
<tr>
<td>flag flag &lt;flag-modifier&gt; &lt;disable&gt;;</td>
<td>group-limit &lt;1..65535&gt;;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>host-only-interface</td>
<td></td>
</tr>
<tr>
<td>vlan (all</td>
<td>vlan-identifier) {</td>
<td>multicast-router-interface;</td>
</tr>
<tr>
<td>disable;</td>
<td>immediate-leave;</td>
<td></td>
</tr>
<tr>
<td>data-forwarding {</td>
<td>static {</td>
<td></td>
</tr>
<tr>
<td>receiver {</td>
<td>group multicast-ip-address {</td>
<td></td>
</tr>
<tr>
<td>install;</td>
<td>source &lt;&gt;;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>immediate-leave;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>interface (all</td>
<td>interface-name) {</td>
<td>}</td>
</tr>
<tr>
<td>multicast-router-interface;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>static {</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>group multicast-ip-address;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>proxy {</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>source-address ip-address;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>robust-count (IGMP Snooping) number;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td>Statements removed.</td>
</tr>
<tr>
<td><strong>vlans</strong> {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dot1q-tunneling {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer-vlans (id</td>
<td>native</td>
<td>range);</td>
</tr>
<tr>
<td>layer2-protocol-tunneling all</td>
<td>protocol-name {</td>
<td></td>
</tr>
<tr>
<td>drop-threshold number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>shutdown-threshold number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 3: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statements moved to different hierarchy.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td>filter {</td>
<td>forwarding-options {</td>
<td></td>
</tr>
<tr>
<td>input filter-name</td>
<td>input filter-name</td>
<td></td>
</tr>
<tr>
<td>output filter-name</td>
<td>output filter-name</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statements removed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td>You can assign interfaces to a VLAN using the [edit interfaces</td>
</tr>
<tr>
<td>interface interface-name {</td>
<td>interface-name unit</td>
<td>interface-name unit</td>
</tr>
<tr>
<td>egress;</td>
<td>logical-unit-number</td>
<td>logical-unit-number</td>
</tr>
<tr>
<td>ingress;</td>
<td>family</td>
<td>family</td>
</tr>
<tr>
<td>mapping (native (push</td>
<td>swap)</td>
<td>policy</td>
</tr>
<tr>
<td></td>
<td>tag (push</td>
<td>swap));</td>
</tr>
<tr>
<td>pvlan-trunk;</td>
<td></td>
<td>hierarchy.</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statement removed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td>isolation-id id-number;</td>
<td>isolation-id id-number;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Syntax changed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td>l3-interface vlan.logical-interface-number;</td>
<td>l3-interface irb.logical-interface-number;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statement removed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td>Ingress traffic is automatically tracked.</td>
</tr>
<tr>
<td>l3-interface-ingress-counting layer-3-interface-name;</td>
<td>l3-interface-ingress-counting layer-3-interface-name;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
Table 3: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statements moved to different hierarchies and renamed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td>mac-limit limit action action;</td>
<td>switch-options {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>interface-mac-limit limit {</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>packet-action action;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlans {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch-options {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface interface-name {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface-mac-limit limit {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet-action action;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlans {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mac-limit limit action action;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>protocols {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>l2-learning {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>global-mac-table-aging-time seconds;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlans {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mac-table-aging-time seconds;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlans {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no-local-switching;</td>
<td>Statement removed.</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlans {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>no-mac-learning;</td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlans {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td></td>
<td>primary-vlan vlan-name;</td>
<td>Statement removed.</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
Table 3: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlans {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-prune;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-range vlan-id-low-vlan-id-high;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td>vs</td>
<td>Statement removed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-id-list [vlan-id-numbers];</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enhanced Layer 2 CLI Configuration Statement and Command Changes

The enhanced Layer 2 Command Line Interface (CLI) feature is introduced in Junos OS Release 12.3R2. The enhanced Layer 2 CLI feature changes the CLI for some Layer 2 features on EX Series switches. This enhanced CLI will be used to configure Layer 2 features on future EX Series hardware platforms, and also to configure Layer 2 features on other Juniper Networks products.

The following tables provide a list of existing commands that were moved to new hierarchies or changed on EX Series switches as part of this CLI enhancement effort. The table is provided as a high-level reference only. For detailed information about these commands, use the links to the configuration statements provided in the table or see the technical documentation.

Table 4: Enhanced Layer 2 CLI Changes

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-switching-options {</td>
<td>forwarding-options {</td>
<td>Statements moved to different hierarchy.</td>
</tr>
<tr>
<td>analyzer {</td>
<td>analyzer {</td>
<td></td>
</tr>
<tr>
<td>name {</td>
<td>name {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>switch-options {</td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td>authentication-whitelist {</td>
<td>switch-options {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>authentication-whitelist {</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-switching-options {</td>
<td>protocols {</td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td>bpdu-block {</td>
<td>layer2-control {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>bpdu-block {</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>—</td>
<td>Statements deleted.</td>
</tr>
<tr>
<td>dot1q-tunneling {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ether-type (0x8100</td>
<td>0x88a8</td>
<td>0x9100);</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>switch-options {</td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td>interfaces interface-name {</td>
<td>interfaces interface-name {</td>
<td></td>
</tr>
<tr>
<td>no-mac-learning;</td>
<td>no-mac-learning;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>—</td>
<td>Statements deleted.</td>
</tr>
<tr>
<td>mac-notification {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>notification-interval seconds;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>protocols {</td>
<td>Statement replaced with new statement and moved to different hierarchy.</td>
</tr>
<tr>
<td>mac-table-aging-time seconds;</td>
<td>l2-learning {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>global-mac-table-aging-time seconds;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>interfaces interface-name family</td>
<td>Statement replaced with a new statement.</td>
</tr>
<tr>
<td>port-error-disable {</td>
<td>ethernet-switching {</td>
<td></td>
</tr>
<tr>
<td>disable-timeout timeout;</td>
<td>recovery-timeout seconds;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>switch-options {</td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td>redundant-trunk-group {</td>
<td>redundant-trunk-group {</td>
<td></td>
</tr>
<tr>
<td>group name {</td>
<td>group name {</td>
<td></td>
</tr>
<tr>
<td>description;</td>
<td>description;</td>
<td></td>
</tr>
<tr>
<td>interface interface-name {</td>
<td>interface interface-name {</td>
<td></td>
</tr>
<tr>
<td>primary;</td>
<td>primary;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>preempt-cutover-timer seconds;</td>
<td>preempt-cutover-timer seconds;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ethernet-switching-options {</strong></td>
<td><strong>vlans vlan-name forwarding-options{</strong></td>
<td>Statements moved to different hierarchy.</td>
</tr>
<tr>
<td>secure-access-port {</td>
<td>dhcp-security {</td>
<td><strong>NOTE:</strong> The statement examine-dhcp does not exist in the changed hierarchy.</td>
</tr>
<tr>
<td>interface (all</td>
<td>interface-name) {</td>
<td>arp-inspection;</td>
</tr>
<tr>
<td>(dhcp-trusted</td>
<td>no-dhcp-trusted );</td>
<td>group group-name {</td>
</tr>
<tr>
<td>static-ip ip-address {</td>
<td>interface interface-name {</td>
<td>on page 4023 for additional information.</td>
</tr>
<tr>
<td>mac mac-address;</td>
<td>static-ip ip-address {</td>
<td></td>
</tr>
<tr>
<td>vlan vlan-name;</td>
<td>mac mac-address;</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>overrides {</td>
<td></td>
</tr>
<tr>
<td>_vlan (all</td>
<td>vlan-name) {</td>
<td>no-option-82;</td>
</tr>
<tr>
<td>(arp-inspection</td>
<td>no-arp-inspection );</td>
<td>trusted;</td>
</tr>
<tr>
<td>dhcp-option82 {</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>disable;</td>
<td><strong>ip-source-guard;</strong></td>
<td></td>
</tr>
<tr>
<td>circuit-id {</td>
<td>no-dhcp-snooping;</td>
<td></td>
</tr>
<tr>
<td>prefix hostname;</td>
<td>option-82 {</td>
<td></td>
</tr>
<tr>
<td>use-interface-description;</td>
<td>circuit-id {</td>
<td></td>
</tr>
<tr>
<td>use-vlan-id;</td>
<td>prefix {</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>host-name;</td>
<td></td>
</tr>
<tr>
<td>remote-id {</td>
<td>routing-instance-name;</td>
<td></td>
</tr>
<tr>
<td>prefix (hostname</td>
<td>mac</td>
<td>none);</td>
</tr>
<tr>
<td>use-interface-description;</td>
<td>use-vlan-id;</td>
<td></td>
</tr>
<tr>
<td>use-string string;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>vendor-id [string];</td>
<td><strong>remote-id {</strong></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>host-name;</td>
<td></td>
</tr>
<tr>
<td>(examine-dhcp</td>
<td>no-examine-dhcp);</td>
<td>use-interface-description (device</td>
</tr>
<tr>
<td>}</td>
<td>use-string string;</td>
<td></td>
</tr>
<tr>
<td>(ip-source-guard</td>
<td>no-ip-source-guard);</td>
<td>vendor-id [string];</td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td><strong>ethernet-switching-options {</strong></td>
<td><strong>system {</strong></td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td>secure-access-port {</td>
<td>processes {</td>
<td></td>
</tr>
<tr>
<td>dhcp-snooping-file {</td>
<td>dhcp-service</td>
<td></td>
</tr>
<tr>
<td>location local_pathname</td>
<td>remote_URL;</td>
<td>dhcp-snooping-file local_pathname</td>
</tr>
<tr>
<td>timeout seconds;</td>
<td>write-interval interval;</td>
<td></td>
</tr>
<tr>
<td>write-interval seconds;</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ethernet-switching-options {</strong></td>
<td><strong>vlans vlan-name switch-options {</strong></td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td>secure-access-port vlan (all</td>
<td>vlan-name{</td>
<td>mac-move-limit</td>
</tr>
<tr>
<td>mac-move-limit</td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-switching-options {</td>
<td>vlans {</td>
<td>Statement replaced with new statement and moved to different hierarchy.</td>
</tr>
<tr>
<td>static [</td>
<td>vlan-name [</td>
<td></td>
</tr>
<tr>
<td>vlan vlan-id {</td>
<td>switch-options [</td>
<td></td>
</tr>
<tr>
<td>mac mac-address next-hop</td>
<td>interface interface-name [</td>
<td></td>
</tr>
<tr>
<td>interface interface-name {</td>
<td>static-mac mac-address;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>forwarding-options {</td>
<td>Storm control configuration is done in two steps. The first step is to create a storm control profile at the [edit forwarding-options] hierarchy, and the second step is to bind the profile to a logical interface at the [edit interfaces] hierarchy. See “Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches” on page 2019 for additional information.</td>
</tr>
<tr>
<td>storm-control {</td>
<td>storm-control-profiles profile-name {</td>
<td></td>
</tr>
<tr>
<td>(...}</td>
<td>(...)</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>—</td>
<td>Statements removed.</td>
</tr>
<tr>
<td>traceoptions {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>file filename &lt;files number&gt; &lt;no-stamp&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;replace&gt; &lt;size size&gt; &lt;world-readable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ethernet-switching-options {</td>
<td>switch-options on page 2027 {</td>
<td>Hierarchy renamed.</td>
</tr>
<tr>
<td>unknown-unicast-forwarding {</td>
<td>unknown-unicast-forwarding {</td>
<td></td>
</tr>
<tr>
<td>(...}</td>
<td>(...)</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
### Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ethernet-switching-options {</code>&lt;br&gt;  <code>voip {</code>&lt;br&gt;  `  interface (all</td>
<td>[interface-name</td>
<td><code>&lt;br&gt;  </code>    access-ports]) {<code>&lt;br&gt;  </code>    forwarding-class (assured-forwarding</td>
</tr>
<tr>
<td><code>interfaces interface-name {</code>&lt;br&gt;  <code>  ether-options {</code>&lt;br&gt;  <code>    link-mode mode;</code>&lt;br&gt;  `    speed (auto-negotiation</td>
<td>speed)<code>&lt;br&gt;  </code>  } }`</td>
<td><code>interfaces interface-name {</code>&lt;br&gt;  <code>  link-mode mode;</code>&lt;br&gt;  <code>  speed speed)</code>&lt;br&gt;  <code> } }</code></td>
</tr>
<tr>
<td><code>interfaces interface-name {</code>&lt;br&gt;  <code>  unit logical-unit-number {</code>&lt;br&gt;  <code>    family ethernet-switching {</code>&lt;br&gt;  <code>      native-vlan-id vlan-id</code>&lt;br&gt;  <code>    }</code>&lt;br&gt;  <code>  } }</code></td>
<td><code>interfaces interface-name {</code>&lt;br&gt;  <code>  native-vlan-id vlan-id</code>&lt;br&gt;  <code> } }</code></td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td><code>interfaces interface-name {</code>&lt;br&gt;  <code>  unit logical-unit-number {</code>&lt;br&gt;  <code>    family ethernet-switching {</code>&lt;br&gt;  <code>      port-mode mode</code>&lt;br&gt;  <code>    }</code>&lt;br&gt;  <code>  } }</code></td>
<td><code>interfaces interface-name {</code>&lt;br&gt;  <code>  unit logical-unit-number {</code>&lt;br&gt;  <code>    family ethernet-switching {</code>&lt;br&gt;  <code>      interface-mode mode</code>&lt;br&gt;  <code>    }</code>&lt;br&gt;  <code>  } }</code></td>
<td>Statement replaced with a new statement.</td>
</tr>
<tr>
<td><code>interfaces vlan</code></td>
<td><code>interfaces irb</code></td>
<td>Statement replaced with a new statement.</td>
</tr>
</tbody>
</table>
Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocols {</td>
<td>protocols {</td>
<td>IGMP snooping is</td>
</tr>
<tr>
<td>igmp-snooping {</td>
<td>igmp-snooping</td>
<td>configured on a VLAN.</td>
</tr>
<tr>
<td>traceoptions {</td>
<td>vlan</td>
<td></td>
</tr>
<tr>
<td>file filename &lt;files number&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;no-stamp&gt; &lt;replace&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;size maximum-file-size&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;world-readable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>no-world-readable&gt;;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>flag flag &lt;flag-modifier&gt; &lt;disable&gt;;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>vlan-name</td>
<td></td>
</tr>
<tr>
<td>interface interface-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>immediate-leave;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>group-limit &lt;1..65535&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>host-only-interface</td>
<td></td>
</tr>
<tr>
<td>multicast-router-interface;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>immediate-leave;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static {</td>
<td>group multicast-ip-address</td>
<td></td>
</tr>
<tr>
<td>group multicast-ip-address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>proxy {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>source-address ip-address;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>query-interval number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>query-last-member-interval number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>query-response-interval number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>robust-count number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>traceoptions {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>file filename &lt;files number&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;no-stamp&gt; &lt;replace&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;size maximum-file-size&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;world-readable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>no-world-readable&gt;;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>flag flag &lt;flag-modifier&gt;;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td></td>
<td>Statements removed.</td>
</tr>
<tr>
<td>vlan-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dot1q-tunneling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer-vlans (id</td>
<td>native</td>
<td>range);</td>
</tr>
<tr>
<td>layer2-protocol-tunneling all</td>
<td></td>
<td></td>
</tr>
<tr>
<td>protocol-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drop-threshold number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>shutdown-threshold number;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statements moved to</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td>different hierarchy.</td>
</tr>
<tr>
<td>filter{</td>
<td>forwarding-options {</td>
<td></td>
</tr>
<tr>
<td>input filter-name</td>
<td>input filter-name</td>
<td></td>
</tr>
<tr>
<td>output filter-name;</td>
<td>output filter-name;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

| vlans {           | —                  | Statements removed. |
|       vlan-name {  |                     | You can assign interfaces |
|           interface interface-name {  |                     | to a VLAN using the [edit |
|               egress;                    |                     | interfaces%
|               ingress;                   |                     | interface-name unit |
|               mapping (native (push | swap) | policy |
|                   | tag (push | swap));       | ethernet-switching vlan |
|               pvlan-trunk;              |                     | members vlan-name] |
|         ...       |                     | hierarchy. |
|       }            |                     |
| }                  |                     |

| vlans {           | —                  | Statement removed. |
|       vlan-name {  |                     |                      |
|           isolation-id id-number;  |                     |
|         ...       |                     |
| }                  |                     |

| vlans {           | vlans {           | Syntax changed. |
|       vlan-name {  |       vlan-name {  |                      |
|           13-interface vlan.logical-interface-number; |           13-interface irb.logical-interface-number;  |
|         ...       |         ...       |
|       }            |       }            |

| vlans {           | —                  | Statement removed. |
|       vlan-name {  |                     | Ingress traffic is |
|           13-interface-ingress-counting |                     | automatically tracked. |
|               layer-3-interface-name;  |                     |
|         ...       |                     |
| }                  |                     |
Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statements moved to different hierarchies and renamed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>vlan-name {</td>
<td></td>
</tr>
<tr>
<td>mac-limit limit action action;</td>
<td>switch-options {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>interface-mac-limit limit {</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>packet-action action;</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td>protocols {</td>
<td>Statement moved to different hierarchy and renamed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td>l2-learning {</td>
<td></td>
</tr>
<tr>
<td>switch-options {</td>
<td>global-mac-table-aging-time seconds;</td>
<td></td>
</tr>
<tr>
<td>interface interface-name {</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>interface-mac-limit limit {</td>
<td>packet-action action;</td>
<td></td>
</tr>
<tr>
<td>packet-action action;</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Statement removed.</td>
</tr>
<tr>
<td>vlans {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>no-local-switching;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Statement moved to different hierarchy.</td>
</tr>
<tr>
<td>vlans {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>no-mac-learning;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Statement removed.</td>
</tr>
<tr>
<td>vlans {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>primary-vlan vlan-name;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 4: Enhanced Layer 2 CLI Changes (continued)

<table>
<thead>
<tr>
<th>Original Hierarchy</th>
<th>Changed Hierarchy</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlans {</td>
<td>—</td>
<td>Statement removed.</td>
</tr>
<tr>
<td>vlan-name {</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlan-prune;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vlans {</td>
<td>vlans {</td>
<td>Statement replaced</td>
</tr>
<tr>
<td>vlan-name [</td>
<td>vlan-name [</td>
<td>with new statement.</td>
</tr>
<tr>
<td>vlan-range vlan-id-low-vlan-id-high;</td>
<td>vlan-id-list [vlan-id-numbers];</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

Related Documentation

- EX4300 Switches Hardware Overview
PART 2

Software Features Overview

• Software Features Overview on page 27
Software Features Overview

This topic lists the Juniper Networks EX Series Ethernet Switches software features, the Juniper Networks Junos operating system (Junos OS) release in which they were introduced, and the first Junos OS release for each switch.

NOTE: For Virtual Chassis features, see "EX Series Virtual Chassis Software Features Overview" on page 75.

NOTE: In all tables in this topic, "N.S." = "Not supported", and "–" = "Not applicable".

- Table 5 on page 28—First Junos OS Release for Each EX Series Switch
- Table 6 on page 29—Access Control Features
- Table 7 on page 30—Administration Features
- Table 8 on page 31—Class-of-Service (CoS) Features
- Table 9 on page 32—Class-of-Service (CoS) Features for EX9200 Switches
- Table 10 on page 34—Converged Networks (LAN and SAN) Features
- Table 11 on page 34—Device Security Features
- Table 12 on page 35—High Availability and Resiliency Features
- Table 13 on page 37—High Availability and Resiliency Features on EX9200 Switches
- Table 14 on page 39—Interfaces Features
The Junos OS release for software features on a switch cannot be earlier than the first Junos OS release for that switch.

Table 5: First Junos OS Release for Each EX Series Switch

<table>
<thead>
<tr>
<th>Switch</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200 switches*</td>
<td>Junos OS Release 10.1R1</td>
</tr>
<tr>
<td></td>
<td>*EX2200-C models: Junos OS Release 11.3R1</td>
</tr>
<tr>
<td>EX3200 switches</td>
<td>Junos OS Release 9.0R1</td>
</tr>
</tbody>
</table>
Table 5: First Junos OS Release for Each EX Series Switch (continued)

<table>
<thead>
<tr>
<th>Switch</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3300 switches</td>
<td>Junos OS Release 11.3R1</td>
</tr>
<tr>
<td>EX4200 switches</td>
<td>Junos OS Release 9.0R1</td>
</tr>
<tr>
<td>EX4300 switches</td>
<td>Junos OS Release 13.2X50-D10</td>
</tr>
<tr>
<td><strong>EX4500 switches</strong></td>
<td>Junos OS Release 10.2R1*</td>
</tr>
<tr>
<td><strong>EX4500-C models: Junos OS Release 10.3R2</strong></td>
<td></td>
</tr>
<tr>
<td>EX4550 switches</td>
<td>Junos OS Release 12.2R1</td>
</tr>
<tr>
<td>EX6200 switch</td>
<td>Junos OS Release 11.3R2</td>
</tr>
<tr>
<td>EX8208 switches</td>
<td>Junos OS Release 9.4R1</td>
</tr>
<tr>
<td>EX8216 switches</td>
<td>Junos OS Release 9.5R1</td>
</tr>
<tr>
<td>EX9200 switches</td>
<td>Junos OS Release 12.3R2</td>
</tr>
</tbody>
</table>

Table 6: Access Control Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X authentication (port-based, multiple supplicant)</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.2R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>802.1X authentication with authentication bypass</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.2R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>802.1X authentication with VLAN assignment, VoIP VLAN support</td>
<td>10.1R1</td>
<td>9.0R1</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>802.1X user-based dynamic firewall filters</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>802.1X user-based dynamic firewall filters on multiple-supplicant ports</td>
<td>10.1R1</td>
<td>9.5R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>802.1X per-user statistics</td>
<td>10.1R1</td>
<td>9.2R1</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>10.3R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Authentication fallback</td>
<td>11.3R1</td>
<td>10.3R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
</tbody>
</table>
Table 6: Access Control Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captive portal authentication for Layer 3 interfaces</td>
<td>11.3R1</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Captive portal authentication for Layer 2 interfaces</td>
<td>11.3R1</td>
<td>10.3R1</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Energy Efficient Ethernet (EEE)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Infranet Controller (IC) as an external captive-portal server</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>MAC RADIUS authentication</td>
<td>10.1R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>NetBIOS snooping</td>
<td>11.3R5</td>
<td>11.1R1</td>
<td>11.3R5</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R5</td>
<td>11.1R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Server fail fallback</td>
<td>10.1R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

Table 7: Administration Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>System logging (syslog) over IPv4</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>System logging (syslog) over IPv6</td>
<td>10.3R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.4R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.1R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>System snapshot</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 8: Class-of-Service (CoS) Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of service (CoS)—Class-based queuing with prioritization, Layer 2 and Layer 3 classification, rewrite, and queuing; strict priority queuing on egress</td>
<td>10.1R</td>
<td>9.0R2</td>
<td>11.3R</td>
<td>13.2X50 - D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td>See Table 9 on page 32 for a list of EX9200 CoS features</td>
</tr>
<tr>
<td>CoS—DSCP, IEEE 802.1p, and IP precedence packet rewrites on RVIs or IRB interfaces</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>11.3R</td>
<td>N.S.</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>CoS—Interface-specific classifiers on RVIs or IRB interfaces</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>11.3R</td>
<td>13.2X50 - D10</td>
<td>11.3R1</td>
<td>12.2R</td>
<td>N.S.</td>
<td>10.2R1</td>
<td></td>
</tr>
<tr>
<td>CoS—Multidestination</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>N.S.</td>
<td>9.5R1</td>
</tr>
<tr>
<td>CoS—Per-interface classification</td>
<td>N.S.</td>
<td>9.3R1</td>
<td>11.3R</td>
<td>13.2X50 - D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R2</td>
<td>10.2R1</td>
<td></td>
</tr>
<tr>
<td>CoS support on link aggregation groups (LAGs)</td>
<td>10.1R</td>
<td>9.2R1</td>
<td>11.3R</td>
<td>13.2X50 - D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>N.S.</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>CoS support on RVIs or IRB interfaces</td>
<td>10.3R</td>
<td>9.4R1</td>
<td>11.3R</td>
<td>13.2X50 - D10</td>
<td>10.4R</td>
<td>12.2R</td>
<td>N.S.</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>DSCP setting on ingress interface</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td></td>
</tr>
<tr>
<td>Flexible CoS-outer 802.1p marking</td>
<td>N.S.</td>
<td>9.6R1</td>
<td>12.3R</td>
<td>N.S.</td>
<td>12.1R</td>
<td>12.2R</td>
<td>N.S.</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>Interface-specific CoS rewrite rules</td>
<td>10.3R</td>
<td>9.4R1</td>
<td>N.S.</td>
<td>11.2R</td>
<td>12.2R</td>
<td>N.S.</td>
<td>10.2R1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 8: Class-of-Service (CoS) Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.2X50-D10 (for Layer 3 interfaces; IRB interfaces and Layer 3 subinterfaces. N.S.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Junos EZQoS for CoS</td>
<td>10.1R</td>
<td>9.3R</td>
<td>11.3R</td>
<td>13.2X50-D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R</td>
<td>9.4R</td>
<td></td>
</tr>
<tr>
<td>Port shaping and queue shaping</td>
<td>10.1R</td>
<td>9.3R</td>
<td>11.3R</td>
<td>13.2X50-D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R</td>
<td>10.1R</td>
<td></td>
</tr>
<tr>
<td>Re-marking of bridged packets</td>
<td>11.2R</td>
<td>9.4R</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R</td>
<td>10.2R</td>
<td></td>
</tr>
<tr>
<td>Shaped-deficit weighted round-robin (SDWRR)</td>
<td>10.1R</td>
<td>9.0R</td>
<td>11.3R</td>
<td>13.2X50-D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R</td>
<td>9.4R</td>
<td></td>
</tr>
<tr>
<td>Single-rate two-color marking</td>
<td>10.1R</td>
<td>9.0R</td>
<td>11.3R</td>
<td>13.2X50-D10</td>
<td>10.2R</td>
<td>12.2R</td>
<td>11.3R</td>
<td>9.4R</td>
<td></td>
</tr>
</tbody>
</table>

### Table 9: Class-of-Service (CoS) Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning forwarding class and DSCP value for Routing Engine generated traffic</td>
<td>12.3R</td>
</tr>
<tr>
<td>BA classification for VPLS based on IEEE 802.1p bits</td>
<td>12.3R</td>
</tr>
<tr>
<td>Classification—Associate packets with CoS servicing levels. Types of classification:</td>
<td>12.3R</td>
</tr>
<tr>
<td>• Behavior aggregate (BA)—Operates on packets as they enter the switch</td>
<td></td>
</tr>
<tr>
<td>• Multifield classification—Examines multiple fields in packets.</td>
<td></td>
</tr>
<tr>
<td>• Fixed classification—Associate a forwarding class with a packet regardless of packet contents.</td>
<td></td>
</tr>
<tr>
<td>Classification and DSCP marking of distributed protocol handler traffic</td>
<td>12.3R</td>
</tr>
<tr>
<td>Classification of control-plane traffic</td>
<td>12.3R</td>
</tr>
<tr>
<td>CoS classification and rewrite for IRB and Layer 2 interfaces and for other Layer 3 interfaces. Port-level queuing, scheduling, and shaping are supported.</td>
<td>12.3R</td>
</tr>
</tbody>
</table>
Table 9: Class-of-Service (CoS) Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress GRE classification based on DSCP</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IEEE 802.1p inheritance push and swap from transparent tags configuration</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Elevated packet drops during oversubscription</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 policers for the ingress and egress interfaces. Policer types:</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Single-rate two-color</td>
<td></td>
</tr>
<tr>
<td>• Single-rate three-color (color-blind and color-aware)</td>
<td></td>
</tr>
<tr>
<td>• Two-rate three-color (color-blind and color-aware)</td>
<td></td>
</tr>
<tr>
<td>Independent values for DSCP and EXP bits</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Apply CoS schedulers on ingress interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Ingress DSCP bits for multicast traffic over Layer 3 VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 traffic policing</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Policer support for aggregated Ethernet bundles (link aggregation groups, or LAGs)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Queuing support for logical tunnel interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Rate-limit and excess rate or excess priority option</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Re-marking of MVPN GRE encapsulation DCSP at ASBR</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Scheduling</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Set IPv6 DSCP and MPLS EXP independently</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Set IPv6 DiffServ code point (DSCP) and MPLS EXP independently</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for Layer 2 policers at the VLAN level</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for applying a transmit rate limit to logical interfaces on Type 1, 2, or 3 Multiservices PICs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for configuring ToS rewrite rules so that DCSP bits of GRE packets are consistent with service providers’ CoS policy</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for copying the TOS bits to the outer IP header on GRE tunnel traffic sent by the Routing Engine</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for setting the forwarding class and DSCP value for traffic generated by the Routing Engine</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Unified command to display all CoS statistics</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
**Table 10: Converged Networks (LAN and SAN) Features on Switches by Junos OS Release**

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE: The EX4500 switch models that support Fibre Channel over Ethernet features must be Converged Enhanced Ethernet (CEE) capable. The CEE-capable EX4500 switch models have a “–C” in the hardware model number. See EX4500 Switch Models.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Center Bridging Capability Exchange protocol (DCBX)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>DCBX application protocol TLV exchange</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>FIP snooping</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.4R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Priority-based flow control (PFC)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.4R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
</tbody>
</table>

**Table 11: Device Security Features on Switches by Junos OS Release**

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic recovery for port error disable conditions</td>
<td>10.1R1</td>
<td>9.6R1</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.0R1</td>
</tr>
<tr>
<td>Storm control (broadcast and unicast)</td>
<td>10.1R1</td>
<td>9.1R1</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>Storm control (multicast)</td>
<td>10.3R2</td>
<td>10.3R2</td>
<td>N.S.</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>10.3R2</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R2</td>
</tr>
<tr>
<td>Unknown Layer 2 unicast forwarding</td>
<td>10.1R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.0R1</td>
</tr>
</tbody>
</table>
Table 12: High Availability and Resiliency Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful protocol restart for BGP</td>
<td>–</td>
<td>9.0R2</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>–</td>
<td>–</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>Graceful protocol restart for IS-IS</td>
<td>–</td>
<td>9.3R2</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>–</td>
<td>–</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>Graceful protocol restart for OSPF</td>
<td>–</td>
<td>9.0R2</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>–</td>
<td>–</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>Graceful protocol restart for RSVP and LDP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
</tr>
<tr>
<td>GRES for ARP entries, forwarding database, and Layer 3 protocols</td>
<td>–</td>
<td>9.2R1  (Virtual Chassis only)</td>
<td>11.3R1  (Virtual Chassis only)</td>
<td>13.2X50-D10</td>
<td>11.2R1  (Virtual Chassis only)</td>
<td>12.2R1  (Virtual Chassis only)</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>GRES for IGMP snooping</td>
<td>–</td>
<td>11.3R1  (Virtual Chassis only)</td>
<td>12.1R1  (Virtual Chassis only)</td>
<td>13.2X50-D10</td>
<td>11.4R1  (Virtual Chassis only)</td>
<td>12.2R1  (Virtual Chassis only)</td>
<td>N.S.</td>
<td>11.3R1</td>
</tr>
<tr>
<td>GRES for LACP</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.3R1</td>
</tr>
<tr>
<td>GRES for Layer 2 and Layer 3 VPN LSPs</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
</tr>
<tr>
<td>GRES for port security (DHCP snooping, DAI, and IP source guard)</td>
<td>–</td>
<td>9.2R1  (Virtual Chassis only)</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>–</td>
<td>–</td>
<td>11.3R2</td>
<td>9.6R1</td>
</tr>
<tr>
<td>LACP support for dual-homing applications in data centers</td>
<td>10.1R1</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.0R1</td>
</tr>
<tr>
<td>Link Aggregation Control Protocol (LACP)</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>Link aggregation groups (LAGs)</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
</tbody>
</table>

**NOTE:** For complete lists of Virtual Chassis features, see “EX Series Virtual Chassis Software Features Overview” on page 75.
<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonstop active routing (NSR) for BGP, IS-IS, IGMP with BFD, and RIP</td>
<td>–</td>
<td>11.1R1 (Virtual Chassis only)</td>
<td>12.1R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>11.3R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>11.3R2</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for IPv6 IS-IS, RIPng, and OSPFv3 with BFD</td>
<td>–</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>11.2R1</td>
<td></td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for OSPFv2</td>
<td>–</td>
<td>11.1R1</td>
<td>12.1R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>11.2R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>11.3R2</td>
<td>10.4R1</td>
<td></td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for Protocol Independent Multicast (PIM)</td>
<td>N.S.</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>11.4R2</td>
<td></td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for RSVP and LDP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td></td>
</tr>
<tr>
<td>Nonstop bridging (NSB) for LAGs and LACP</td>
<td>–</td>
<td>11.4R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>11.4R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>12.1R1</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>Nonstop bridging (NSB) for LLDP and LLDP-MED</td>
<td>–</td>
<td>11.3R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>Nonstop bridging (NSB) for spanning-tree protocols</td>
<td>–</td>
<td>11.3R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>12.1R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>12.1R1</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>Nonstop software upgrade (NSSU)</td>
<td>–</td>
<td>12.1R1 (Virtual Chassis only)</td>
<td>12.2R1 (Virtual Chassis only)</td>
<td>N.S.</td>
<td>12.1R1 (Virtual Chassis only)</td>
<td>12.1R1 (Virtual Chassis only)</td>
<td>12.2R1</td>
<td>10.4R1</td>
<td></td>
</tr>
<tr>
<td>Power budget management</td>
<td>–</td>
<td>–</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>–</td>
<td>–</td>
<td>11.3R2</td>
<td>10.2R1</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
### Table 12: High Availability and Resiliency Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Router—Network Time Protocol (NTP), system logging, Simple Network Management Protocol (SNMP), RADIUS, and TACACS support in a virtual router</td>
<td>9.4R1</td>
<td>12.3R1</td>
<td>12.1Rl</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol (VRRP)</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td></td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol (VRRP)—Support for multiple VRRP owners per physical interface</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.1R1</td>
<td></td>
</tr>
</tbody>
</table>

### Table 13: High Availability and Resiliency Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful Routing Engine switchover (GRES)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) support for Protocol Independent Multicast (PIM) for IPv4 and IPv6</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) support for VPLS and for LDP-based VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) support for LDP OAM features</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) support for Layer 2 VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Unified ISSU (requires EX9200-40T or EX9200-40F line cards)</td>
<td>12.3R3</td>
</tr>
</tbody>
</table>
Table 13: High Availability and Resiliency Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Router Redundancy Protocol version 3 (VRRPv3)</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 14: Interfaces Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital optical monitoring (DOM)</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.0R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface ranges</td>
<td>10.1R1</td>
<td>10.0R1</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.1R1</td>
<td></td>
</tr>
<tr>
<td>IPv4 over generic routing encapsulation (GRE) tunnels—encapsulation support</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 over generic routing encapsulation (GRE) tunnels—encapsulation support</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 over generic routing encapsulation (GRE) tunnels—de-encapsulation support</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP directed broadcast</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Time domain reflectometry (TDR)</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Unicast reverse-path forwarding (RPF)</td>
<td>N.S.</td>
<td>9.3R2</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.1R1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>N.S.</td>
<td>9.2R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

See Table 15 on page 40 for a list of EX9200 interfaces features.
Table 14: Interfaces Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN-tagged</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 3 subinterfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 15: Interfaces Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP redirect</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Clear MAC address information</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IPv6 subnet support on loopback interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IPv6 support for unnumbered Ethernet interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Multichassis link aggregation (MC-LAG)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) support for Bidirectional Forwarding Detection (BFD)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Protection against distributed denial-of-service (DDOS) attacks</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Software support for IPv4 to IPv6 transition</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Static mapping for port forwarding</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for active monitoring on logical systems</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for VRF in Routing Engine-based sampling</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for integrated routing and bridging (IRB) MAC synchronization in MC-LAG for aggregated Ethernet</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Targeted broadcast for virtual routing and forwarding (VRF) instances</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Trunk interface enhancements:</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Configure a single logical trunk interface to support a list of VLANs or to accept packets with no VLAN tag.</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Configure multiple logical trunk interfaces on a single physical interface.</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Unicast reverse-path forwarding (RPF) loose mode, with ability to discard packets with source addresses pointing to the discard interface</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Unnumbered Ethernet—Configure IPv4 processing on interfaces without assigning explicit IP addresses to the interfaces.</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VLAN rewrite operations on incoming and outgoing frames</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
### Table 16: IP Address Management Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server and relay with option 82 for Layer 2 VLANs</td>
<td>10.2R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>DHCP server and relay with option 82 for Layer 3 interfaces</td>
<td>10.1R1</td>
<td>9.0R1</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>DNS for IPv6</td>
<td>N.S.</td>
<td>9.3R2</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>Local DHCP server</td>
<td>10.1R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Virtual router aware DHCP (VR-aware DHCP)</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td></td>
</tr>
<tr>
<td>Virtual router aware DHCPv6 (VR-aware DHCPv6)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td></td>
</tr>
<tr>
<td>Static addresses</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

See Table 17 on page 41 for a list of EX9200 IP address management features.

### Table 17: IP Address Management Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server and relay</td>
<td>12.3R2</td>
</tr>
<tr>
<td>DHCPv6 local server</td>
<td>12.3R2</td>
</tr>
<tr>
<td>DHCPv6 support</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Distinguishing DHCP duplicate clients by subinterface</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Dynamic reconfiguration of extended DHCP and DHCPv6 local server clients</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Dynamic IPv6 filters</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Expression support for dynamic profiles</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Extended DHCP relay proxy</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 17: IP Address Management Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional disabling of automatic ARP table population</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IPv6 address assignment pools</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Overriding DHCP settings on specific interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Per-interface DHCP tracing operations</td>
<td>12.3R2</td>
</tr>
<tr>
<td>S-VLAN-based shaping for dynamic profiles</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Sending a DHCP relay and relay proxy release message</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Specifying the DHCP source address used for IP packets</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for MAC address validation</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for address pool threshold traps</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Address assignment pools</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Per-interface DHCP lease limits</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

Table 18: IPv6 Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application identification (APPID) for IPv6 packets</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BFD for IPv6</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BGP for IPv6</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.1R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IPv6 CoS (multifield classification and rewrite)</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.4R1</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

### Table 18: IPv6 Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 management</td>
<td>10.3R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.4R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>(using loopback addresses only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 multicast protocols (PIM, MLDv1/v2)</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.2R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IPv6 neighbor redirect compliance with RFC 4861</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R2</td>
<td></td>
</tr>
<tr>
<td>IPv6 path MTU discovery</td>
<td>10.3R1</td>
<td>9.3R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>10.4R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IS-IS for IPv6</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.1R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>MBGP for IPv6</td>
<td>N.S.</td>
<td>9.3R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>10.1R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>OSPFv3</td>
<td>N.S.</td>
<td>9.3R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.1R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>RFC 4291 compliance</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R2</td>
<td></td>
</tr>
<tr>
<td>(See note at end of table)</td>
<td></td>
<td></td>
<td></td>
<td>See note at end of table</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIPng</td>
<td>N.S.</td>
<td>9.3R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.1R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VRRPv3 (RFC 5798 compliance, ability to send SNMP traps)</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
NOTE: Compliance with RFC 4291

EX Series switches drop the following types of illegal IPv6 packets:

- Packets that have a link-local source or destination address. Because link-local addresses are intended to be used for addressing only on a single link, EX Series switches do not forward any packets with such addresses to other links.
- Packets with the IPv6 unspecified source address 0:0:0:0:0:0:0:0.
- Packets that are to be sent outside a node but have the IPv6 loopback address 0:0:0:0:0:0:0:1 as the source address. When IPv6 packets are received on an interface, EX Series switches drop packets that have the loopback address as the destination address.

EX Series switches do not support Subnet-Router Anycast address.
### Table 19: Layer 2 Network Protocols Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q VLAN tagging</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Edge virtual bridging (EVB) support with virtual Ethernet port aggregator (VEPA)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td></td>
</tr>
<tr>
<td>Ethernet ring protection switching (ERPS, G.8032/Y.1344)</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td></td>
</tr>
<tr>
<td>Layer 2 protocol tunneling (L2PT)</td>
<td>11.1R1</td>
<td>10.0R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) with voice over IP (VoIP) integration</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>MAC-based VLANs</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Multiple VLAN Registration Protocol (MVRP, IEEE 802.1ak)</td>
<td>11.3R1</td>
<td>10.0R1</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.0R1</td>
<td></td>
</tr>
<tr>
<td>Private VLANs (PVLANs)</td>
<td>11.1R1</td>
<td>9.3R2</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.1R1</td>
<td></td>
</tr>
<tr>
<td>Private VLANs (PVLANs) support across switches</td>
<td>11.1R1</td>
<td>10.4R1</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>11.2R1</td>
<td></td>
</tr>
<tr>
<td>Proxy ARP—Restricted</td>
<td>10.1R1</td>
<td>10.0R1</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.0R1</td>
<td></td>
</tr>
</tbody>
</table>

See Table 20 on page 46 for a list of EX9200 Layer 2 networking protocols features.
Table 19: Layer 2 Network Protocols Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy ARP—Unrestricted</td>
<td>10.1R1</td>
<td>9.6R1</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.0R1</td>
<td></td>
</tr>
<tr>
<td>Proxy ARP per VLAN</td>
<td>10.1R1</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.1R1</td>
<td></td>
</tr>
<tr>
<td>Q-in-Q tunneling</td>
<td>11.1R1</td>
<td>9.3R2</td>
<td>11.4R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>Q-in-Q VLAN extended support for multiple S-VLANs per access interface, firewall-filter-based VLAN assignment, and RVIs or IRB interfaces</td>
<td>N.S.</td>
<td>9.6R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>Redundant trunk groups</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Routed VLAN interfaces (RVIs)—Also known as integrated routing and bridging (IRB) interfaces</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>VLAN ID translation</td>
<td>11.1R1</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>VLAN ranges</td>
<td>10.1R1</td>
<td>9.2R1</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

Table 20: Layer 2 Networking Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANS and virtual switching</td>
<td>12.3R2</td>
</tr>
<tr>
<td>DHCP support for integrated routing and bridging (IRB)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>MC-LAG support for IGMP snooping in IRB</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Hash-key load-balancing support for Layer 3 and Layer 4 fields</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
### Table 20: Layer 2 Networking Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP multicast over Layer 2 trunk port support</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Integrated routing and bridging (IRB)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 Ethernet OAM:</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Distributed periodic packet management process (ppmd) for improved scaling</td>
<td></td>
</tr>
<tr>
<td>• Graceful Routing Engine switchover (GRES)</td>
<td></td>
</tr>
<tr>
<td>• Remote defect indication (RDI)</td>
<td></td>
</tr>
<tr>
<td>• Configuration of action profiles</td>
<td></td>
</tr>
<tr>
<td>Layer 2 address learning in logical systems</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 forwarding support for bridging and VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 policer statistics MIB</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Firewall filter match conditions for Layer 2 bridging and VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Next-hop groups using either IP addresses or Layer 2 addresses for the next hop</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Unicast reverse-path forwarding (RPF) loose mode, with ability to discard packets with source addresses pointing to the discard interface</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Spanning-tree protocols support for Layer 2 bridging and VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VLAN rewrite operations on incoming and outgoing frames</td>
<td>12.3R2</td>
</tr>
<tr>
<td>STP root guard (root protection)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for Layer 2 and Layer 2.5 features:</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Extensive set of Layer 2 label-manipulation capabilities, Q-in-Q support</td>
<td></td>
</tr>
<tr>
<td>• MC-LAG active / standby and MC-LAG active / active</td>
<td></td>
</tr>
<tr>
<td>• xSTP protocol support</td>
<td></td>
</tr>
<tr>
<td>• Integrated Routing and Bridging (IRB) interface support</td>
<td></td>
</tr>
<tr>
<td>• IGMP snooping for multichassis link aggregation group (MC-LAG) interfaces</td>
<td></td>
</tr>
<tr>
<td>• Configurable label block sizes for VPLS</td>
<td></td>
</tr>
<tr>
<td>• Connectivity fault management process flooding to interfaces based on mesh groups</td>
<td></td>
</tr>
<tr>
<td>• Layer 2 address learning in logical systems</td>
<td></td>
</tr>
<tr>
<td>• Virtual switch support, providing virtual Layer 2 switch instances with separate Layer 2 learning domains, isolated 4K VLAN ID spaces, and STP instances</td>
<td></td>
</tr>
<tr>
<td>• Ethernet Ring Protocol (ERP) for multiple ring instances on the same physical ring</td>
<td></td>
</tr>
<tr>
<td>• Transit and bypass static label-switched paths (LSPs)</td>
<td></td>
</tr>
<tr>
<td>• Layer 2 Gigabit Ethernet logical interface policing</td>
<td></td>
</tr>
<tr>
<td>• Static LSP statistics</td>
<td></td>
</tr>
<tr>
<td>• Multiple VLAN Registration Protocol (MVRP)—IEEE 802.1ak-2007</td>
<td></td>
</tr>
</tbody>
</table>
**Table 20: Layer 2 Networking Features on EX9200 Switches by Junos OS Release (continued)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPLS root protection topology change-action control</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VLAN ranges</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Q-in-Q VLAN extended support for multiple S-VLANs per access interface, firewall-filter-based VLAN assignment, and RVIs or IRB interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Q-in-Q tunneling</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Proxy ARP—Unrestricted and restricted</td>
<td>12.3R2</td>
</tr>
<tr>
<td>MAC-based VLANs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 protocol tunneling (L2PT)</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

**Table 21: Layer 3 Protocols Features on Switches by Junos OS Release**

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidirectional Forwarding Detection (BFD)</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>12.1R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Border Gateway Protocol (BGP)</td>
<td>N.S.</td>
<td>9.0R2</td>
<td>12.1R1</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Multiprotocol Border Gateway Protocol (MBGP)</td>
<td>N.S.</td>
<td>9.3R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

See **Table 22** for a list of EX9200 Layer 3 protocols features.

A separate software license is required for BGP and MBGP. See [Understanding Software Licenses for EX Series Switches](#).
<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed periodic packet management (PPM) with BFD</td>
<td>N.S.</td>
<td>10.4R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>10.4R1</td>
<td></td>
</tr>
<tr>
<td>Distributed periodic packet management (PPM) with LACP</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.2R1</td>
<td></td>
</tr>
<tr>
<td>Filter-based forwarding</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.6R1</td>
<td></td>
</tr>
<tr>
<td>Filter-based forwarding over IPv6</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.3R1</td>
<td></td>
</tr>
<tr>
<td>Intermediate System-to-Intermediate System (IS-IS)</td>
<td>N.S.</td>
<td>9.0R2</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

A separate software license is required for IS-IS. See Understanding Software Licenses for EX Series Switches.

IPv6 Layer 3 multicast protocols                                    | N.S.   | 10.1R1         | N.S.   | 13.2X50-D10 | N.S.   | N.S.   | N.S.   | 10.2R1 |

Jumbo frames on RVIs or IRB interfaces                               | N.S.   | 9.4R1          | 11.3R1 | 13.2X50-D10 | 10.2R1 | 12.2R1 | N.S.   | 9.4R1  |

OSPF Multitopology Routing (MT-OSPF)                                 | N.S.   | 9.5R1          | N.S.   | 13.2X50-D10 | N.S.   | N.S.   | N.S.   | N.S.   |

See the Junos OS Routing Protocols Configuration Guide.
### Table 21: Layer 3 Protocols Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv2</td>
<td>11.1R1</td>
<td>9.0R2</td>
<td>11.4R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>OSPFv3 IPSec support</td>
<td>N.S.</td>
<td>10.3R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>Routing Information Protocol version 1 (RIPv1) and RIPv2</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Static routes</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Virtual routing and forwarding (VRF) with IPv4—Virtual routing instances</td>
<td>12.3R1</td>
<td>9.2R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.6R1</td>
<td></td>
</tr>
<tr>
<td>VRF with IPv4—Virtual routing instances for PIM and IGMP</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.0R1</td>
<td></td>
</tr>
<tr>
<td>VRF with IPv4—Virtual routing instances for IGMP snooping</td>
<td>N.S.</td>
<td>11.4R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>VRF with IPv6—Virtual routing instances for multicast traffic</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.1R1</td>
<td></td>
</tr>
<tr>
<td>VRF with IPv6—Virtual routing instances for unicast traffic</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.1R1</td>
<td></td>
</tr>
</tbody>
</table>

### Table 22: Layer 3 Protocols Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accumulated IGP attribute for BGP</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Advertisement of the best external BGP path to internal peers</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
# Table 22: Layer 3 Protocols Features on EX9200 Switches by Junos OS Release (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias support for local autonomous system numbers for BGP</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BFD liveness detection</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BFD protocol support for OSPFv3</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BGP remote next-hop support for single-hop EBGP peers</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BGP support for 4-byte autonomous system numbers</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BGP support for MDT-SAFI updates without a route target</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Behavior change for BGP-independent autonomous system (AS) domains</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Bidirectional Forwarding Detection (BFD) hold-down timer</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Distributed periodic packet management support for aggregate interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Egress filtering PIMv4/v6 join messages</td>
<td>12.3R2</td>
</tr>
<tr>
<td>For internal BGP (IBGP), advertise multiple paths to a destination</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Frequent BGP keepalive messages and short BGP hold time</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Hitless authentication key rollover for IS-IS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Hub-and-spoke support for multiprotocol BGP-based multicast VPNs with PIM-SSM GRE S-PMSI transport</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IPv4 subnet support on loopback interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IS-IS hold-down timer for subsequent SPF calculations</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Keepalive support for GRE interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Multitopology routing (MTR)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) support for the Routing Information Protocol (RIP) and RIP next generation (RIPng)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) support</td>
<td>12.3R2</td>
</tr>
<tr>
<td>OSPF graceful restart enhancement</td>
<td>12.3R2</td>
</tr>
<tr>
<td>OSPF hold-down timer for subsequent SPF calculations</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Only the system log notes failure to add routes</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 22: Layer 3 Protocols Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin validation for BGP</td>
<td>12.3R2</td>
</tr>
<tr>
<td>PIM join suppression support</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Priority assignment for prefixes in OSPF import policies</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Reduction in flooding of self-originated OSPF LSAs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for BFD over multihop static routes</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for BFD on logical switches</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for IPSec authentication for OSPFv2</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for OSPF database protection for OSPF and OSPFv3</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for OSPF export and import policies for network-summary LSAs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for alternate loop-free routes for IS-IS and OSPF</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for clearing the VPN tag</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for disabling the attribute set messages on independent AS domains for BGP loop detection</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for disabling traps for passive OSPFv2 interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for display of flood next-hop branch overflow condition</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for dropping and ignoring path attributes during BGP neighbor updates</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for the algorithm that determines the single best path to skip the step that evaluates an AS path</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for limiting the number of prefixes accepted from a BGP peer</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for multiarea adjacency in OSPFv2</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for multiple address families in OSPFv3</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for route leaking when the switch is in overload mode</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for route-filter-based BGP outbound route filtering</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for the BGP Monitoring Protocol</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support to hold down BGP peering sessions after a nonstop active routing (NSR) switchover Timer to delay MED updates for routes advertised by BGP groups or peers configured with the metric-out igp statement Virtual Router Redundancy Protocol (VRRP)</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
### Table 22: Layer 3 Protocols Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer to delay MED updates for routes advertised by BGP groups or peers configured with the metric-out igp statement</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol (VRRP)</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

### Table 23: Logical Systems Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical systems</td>
<td></td>
</tr>
<tr>
<td>Layer 2 address learning in logical systems</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

### Table 24: MPLS Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
</table>

A separate software license is required for MPLS. See Understanding Software Licenses for EX Series Switches.
### Table 24: MPLS Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Ethernet interfaces (LAGs) on circuit cross-connects (CCCs)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>BFD for an LDP-based LSP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td></td>
</tr>
<tr>
<td>BFD for an RSVP-based LSP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td></td>
</tr>
<tr>
<td>CCC between 2 interfaces in the same switch</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>Interior gateway protocol (IGP), IS-IS and OSPF shortcuts</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>IP over MPLS</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>IPv6 over MPLS label-switched paths (LSPs)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td></td>
</tr>
<tr>
<td>LDP-based MPLS</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>LDP tunneling (LDP over RSVP)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS-based circuit cross-connects (CCC)</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS label-switched router (LSR) support</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
</tbody>
</table>

See **Table 25** on page 56 for a list of EX9200 MPLS features.
<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Layer 2 CCC on Ethernet-encapsulated interfaces (RFC 6624)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS Layer 2 CCC on VLAN-encapsulated interfaces (RFC 4905)</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>MPLS Layer 2 VLAN CCC on Ethernet-encapsulated interfaces (RFC 6624)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>MPLS Layer 2 VLAN CCC on VLAN-encapsulated interfaces (RFC 4905)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>MPLS Layer 2 VPN over CCC</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS Layer 2 VPN over VLAN CCC</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.3R1</td>
<td></td>
</tr>
<tr>
<td>MPLS OAM-LSP ping</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS over untagged Layer 3 interfaces</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS with class of service (CoS)</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R5</td>
<td>12.2R5</td>
<td>N.S.</td>
<td>12.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS Layer 3 VPNs</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
<tr>
<td>MPLS with RSVP-based label-switched paths (LSPs)</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td></td>
</tr>
</tbody>
</table>

Table 24: MPLS Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 3 subinterfaces as MPLS core interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12.2R1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routed VLAN interfaces (RVIs) as MPLS core</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path maximum transmission unit (MTU) and uncast</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.1R1</td>
</tr>
<tr>
<td>reverse-path forwarding (RPF) checks for VPNs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource Reservation Protocol—traffic engineering</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.1R1</td>
</tr>
<tr>
<td>(RSVP-TE)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standby secondary path protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12.1R1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static label-switched paths (LSPs)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: Layer 3 subinterfaces as MPLS core interfaces—For EX4500 and EX4550 switches to support Layer 3 subinterfaces as MPLS core interfaces, the peer switch that the Layer 3 subinterfaces connect to, must be an EX8200 switch.

IP over MPLS—The EX4500 and EX4550 switches do not support IP over MPLS (single MPLS label in the packet) when the switch is positioned as a non-penultimate-hop popping (non-PHP) switch.

Table 25: MPLS Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A separate software license is required for MPLS. See Understanding Software Licenses for EX Series Switches.
Table 25: MPLS Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass static LSPs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>LDP LSP action based on a BFD failure event</td>
<td>12.3R2</td>
</tr>
<tr>
<td>LDP downstream on demand</td>
<td>12.3R2</td>
</tr>
<tr>
<td>LDP, BGP, and VPLS interworking</td>
<td>12.3R2</td>
</tr>
<tr>
<td>P2MP LSP traceroute</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Static LSP:</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Revert timer</td>
<td></td>
</tr>
<tr>
<td>• Statistics</td>
<td></td>
</tr>
<tr>
<td>• Traceoptions</td>
<td></td>
</tr>
<tr>
<td>• At the ingress switch</td>
<td></td>
</tr>
<tr>
<td>• At the transit switch</td>
<td></td>
</tr>
<tr>
<td>Statistics for P2MP LSPs</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
### Table 26: Multicast Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP (Internet Group Management Protocol) version 1 (IGMPv1) and IGMPv2</td>
<td>11.1R1</td>
<td>9.0R2</td>
<td>12.1R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td>See Table 27 on page 59 for a list of EX9200 multicast features</td>
</tr>
<tr>
<td>IGMP filtering</td>
<td>11.3R1</td>
<td>9.5R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>11.3R1</td>
<td>11.3R1</td>
<td>11.3R1</td>
<td>9.5R1</td>
<td></td>
</tr>
<tr>
<td>IGMP snooping with RVIs or IRB interfaces</td>
<td>10.1R1</td>
<td>9.2R1</td>
<td>12.1R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>IGMPv3</td>
<td>11.1R1</td>
<td>9.3R2</td>
<td>12.1R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.6R1</td>
<td></td>
</tr>
<tr>
<td>IGMPv1 and IGMPv2 snooping</td>
<td>10.1R1</td>
<td>9.1R1</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>IGMPv3 snooping</td>
<td>10.1R1</td>
<td>9.6R1</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.6R1</td>
<td></td>
</tr>
<tr>
<td>Multicast Listener Discovery version 1 and 2 (MLDv1 and MLDv2)</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.2R1</td>
<td></td>
</tr>
<tr>
<td>Multicast Listener Discovery version 1 (MLDv1) snooping (MLDv1 snooping)</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td></td>
</tr>
<tr>
<td>Multicast Listener Discovery version 2 (MLDv2) snooping (MLDv2 snooping)</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td></td>
</tr>
<tr>
<td>Multicast Source Discovery Protocol (MSDP)</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>12.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

See the [Junos OS Multicast Protocols Configuration Guide](#).
### Table 26: Multicast Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Independent Multicast dense mode (PIM DM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>13.2X50-D10</td>
</tr>
<tr>
<td>See the <a href="#">Junos OS Multicast Protocols Configuration Guide</a>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Independent Multicast sparse mode (PIM SM)</td>
<td>11.1R1</td>
<td>9.0R2</td>
<td>12.1R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>See the <a href="#">Junos OS Multicast Protocols Configuration Guide</a>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Independent Multicast source-specific multicast (PIM SSM)</td>
<td>11.1R1</td>
<td>9.3R1</td>
<td>12.1R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>See the <a href="#">Junos OS Multicast Protocols Configuration Guide</a>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single-source multicast</td>
<td>N.S.</td>
<td>9.0R2</td>
<td>N.S.</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

### Table 27: Multicast Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD for PIM—IPv6</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BFD support for ECMP LSPs signaled using LDP</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Bidirectional PIM (RFC 5015)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Control of PIM resources for multicast VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Disable PIM for IPv6 only</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Dynamic reuse of data multicast distribution tree (MDT) group addresses</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Flexible configuration for IGMP or MLD static-join</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IGMPv3 and MLDv2 full support</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 27: Multicast Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP and MLD enhancements—</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• immediate-leave (IGMP and MLD)</td>
<td></td>
</tr>
<tr>
<td>• promiscuous-mode (IGMP only)</td>
<td></td>
</tr>
<tr>
<td>IGMP and PIM support for unnumbered interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IGMP join and leave recording for system or for specific interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IGMP and MLD source or group access lists and MLD join and leave recording</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IGMP and MLD support for dynamic interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Independently configurable loopback addresses for VRF VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Internet multicast using ingress replication provider tunnels</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Software support for configuring accept any-source multicast (ASM) join messages (*,G) for group addresses</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Software support for configuring a provider network to operate in source-specific multicast (SSM) mode</td>
<td>12.3R2</td>
</tr>
<tr>
<td>LDP signaling for point-to-multipoint LSPs in next-generation MBGP multicast VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Load-balancing PIM join messages on multicast VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Multicast flow maps</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) PIM for Draft-Rosen VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>PIM automatic make-before-break (MBB) join load balancing</td>
<td>12.3R2</td>
</tr>
<tr>
<td>PIM join load balancing</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Source-specific multicast (SSM)-map definition for different groups to different sources</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for filtering unwanted PIM neighbors</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for multicast output interface (OIF) mapping</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Translation of PIM join/prune messages to IGMP or MLD report/leave messages</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Turn off spanning-tree interface state in multicast snooping</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
### Table 28: Network Management and Monitoring Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1ag Ethernet OAM connectivity fault management (CFM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet frame delay measurement (ETH-DM, Y.1731)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet OAM link fault management (LFM—also known as Ethernet in the First Mile, EFM)</td>
<td>11.1R1</td>
<td>9.4R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.0R1</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Port mirroring enhancements</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>–</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
</tr>
<tr>
<td>• Layer 3 interface support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Multiple VLAN support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port mirroring enhancements</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>–</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>• For remote port mirroring, <strong>ingress</strong> and <strong>egress</strong> options on VLAN member interfaces on the intermediate (transit) switch to avoid flooding mirrored traffic to those interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See Table 29 on page 63 for a list of EX9200 network management and monitoring features.
<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port mirroring support for multiple analyzers per session</td>
<td>10.1R1</td>
<td>9.3R2</td>
<td>12.2R1</td>
<td>13.2X50-12.1R</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.1R1</td>
<td></td>
</tr>
<tr>
<td>Real-time performance monitoring (RPM)</td>
<td>N.S.</td>
<td>10.3R1</td>
<td>12.2R1</td>
<td>13.2X50-12.1R</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.3R1</td>
<td></td>
</tr>
<tr>
<td>Real-time performance monitoring (RPM)—hardware timestamps with RVIs or IRB interfaces</td>
<td>10.3R1</td>
<td>10.3R1</td>
<td>12.2R1</td>
<td>13.2X50-11.1R</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.3R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time performance monitoring (RPM)—client and server on same interface</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1 (EX4200 only)</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td></td>
</tr>
<tr>
<td>Routing Engine Software Development Kit (SDK)</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1 (EX4200 only)</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td></td>
</tr>
<tr>
<td>RMON</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-10.2R</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sFlow monitoring technology</td>
<td>11.1R1</td>
<td>9.3R2</td>
<td>12.1R1</td>
<td>13.2X50-11.2R</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.0R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sFlow monitoring technology—Persistent IP addresses for agent IDs and use in datagrams</td>
<td>11.1R1</td>
<td>10.2R1</td>
<td>N.S.</td>
<td>13.2X50-11.2R</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>10.2R1</td>
<td></td>
</tr>
<tr>
<td>Simple Network Management Protocol version 1 (SNMPv1), SNMPv2, and SNMPv3</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50-10.2R</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
### Table 28: Network Management and Monitoring Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uplink failure detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>13.2X50</td>
<td>- D10</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 29: Network Management and Monitoring Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junos OS XML API and scripting—NETCONF Java toolkit for rapid development of Java applications to manage devices running Junos OS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Junos OS XML API and scripting—NETCONF Perl client installation—Supports loading prerequisites from Comprehensive Perl Archive Network (CPAN) global repository</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Junos OS XML API and scripting—NETCONF tracing operations</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Junos OS XML API and scripting:</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Dedicated directory for user script library</td>
<td></td>
</tr>
<tr>
<td>• Global variable provided to Junos OS automation scripts</td>
<td></td>
</tr>
<tr>
<td>• References to a correlating event in a policy action</td>
<td></td>
</tr>
<tr>
<td>• Trigger a policy based on the event count</td>
<td></td>
</tr>
<tr>
<td>• Unique filenames for uploaded files</td>
<td></td>
</tr>
<tr>
<td>• Upload files created by event scripts</td>
<td></td>
</tr>
<tr>
<td>• XML schemata for Junos OS XML operational tag elements</td>
<td></td>
</tr>
<tr>
<td>• jcs:open() extension function support for routing instances</td>
<td></td>
</tr>
<tr>
<td>Configuration options to filter out interfaces from SNMP Get and GetNext operations</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Enhanced SNMP support for logical switches and routing instances</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Generating SNMP traps when MAC address table is full</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Junos OS MIB support for VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>MIB support for VRF route entries</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Proxy SNMP agent</td>
<td>12.3R2</td>
</tr>
<tr>
<td>SNMP MIB support for OSPFv3</td>
<td>12.3R2</td>
</tr>
<tr>
<td>SNMP poll and trap support for DHCP leases</td>
<td>12.3R2</td>
</tr>
<tr>
<td>SNMP support for the DHCP bindings table</td>
<td>12.3R2</td>
</tr>
<tr>
<td>SNMP support for the authd daemon and for radius-acc-server-mib and radius-auth-server-mib</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 29: Network Management and Monitoring Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP support for spanning-tree protocols</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for Internet draft draft-ietf-bfd-mib-02.txt—MIB for BFD liveness detection</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for MIB objects in accounting profiles</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for an enterprise-specific event MIB (mib-jnx-event.txt)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for sending traps over routing instances</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for adding lists of clients to the SNMP community</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for the enterprise-specific Packet Forwarding Engine MIB (mib-jnx-pfe.txt)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for the pimNeighborLoss trap</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for trap spoofing</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IEEE 802.3ah link fault management (LFM) for Ethernet OAM (also known as Ethernet in the First Mile, or EFM)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Port mirroring of Layer 2 VLAN and VPLS traffic</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for native analyzers and remote port-mirroring capabilities</td>
<td>13.2R1</td>
</tr>
<tr>
<td>Fast update filters for dynamic profiles</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Flow aggregation to multiple collectors</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IPv6 flow aggregation templates</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Inline flow monitoring</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

Table 30: Port Security Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic recovery for port error disable conditions</td>
<td>10.1R1</td>
<td>9.6R1</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.0R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>DHCP option 82</td>
<td>10.1R1</td>
<td>9.3R2</td>
<td>11.3R1</td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 30: Port Security Features on Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP snooping</td>
<td>10.1R</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
</tr>
<tr>
<td>Dynamic ARP inspection (DAI)</td>
<td>10.1R</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
</tr>
<tr>
<td>IP source guard</td>
<td>10.1R</td>
<td>9.2R1</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
</tr>
<tr>
<td>Layer 3 virtual private network (VPN) for IPv4 (RFC 2547 and 4364)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 3 virtual private network (VPN) for IPv6 through IPv4 MPLS</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R2</td>
</tr>
<tr>
<td>MAC limiting</td>
<td>10.1R</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>MAC address limit per port</td>
<td>10.1R</td>
<td>9.0R1</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
</tr>
<tr>
<td>MAC limiting per port and per VLAN (VLAN membership MAC limit)</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R2</td>
</tr>
<tr>
<td>MAC move limiting</td>
<td>10.1R</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R2</td>
<td>N.S.</td>
</tr>
<tr>
<td>Persistent MAC learning (sticky MAC)</td>
<td>11.4R</td>
<td>11.4R</td>
<td>12.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>11.4R1</td>
<td>12.2R1</td>
<td>11.4R1</td>
<td>11.4R1</td>
</tr>
<tr>
<td>Persistent storage for DHCP snooping</td>
<td>10.1R</td>
<td>9.4R1</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>10.3R1</td>
</tr>
<tr>
<td>Self-signed digital certificates for enabling SSL services</td>
<td>11.1R</td>
<td>11.1R</td>
<td>N.S.</td>
<td></td>
<td>13.2X50-D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Static ARP support</td>
<td>10.1R</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td></td>
<td>13.2X50-D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>Feature</td>
<td>EX2200</td>
<td>EX3200, EX4200</td>
<td>EX3300</td>
<td>EX4300</td>
<td>EX4500</td>
<td>EX4550</td>
<td>EX6200</td>
<td>EX8200</td>
<td>EX9200</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>----------------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP) with granular Power over Ethernet (PoE) management</td>
<td>12.2R1</td>
<td>12.2R1 (EX4200-24PX and EX4200-48PX models only)</td>
<td>12.2R1</td>
<td>13.2X50-D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
</tr>
</tbody>
</table>

**NOTE:** EX4200 switches must be running PoE controller software firmware version 4.04 or later to support the Link Layer Discovery Protocol (LLDP) with granular Power over Ethernet (PoE) management feature. See `show chassis firmware detail` and `request system firmware upgrade poe` to check or upgrade this firmware.

| Power over Ethernet (PoE) | 10.1R1 | 9.0R2 | 11.3R1 | 13.2X50-D10 | – | – | 11.3R2 | 11.2R1 | N.S. |

| Power over Ethernet Plus (PoE+) | 10.3R1 | 11.2R1 (EX4200-24PX and EX4200-48PX models only) | 11.3R1 | 13.2X50-D10 | – | – | 11.3R2 | 11.2R1 | N.S. |

| Power over Ethernet (PoE) power management mode | 10.1R1 | 9.3R2 | 11.3R1 | 13.2X50-D10 | – | – | 11.3R2 | 11.2R1 | N.S. |
Table 32: Routing Policy and Packet Filtering Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic allocation of TCAM memory to firewall filters</td>
<td>10.1R1</td>
<td>10.0R1</td>
<td>11.3R1</td>
<td>–</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.3R1</td>
<td></td>
</tr>
<tr>
<td>Firewalls filters and rate limiting</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
</tbody>
</table>

For a list of supported firewall filter match conditions and actions, see “Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 4111.

<table>
<thead>
<tr>
<th>Firewall filters on LAGs</th>
<th>10.1R1</th>
<th>9.0R2</th>
<th>11.3R1</th>
<th>13.2X50 - D10</th>
<th>10.2R1</th>
<th>12.2R1</th>
<th>N.S.</th>
<th>10.0R1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall filters on the loopback interface</td>
<td>10.1R1</td>
<td>9.2R1</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.6R1</td>
</tr>
</tbody>
</table>

For a list of supported firewall filter match conditions and actions on a loopback interface, see “Support for Match Conditions and Actions for Loopback Firewall Filters on Switches” on page 4107.

<table>
<thead>
<tr>
<th>Firewall filters on the management interface</th>
<th>11.3R1</th>
<th>10.4R1</th>
<th>N.S.</th>
<th>13.2X50 - D10</th>
<th>10.4R1</th>
<th>12.2R1</th>
<th>12.1R1</th>
<th>10.4R1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall filters on the virtual management interface</td>
<td>–</td>
<td>10.4R1 (EX4200 Virtual Chassis only)</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Firewall filters with IPv6</th>
<th>11.3R1</th>
<th>10.1R1</th>
<th>12.3R1</th>
<th>13.2X50 - D10</th>
<th>12.1R1</th>
<th>12.2R1</th>
<th>12.1R1</th>
<th>10.3R1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policing</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
</tr>
<tr>
<td>Tricolor marking policers</td>
<td>11.2R1</td>
<td>11.2R1</td>
<td>11.4R8</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>N.S.</td>
</tr>
</tbody>
</table>

Table 33: Routing Policy and Firewall Filters on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access and access-internal routes</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Extension of numeric-range match conditions in firewall filters</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Aggregate policer support for different family address types configured on the same interface</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 33: Routing Policy and Firewall Filters on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication for BFD (MD5/SHA1)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BGP multipath link-bandwidth attribute</td>
<td>12.3R2</td>
</tr>
<tr>
<td>DHCP state persistence for DHCP relay agent</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Dynamic configuration support for routing policies</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Extended DHCP relay agent</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Filter-based forwarding to a specific outgoing interface or destination IP address</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Firewall filters within logical systems</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IEEE 802.1p priority match conditions for Layer 2 VPN firewall filters</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Filter-based forwarding to a specific outgoing interface or destination IP address</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 Gigabit Ethernet logical interface extended policing support</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 support for firewall filter match conditions</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Load balancing of VPLS traffic</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Option 60 support for extended DHCP relay agents</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Policers on physical interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Firewall filters feature support</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for policers that limit traffic on logical interfaces in ingress or egress directions</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for policers that rate-limit based on a percentage of physical port speed on an interface</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for the discard action for tricolor marking policers applied to firewall filters</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for the prefix-list match condition for firewall filters for the VPLS protocol family</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for enhanced policer statistics</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for MAC address validation</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Tricolor marking policers</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
## Table 34: Spanning-Tree Protocols Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPDU protection for spanning-tree protocols</td>
<td>10.1R1</td>
<td>9.1R1</td>
<td>11.3R1</td>
<td>13.2X50- D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>BPDU filter</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>13.2X50- D10</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td></td>
</tr>
<tr>
<td>Distributed periodic packet management (PPM) for Spanning Tree Protocols</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td></td>
</tr>
<tr>
<td>Loop protection for spanning-tree protocols</td>
<td>10.1R1</td>
<td>9.1R1</td>
<td>11.3R1</td>
<td>13.2X50- D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Root protection for spanning-tree protocols</td>
<td>10.1R1</td>
<td>9.1R1</td>
<td>11.3R1</td>
<td>13.2X50- D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Spanning tree:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• RSTP and VSTP concurrent configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanning tree:</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50- D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>• Spanning Tree Protocol (STP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Rapid Spanning Tree Protocol (RSTP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Multiple Spanning Tree Protocol (MSTP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanning tree:</td>
<td>10.1R1</td>
<td>9.4R1</td>
<td>11.3R1</td>
<td>13.2X50- D10</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.6R1</td>
<td></td>
</tr>
<tr>
<td>• VLAN Spanning Tree Protocol (VSTP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See Table 35 on page 70 for a list of EX9200 spanning-tree protocols features.
Table 35: Spanning-Tree Protocols Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning tree:</td>
<td>12.3R2</td>
</tr>
<tr>
<td>• Spanning Tree Protocol (STP)</td>
<td></td>
</tr>
<tr>
<td>• Rapid Spanning Tree Protocol (RSTP)</td>
<td></td>
</tr>
<tr>
<td>• Multiple Spanning Tree Protocol (MSTP)</td>
<td></td>
</tr>
<tr>
<td>• VLAN Spanning Tree Protocol (VSTP)</td>
<td></td>
</tr>
<tr>
<td>Root protection for spanning-tree protocols</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Loop protection for spanning-tree protocols</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Distributed periodic packet management (PPM) for Spanning Tree Protocols</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BPDU filter</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
### Table 36: System Management Features on Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX4550</th>
<th>EX6200</th>
<th>EX8200</th>
<th>EX9200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoinstallation of configuration files</td>
<td>10.1R1</td>
<td>9.4R1</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>Automatic software download</td>
<td>10.1R1</td>
<td>9.6R1</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.6R1</td>
<td></td>
</tr>
<tr>
<td>Automatic repair of corrupted partition when booting from alternate partition</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration rollback</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>11.3R1</td>
<td>13.2X50</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R2</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Zero Touch Provisioning (EZ Touchless Provisioning using DHCP)</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R5</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td></td>
</tr>
<tr>
<td>J-Web interface, for switch configuration and management</td>
<td>10.1R1</td>
<td>9.0R2</td>
<td>12.1R1</td>
<td>13.2X50</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>(12.1R1 for EX2200-C switches)</td>
<td>12.1R1</td>
<td>12.3R1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Junos Space Service Now support</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCD panel management support</td>
<td>–</td>
<td>9.0R1</td>
<td>11.3R1</td>
<td>13.2X50</td>
<td>10.2R1</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td></td>
</tr>
<tr>
<td>Online insertion and removal (OIR) of uplink modules</td>
<td>–</td>
<td>10.0R1</td>
<td>–</td>
<td>13.2X50</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>–</td>
<td>–</td>
<td></td>
</tr>
</tbody>
</table>

See Table 37 on page 71 for a list of EX9200 system management features.

### Table 37: System Management Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration rollback</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
### Table 38: User Interface and Configuration Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device-initiated SSH connection (outbound SSH)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Dynamic IPv6 filters</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Dynamic configuration of the switch advertisement protocol</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Dynamic profiles support by extended DHCP local server and extended DHCP relay agent</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Enhanced IPv6 statistics</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Extended DHCP local server</td>
<td>12.3R2</td>
</tr>
<tr>
<td>IGMP dynamic profiles</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Extended DHCP local server</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Protection for device configuration</td>
<td>12.3R2</td>
</tr>
<tr>
<td>RADIUS MSCHAPv2 protocol support for administrator authentication, password aging, and update</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Limit configuration command output</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Remote tracing</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for CLI edit mode wildcard range</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for configuring ARP aging time for a logical interface</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for configuring a proxy server for downloading licenses</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for configuring time-based user access</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for logical router system administrators</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

### Table 39: VPN Features on EX9200 Switches by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Ethernet interfaces for VPLS routing instances</td>
<td>12.3R2</td>
</tr>
<tr>
<td>BGP autodiscovery for LDP VPLS (FEC 129)</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Clearing MAC addresses for better convergence</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Configurable label block sizes for VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Disable TTL propagation behavior for the routes in a VRF routing instance</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
### Table 39: VPN Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXP-based traffic classification for VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Enhanced show interface command for Layer 3 VPN functionality</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Expanded interface support for the vrf-table-label statement</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Extranet next-generation MVPN GRE tunnels for Layer 3 VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>GRE tunnels for Layer 3 VPNs ignore MTU mismatch on Layer 2 circuits</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Integrated routing and bridging support for inter-AS VPLS between BGP-signaled VPLS and LDP-signaled VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>LDP-based VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Label allocation and substitution policy</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 2 VPN multihoming</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 3 VPN BGP routes and labels</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Layer 3 VPN localization</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Load balancing and IP header filtering for Layer 3 VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Local switching support for the ignore-encapsulation-mismatch statement</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Multipath load balancing for EBGP and IBGP VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Multiple logical trunk interfaces per physical interface</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Multiprotocol BGP-based multicast VPN</td>
<td>12.3R2</td>
</tr>
<tr>
<td>NTP support for IPv4 VRF and IPv6 VRF</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Nonstop active routing support for Layer 3 VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>PIM source-specific multicast (PIM-SSM) provider tunnel support added to Multiprotocol BGP-based multicast VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Point-to-multipoint LSP support for VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Point-to-multipoint LSP support for multicast VPNs</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>
Table 39: VPN Features on EX9200 Switches by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy BGP route target filtering</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Static VPLS</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Static route target filtering</td>
<td>12.3R2</td>
</tr>
<tr>
<td>Support for autorp, BSR, PIM dense mode and mtrace for next-generation multicast VPNs</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VLAN range for Layer 2 VPN</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VPLS automatic site ID</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VPLS automatic site ID for nonstop active routing</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VPLS ping</td>
<td>12.3R2</td>
</tr>
<tr>
<td>VPLS trunk interfaces</td>
<td>12.3R2</td>
</tr>
<tr>
<td>eBGP and iBGP load-balancing support for MVPN and PIM</td>
<td>12.3R2</td>
</tr>
</tbody>
</table>

**Related Documentation**
- EX Series Virtual Chassis Software Features Overview on page 75
- EX2200 Switches Hardware Overview
- EX3200 Switches Hardware Overview
- EX3300 Switches Hardware Overview
- EX4200 Switches Hardware Overview
- <will add topic-ref to EX4300 HW overview topic>
- EX4500 Switches Hardware Overview
- EX4550 Switches Hardware Overview
- EX6210 Switch Hardware Overview
- EX8208 Switch Hardware Overview
- EX8216 Switch Hardware Overview
- EX9204 Switch Hardware Overview
- EX9208 Switch Hardware Overview
- EX9214 Switch Hardware Overview
- Line Card Model and Version Compatibility in an EX6200 Switch
- Line Card Model and Version Compatibility in an EX8200 Switch
- Line Card Model and Version Compatibility in an EX9200 Switch
EX Series Virtual Chassis Software Features Overview

This topic lists the Juniper Networks EX Series Virtual Chassis software features, the Juniper Networks Junos operating system (Junos OS) release in which they were introduced, and the first Junos OS release for each Virtual Chassis.

NOTE: For information on software features for standalone Juniper Networks EX Series Ethernet Switches, see “EX Series Switch Software Features Overview” on page 27.

NOTE: In all tables in this topic, “N.S.” = “Not supported”, and “–” = “Not applicable”.

- Table 5 on page 28—First Junos OS Release for Each EX Series Virtual Chassis
- Table 6 on page 29—Access Control Features
- Table 7 on page 30—Administration Features
- Table 8 on page 31—Class-of-Service (CoS) Features
- Table 10 on page 34—Converged Networks (LAN and SAN) Features
- Table 11 on page 34—Device Security Features
- Table 12 on page 35—High Availability and Resiliency Features
- Table 14 on page 39—Interfaces Features
- Table 16 on page 41—IP Address Management Features
- Table 18 on page 42—IPv6 Features
- Table 19 on page 45—Layer 2 Network Protocols Features
- Table 21 on page 48—Layer 3 Protocols Features
- Table 24 on page 53—MPLS Features
- Table 26 on page 58—Multicast Features
- Table 28 on page 61—Network Management and Monitoring Features
- Table 30 on page 64—Port Security Features
- Table 31 on page 66—Power over Ethernet (PoE) Features
- Table 32 on page 67—Routing Policy and Packet Filtering Features
- Table 34 on page 69—Spanning-Tree Protocols Features
### Table 40: First Junos OS Release for Each EX Series Virtual Chassis

<table>
<thead>
<tr>
<th>Virtual Chassis</th>
<th>Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200 Virtual Chassis</td>
<td>Junos OS Release 12.2R1</td>
</tr>
<tr>
<td>EX3300 Virtual Chassis</td>
<td>Junos OS Release 11.3R1</td>
</tr>
<tr>
<td>EX4200 Virtual Chassis</td>
<td>Junos OS Release 9.0R1</td>
</tr>
<tr>
<td>EX4300 Virtual Chassis</td>
<td>Junos OS Release 13.2X50 - D10</td>
</tr>
<tr>
<td>EX4500 Virtual Chassis</td>
<td>Junos OS Release 11.1R1</td>
</tr>
<tr>
<td>EX4550 Virtual Chassis</td>
<td>Junos OS Release 12.2R1</td>
</tr>
<tr>
<td>Mixed EX4200 and EX4500 Virtual Chassis</td>
<td>Junos OS Release 11.1R1</td>
</tr>
<tr>
<td>Mixed EX4200 and EX4550 Virtual Chassis</td>
<td>Junos OS Release 12.2R1</td>
</tr>
<tr>
<td>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</td>
<td>Junos OS Release 12.2R1</td>
</tr>
<tr>
<td>Mixed EX4500 and EX4550 Virtual Chassis</td>
<td>Junos OS Release 12.2R1</td>
</tr>
<tr>
<td>EX8200 Virtual Chassis</td>
<td>Junos OS Release 10.4R1</td>
</tr>
</tbody>
</table>

**NOTE:** A mixed Virtual Chassis generally supports the same feature set regardless of the different combinations of EX4200, EX4500, and EX4550 member switches in the Virtual Chassis and regardless of which member switches are configured in which roles. The supported features for a mixed Virtual Chassis are indicated in the “Mixed EX4200, EX4500, and EX4550” column.

If a software feature only runs on a specific mixed Virtual Chassis, the “Mixed EX4200, EX4500, and EX4550” column entry for that software feature includes a note clarifying the supported mixed Virtual Chassis for that feature.
<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X authentication (port-based, multiple supplicant)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>802.1X authentication with authentication bypass</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>802.1X authentication with VLAN assignment, VoIP VLAN support</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>802.1X user-based dynamic firewall filters</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>802.1X user-based dynamic firewall filters on multiple-suppliant ports</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.5R2</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>802.1X per-user statistics</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Authentication fallback</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>10.3R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Captive portal authentication for Layer 3 interfaces</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>10.1R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Captive portal authentication for Layer 2 interfaces</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>10.3R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Energy Efficient Ethernet (EEE)</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
</tr>
<tr>
<td>Infranet Enforcer as an external captive-portal server</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
</tr>
<tr>
<td>MAC RADIUS authentication</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>NetBIOS snooping</td>
<td>12.2R1</td>
<td>11.3R5</td>
<td>11.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Server fail fallback</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
</tr>
</tbody>
</table>
### Table 42: Administration Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>System logging (syslog) over IPv4</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>System logging (syslog) over IPv6</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>System snapshot</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
</tbody>
</table>

### Table 43: Class-of-Service (CoS) Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class of service (CoS)—Class-based queueing with prioritization, Layer 2 and Layer 3 classification, rewrite, and queuing; strict priority queuing on egress</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>CoS—DSCP, IEEE 802.1p, and IP precedence packet rewrites on RVIs and IRB interfaces</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>CoS—Interface-specific classifiers on RVIs and IRB interfaces</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>CoS—Multidestination</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>11.1R1</td>
</tr>
<tr>
<td>CoS—Per-interface classification</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>9.3R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Feature</td>
<td>EX2200 Virtual Chassis</td>
<td>EX3300 Virtual Chassis</td>
<td>EX4200 Virtual Chassis</td>
<td>EX4300 Virtual Chassis</td>
<td>EX4500 Virtual Chassis</td>
<td>EX4550 Virtual Chassis</td>
<td>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</td>
<td>EX8200 Virtual Chassis</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>CoS support on link aggregation groups (LAGs)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>CoS support on RVIs and IRB interfaces</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>DSCP setting on ingress interface</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Flexible CoS-outer 802.1p marking</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.6R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Interface-specific CoS rewrite rules</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Junos EZQoS for CoS</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Port shaping and queue shaping</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Re-marking of bridged packets</td>
<td>11.2R1</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Shaped-deficit weighted round-robin (SDWRR)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Single-rate two-color marking</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
</tbody>
</table>
Table 44: Converged Networks (LAN and SAN) Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE: The EX4500 Virtual Chassis that support Fibre Channel over Ethernet features must be Converged Enhanced Ethernet (CEE) capable. The CEE-capable EX4500 Virtual Chassis must be composed of switches that have a “–C” in the hardware model number. See EX4500 Switch Models.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Center Bridging Capability Exchange protocol (DCBX)fool</th>
<th>N.S.</th>
<th>N.S.</th>
<th>N.S.</th>
<th>N.S.</th>
<th>11.3R1</th>
<th>12.2R1</th>
<th>N.S.</th>
<th>N.S.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCBX application protocol TLV exchange</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>FIP snooping</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Priority-based flow control (PFC)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
</tbody>
</table>

Table 45: Device Security Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic recovery for port error disable conditions</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.6R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Storm control (broadcast and unicast)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.1R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Storm control (multicast)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>10.3R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Unknown Layer 2 unicast forwarding</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.1R1</td>
</tr>
</tbody>
</table>
### Table 46: High Availability and Resiliency Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful protocol restart for BGP</td>
<td>–</td>
<td>N.S.</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Graceful protocol restart for IS-IS</td>
<td>–</td>
<td>N.S.</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Graceful protocol restart for OSPF</td>
<td>–</td>
<td>N.S.</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Graceful protocol restart for RSVP and LDP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.3R1</td>
</tr>
<tr>
<td>GRES for ARP entries, forwarding database, and Layer 3 protocols</td>
<td>–</td>
<td>11.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>GRES for IGMP snooping</td>
<td>–</td>
<td>12.1R1</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>11.4R1</td>
<td>12.2R1</td>
<td>11.4R1</td>
<td>11.3R1</td>
</tr>
<tr>
<td>GRES for LACP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>13.2X50 - D10</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>11.3R1</td>
</tr>
<tr>
<td>GRES for Layer 2 and Layer 3 VPN LSPs</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.3R1</td>
</tr>
<tr>
<td>GRES for port security (DHCP snooping, DAI, and IP source guard)</td>
<td>–</td>
<td>N.S.</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>LACP support for dual-homing applications in data centers</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Link Aggregation Control Protocol (LACP)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Link aggregation groups (LAGs)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
</tbody>
</table>
Table 46: High Availability and Resiliency Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonstop active routing (NSR) for BGP with BFD, IS-IS with BFD, IGMP with BFD, and RIP with BFD</td>
<td>–</td>
<td>12.1R1</td>
<td>11.1R1</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for IPv6 IS-IS with BFD, RIPng with BFD, and OSPFv3 with BFD</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>11.3R1</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for OSPFv2</td>
<td>–</td>
<td>12.1R1</td>
<td>11.1R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for Protocol Independent Multicast (PIM)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>11.4R2</td>
</tr>
<tr>
<td>Nonstop active routing (NSR) for RSVP and LDP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Nonstop bridging (NSB) for LAGs and LACP</td>
<td>–</td>
<td>12.2R1</td>
<td>11.4R1</td>
<td>N.S.</td>
<td>11.4R1</td>
<td>12.2R1</td>
<td>11.4R1</td>
<td>11.3R1</td>
</tr>
<tr>
<td>Nonstop bridging (NSB) for LLDP and LLDP-MED</td>
<td>–</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.3R1</td>
</tr>
<tr>
<td>Nonstop bridging (NSB) for spanning-tree protocols</td>
<td>–</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Nonstop software upgrade (NSSU)</td>
<td>–</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Power budget management</td>
<td>–</td>
<td>N.S.</td>
<td>–</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
</tbody>
</table>
Table 46: High Availability and Resiliency Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Router—Network Time Protocol (NTP), system logging, Simple Network Management Protocol (SNMP), RADIUS, and TACACS support in a virtual router</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol (VRRP)</td>
<td>12.3R1</td>
<td>12.1R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol (VRRP)—Support for multiple VRRP owners per physical interface</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Virtual Router Redundancy Protocol (VRRP) for IPv6 (except authentication type and authentication key)</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>10.2R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>

Table 47: Interfaces Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital optical monitoring (DOM)</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Interface ranges</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Feature</td>
<td>EX2200 Virtual Chassis</td>
<td>EX3300 Virtual Chassis</td>
<td>EX4200 Virtual Chassis</td>
<td>EX4300 Virtual Chassis</td>
<td>EX4500 Virtual Chassis</td>
<td>EX4550 Virtual Chassis</td>
<td>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>IPv4 over generic routing encapsulation (GRE) tunnels—encapsulation support</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>IPv4 over generic routing encapsulation (GRE) tunnels—de-encapsulation support</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>IPv6 over generic routing encapsulation (GRE) tunnels using IPv4 transport—encapsulation support</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>IPv6 over generic routing encapsulation (GRE) tunnels using IPv4 transport—de-encapsulation support</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>IP directed broadcast</td>
<td>11.3R1</td>
<td>12.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Time domain reflectometry (TDR)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Unicast reverse-path forwarding (RPF)</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>VLAN-tagged Layer 3 subinterfaces</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>
### Table 48: IP Address Management Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>EX8200 Mixed Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP server and relay with option 82 for Layer 2 VLANs</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>N.S.</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>DHCP server and relay with option 82 for Layer 3 interfaces</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>DNS for IPv6</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Local DHCP server</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Virtual router aware DHCP (VR-aware DHCP)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Virtual router aware DHCPv6 (VR-aware DHCPv6)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Static addresses</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.1R1</td>
</tr>
</tbody>
</table>

### Table 49: IPv6 Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>EX8200 Mixed Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD for IPv6</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>BGP for IPv6</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>

**NOTE:** A separate software license is required for IPv6. See [Understanding Software Licenses for EX Series Switches](#).
### Table 49: IPv6 Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 CoS (multifield classification and rewrite)</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>10.2R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.3R1</td>
</tr>
<tr>
<td>IPv6 management</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>IPv6 multicast protocols (PIM, MLDv1/v2)</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>10.1R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>IPv6 neighbor redirect compliance with RFC 4861</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>IPv6 path MTU discovery</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>9.3R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>IS-IS for IPv6</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>MBGP for IPv6</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.3R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>OSPFv3</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.3R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>RFC 4291 Compliance</td>
<td>12.3R1</td>
<td>See note at end of table</td>
<td>See note at end of table</td>
<td>See note at end of table</td>
<td>N.S.</td>
<td>See note at end of table</td>
<td>See note at end of table</td>
<td>See note at end of table</td>
</tr>
<tr>
<td>RIPIg</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.3R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>VRRPv3 (RFC 5798 Compliance, ability to send SNMP traps)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
</tbody>
</table>
NOTE: Compliance with RFC 4291

EX Series switches drop the following types of illegal IPv6 packets:

- Packets that have a link-local source or destination address. Because link-local addresses are intended to be used for addressing only on a single link, EX Series switches do not forward any packets with such addresses to other links.
- Packets with the IPv6 unspecified source address 0:0:0:0:0:0:0:0.
- Packets that are to be sent outside a node but have the IPv6 loopback address 0:0:0:0:0:0:0:1 as the source address. When IPv6 packets are received on an interface, EX Series switches drop packets that have the loopback address as the destination address.

EX Series switches do not support Subnet-Router Anycast address.

Table 50: Layer 2 Network Protocols Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q VLAN tagging</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Edge virtual bridging (EVB) support with virtual Ethernet port aggregator (VEPA)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Ethernet ring protection switching (ERPS, G.8032/Y.1344)</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>12.1R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Layer 2 protocol tunneling (L2PT)</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) with voice over IP (VoIP) integration</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
</tbody>
</table>
### Table 50: Layer 2 Network Protocols Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC-based VLANs</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Multiple VLAN Registration Protocol (MVRP, IEEE 802.1ak)</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Private VLANs (PVLANs)</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.3R2</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Private VLANs (PVLANs) support across switches</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>10.4R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Proxy ARP—Restricted</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Proxy ARP—Unrestricted</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.6R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Proxy ARP per VLAN</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Q-in-Q tunneling</td>
<td>12.2R1</td>
<td>11.4R1</td>
<td>9.3R2</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Q-in-Q VLAN extended support for multiple S-VLANs per access interface, firewall-filter-based VLAN assignment, and RVIs and IRB interfaces</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.6R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Redundant trunk groups</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>RVIs and IRB interfaces</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>VLAN ID translation</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>
### Table 50: Layer 2 Network Protocols Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ranges</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.4R1</td>
</tr>
</tbody>
</table>

### Table 51: Layer 3 Protocols Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidirectional Forwarding Detection (BFD)</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Border Gateway Protocol (BGP)</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Multiprotocol Border Gateway Protocol (MBGP)</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.3R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>12.1R1</td>
</tr>
</tbody>
</table>

A separate software license is required for BGP and MBGP. See **Understanding Software Licenses for EX Series Switches**.

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed periodic packet management (PPM) with BFD</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.4R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Distributed periodic packet management (PPM) with LACP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.2R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Filter-based forwarding</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Filter-based forwarding over IPv6</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>
### Table 51: Layer 3 Protocols Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intermediate System-to-Intermediate System (IS-IS)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td><strong>A separate software license is required for IS-IS. See Understanding Software Licenses for EX Series Switches.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Layer 3 multicast protocols</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Jumbo frames on RVIs and IRB interfaces</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>OSPF Multitopology Routing (MT-OSPF)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td><strong>See the Junos OS Routing Protocols Configuration Guide.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSPFv2</td>
<td>12.2R1</td>
<td>11.4R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>OSPFv3 IPSec support</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.3R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Routing Information Protocol version 1 (RIPv1) and RIPv2</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Static routes</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Virtual routing and forwarding (VRF) with IPv4—Virtual routing instances</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>VRF with IPv4—Virtual routing instances for PIM and IGMP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>
Table 51: Layer 3 Protocols Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF with IPv4—Virtual routing instances for IGMP snooping</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.4R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.3R1</td>
</tr>
<tr>
<td>VRF with IPv6—Virtual routing instances for multicast traffic</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>VRF with IPv6—Virtual routing instances for unicast traffic</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>10.1R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>

Table 52: MPLS Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Ethernet interfaces (LAGs) on circuit cross-connects (CCCs)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>BFD for an LDP-based LSP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
</tr>
<tr>
<td>BFD for an RSVP-based LSP</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
</tr>
<tr>
<td>CCC between 2 interfaces in the same switch</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
</tbody>
</table>

A separate software license is required for MPLS. See Understanding Software Licenses for EX Series Switches.
Table 52: MPLS Features by Junos OS Release  
(continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interior gateway protocol (IGP) IS-IS and OSPF shortcuts</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>IP over MPLS</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>IPv6 over MPLS label-switched paths (LSPs)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>LDP-based MPLS</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>LDP tunneling (LDP over RSVP)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS-based circuit cross-connects (CCC)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS label-switched router (LSR) support</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS Layer 2 CCC on Ethernet-encapsulated interfaces (RFC 6624)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS Layer 2 CCC on VLAN-encapsulated interfaces (RFC 4905)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
</tbody>
</table>

See Note at end of table
Table 52: MPLS Features by Junos OS Release *(continued)*

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Layer 2 VLAN CCC on Ethernet-encapsulated interfaces (RFC 6624)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS Layer 2 VLAN CCC on VLAN-encapsulated interfaces (RFC 4905)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS Layer 2 VPN over CCC</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS Layer 2 VPN over VLAN CCC</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS OAM-LSP ping</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS over untagged Layer 3 interfaces</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS with class of service (CoS)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>12.2R5</td>
<td>12.2R5</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS with Layer 3 VPNs—Includes support for RVIs on customer-edge interfaces</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>MPLS with RSVP-based label-switched paths (LSPs)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Layer 3 subinterfaces as MPLS core interfaces</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
</tbody>
</table>

See Note at end of table.
Table 52: MPLS Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>RVIs and IRB interfaces as MPLS core interfaces</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Path maximum transmission unit (MTU) and unicast reverse-path forwarding (RPF) checks for VPNs</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Resource Reservation Protocol—traffic engineering (RSVP-TE)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Standby secondary path protection</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Static label-switched paths (LSPs)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Layer 3 subinterfaces as MPLS core interfaces—For EX4500 and EX4550 switches to support Layer 3 subinterfaces as MPLS core interfaces, the peer switch that the Layer 3 subinterfaces connect to, must be an EX8200 switch.

IP over MPLS—The EX4500 and EX4550 switches do not support IP over MPLS (single MPLS label in the packet) when the switch is positioned as a non-penultimate-hop popping (non-PHP) switch.
Table 53: Multicast Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP (Internet Group Management Protocol) version 1 (IGMPv1) and IGMPv2</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>IGMP filtering</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>9.5R1</td>
<td>13.2X50 - D10</td>
<td>11.3R1</td>
<td>11.3R1</td>
<td>11.3R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>IGMP Snooping with RVIs and IRB interfaces</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>IGMPv3</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>IGMPv1 and IGMPv2 Snooping</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.1R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>IGMPv3 Snooping</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.6R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Multicast Listener Discovery version 1 and 2 (MLDv1 and MLDv2)</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.1R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Multicast Listener Discovery version 1 (MLDv1) snooping (MLDv1 snooping)</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Multicast Listener Discovery version 2 (MLDv2) snooping (MLDv2 snooping)</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Multicast Source Discovery Protocol (MSDP)</td>
<td>N.S.</td>
<td>12.1R2</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>See the <em>Junos OS Multicast Protocols Configuration Guide</em>.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast VLAN registration (MVR)</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.6R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
</tbody>
</table>
Table 53: Multicast Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Independent Multicast dense mode (PIM DM)</td>
<td>11.2R1</td>
<td>12.1R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>11.1R1</td>
</tr>
</tbody>
</table>

See the [Junos OS Multicast Protocols Configuration Guide](#).

| Protocol Independent Multicast sparse mode (PIM SM) | 12.2R1 | 12.1R1 | 9.0R2 | 13.2X50 - D10 | 11.1R1 | 12.2R1 | 11.1R1 | 11.1R1 |

See the [Junos OS Multicast Protocols Configuration Guide](#).

| Protocol Independent Multicast source-specific multicast (PIM SSM) | 12.2R1 | 12.1R1 | 9.3R1 | 13.2X50 - D10 | 11.1R1 | 12.2R1 | 11.1R1 | 11.1R1 |

See the [Junos OS Multicast Protocols Configuration Guide](#).

Single-source multicast | N.S. | N.S. | 9.0R2 | 13.2X50 - D10 | N.S. | N.S. | N.S. | 11.R1 |

Table 54: Network Management and Monitoring Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1ag Ethernet OAM connectivity fault management (CFM)</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>10.2R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
</tbody>
</table>

| Ethernet frame delay measurement (ETH-DM, Y.1731) | N.S. | N.S. | 11.4R1 (EX4200 only) | 13.2X50 - D10 | N.S. | N.S. | N.S. | 11.4R1 |
Table 54: Network Management and Monitoring Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet OAM link fault management (LFM—also known as Ethernet in the First Mile, EFM)</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Port mirroring enhancements</td>
<td>N.S.</td>
<td>N.S.</td>
<td>9.5R1</td>
<td>--</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>• Layer 3 interface support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Multiple VLAN support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port mirroring enhancements</td>
<td>N.S.</td>
<td>N.S.</td>
<td>10.0R1</td>
<td>--</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>• For remote port mirroring, ingress and egress options on VLAN member interfaces on the intermediate (transit) switch to avoid flooding mirrored traffic to those interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port mirroring support for multiple analyzers per session</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Real-time performance monitoring (RPM)</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Feature</td>
<td>EX2200 Virtual Chassis</td>
<td>EX3300 Virtual Chassis</td>
<td>EX4200 Virtual Chassis</td>
<td>EX4300 Virtual Chassis</td>
<td>EX4500 Virtual Chassis</td>
<td>EX4550 Virtual Chassis</td>
<td>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</td>
<td>EX8200 Virtual Chassis</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>---------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Real-time performance monitoring (RPM)—hardware timestamps with RVIs and IRB interfaces</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>10.3R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Real-time performance monitoring (RPM)—client and server on same interface</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>10.3R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Routing Engine Software Development Kit (SDK)</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
</tr>
<tr>
<td>RMON</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>sFlow monitoring technology</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>12.2R1</td>
<td>11.2R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>sFlow monitoring technology—Persistent IP addresses for agent IDs and use in datagrams</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>10.2R1</td>
<td>13.2X50 - D10</td>
<td>11.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Simple Network Management Protocol version 1 (SNMPv1), SNMPv2, and SNMPv3</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Uplink failure detection</td>
<td>12.2R1</td>
<td>12.1R2</td>
<td>11.1R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Feature</td>
<td>EX2200 Virtual Chassis</td>
<td>EX3300 Virtual Chassis</td>
<td>EX4200 Virtual Chassis</td>
<td>EX4300 Virtual Chassis</td>
<td>EX4500 Virtual Chassis</td>
<td>EX4550 Virtual Chassis</td>
<td>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</td>
<td>EX8200 Virtual Chassis</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------</td>
<td>------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Automatic recovery for port error disable conditions</td>
<td>11.2R1</td>
<td>11.3R1</td>
<td>9.6R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>DHCP option 82</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>DHCP snooping</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Dynamic ARP inspection (DAI)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>IP source guard</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>MAC limiting</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>MAC address limit per port</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>MAC limiting per port and per VLAN (VLAN membership MAC limit)</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>MAC move limiting</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Persistent MAC learning (sticky MAC)</td>
<td>12.2R1</td>
<td>12.3R1</td>
<td>11.4R1</td>
<td>13.2X50 - D10</td>
<td>11.4R1</td>
<td>12.2R1</td>
<td>11.4R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Persistent storage for DHCP snooping</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Static ARP support</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
</tbody>
</table>
### Table 56: Power over Ethernet (PoE) Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Layer Discovery Protocol (LLDP) with granular Power over Ethernet (PoE) management</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.2R1</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** The member switches in an EX4200 Virtual Chassis must be running PoE controller software firmware version 4.04 or later. See show chassis firmware detail and request system firmware upgrade poe to check or upgrade this firmware.

This feature is supported for EX4200-24PX and EX4200-48PX member switch interfaces in any EX4200 Virtual Chassis.

| Power over Ethernet (PoE)                                            | 12.2R1                  | 11.3R1                  | 9.0R2                   | 13.2X50 - D10           | --                      | N.S.                    | 11.4R1                                                                                   |                         |
|-----------------------------------------------------------------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|--------------------------------------------------------------------------------|                         |
| Power over Ethernet Plus (PoE+)                                       | 12.2R1                  | 11.3R1                  | 11.2R1                  | 13.2X50 - D10           | --                      | N.S.                    | 11.4R1                                                                                   |                         |
| (EX4200-24PX and EX4200-48PX models only)                             |                         |                         |                         |                         |                         |                         |                                                                                       |                         |
| Power over Ethernet (PoE) power management mode                       | 12.2R1                  | 11.3R1                  | 9.3R2                   | 13.2X50 - D10           | --                      | N.S.                    | 11.2R1                                                                                   |                         |

### Table 57: Routing Policy and Packet Filtering Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic allocation of TCAM memory to firewall filters</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>10.0R1</td>
<td>--</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Firewall filters and rate limiting</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
</tbody>
</table>
## Table 57: Routing Policy and Packet Filtering Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall filters on LAGs</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Firewall filters on the loopback interface</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Firewall filters on the management interface</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>10.4R1</td>
<td>13.2X50 - D10</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Firewall filters on the virtual management interface</td>
<td>–</td>
<td>N.S.</td>
<td>10.4R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>–</td>
</tr>
<tr>
<td>Firewall filters with IPv6</td>
<td>11.3R1</td>
<td>12.3R1</td>
<td>10.1R1</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>12.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Policing</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Tricolor marking policers</td>
<td>11.2R1</td>
<td>11.4R8</td>
<td>11.2R1</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
</tr>
</tbody>
</table>

For a list of supported firewall filter match conditions and actions, see “Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 4111.

## Table 58: Spanning-Tree Protocols Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPDU protection for spanning-tree protocols</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.1R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
</tbody>
</table>
### Table 58: Spanning-Tree Protocols Features by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPDU filter</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>13.2X50 - D10</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
</tr>
<tr>
<td>Distributed periodic packet management (PPM) for Spanning Tree Protocols</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Loop protection for spanning-tree protocols</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.1R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Root protection for spanning-tree protocols</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.1R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Spanning tree:</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>10.2R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>• RSTP and VSTP concurrent configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanning tree:</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>• Spanning Tree Protocol (STP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Rapid Spanning Tree Protocol (RSTP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Multiple Spanning Tree Protocol (MSTP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spanning tree:</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
<tr>
<td>• VLAN Spanning Tree Protocol (VSTP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 59: System Management Features by Junos OS Release

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autoinstallation of configuration files</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.4R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Automatic software download</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.6R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>11.2R1</td>
</tr>
<tr>
<td>Automatic repair of corrupted partition when booting from alternate partition</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>13.2X50 - D10</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Configuration rollback</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Zero Touch Provisioning (EZ Touchless Provisioning using DHCP)</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>J-Web interface, for switch configuration and management</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>9.0R2</td>
<td>13.2X50 - D10</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Junos Space Service Now support</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>N.S.</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
<td>12.3R1</td>
</tr>
<tr>
<td>LCD panel management support</td>
<td>–</td>
<td>11.3R1</td>
<td>9.0R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>12.1R1</td>
</tr>
<tr>
<td>Online insertion and removal (OIR) of uplink modules</td>
<td>–</td>
<td>–</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>–</td>
</tr>
<tr>
<td>Self-signed digital certificates for enabling SSL services</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.2R1</td>
</tr>
</tbody>
</table>
Table 60: Virtual Chassis Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic software update on prospective member switches</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>10.0R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>N.S.</td>
<td>N.S.</td>
</tr>
<tr>
<td>Digital optical monitoring (DOM) on Virtual Chassis ports (VCPs)</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>13.2X50 - D10</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>12.2R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>EX8200 Virtual Chassis Management Information Base (MIB) Enhancements (including temperature and user-configured VCP monitoring)</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>12.3R1</td>
</tr>
<tr>
<td>Front-panel configuration of uplink module ports as Virtual Chassis ports (VCPs)</td>
<td>–</td>
<td>11.3R1</td>
<td>10.0R1</td>
<td>N.S.</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Graceful Routing Engine switchover (GRES) for Virtual Chassis</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>9.1R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>11.1R1</td>
</tr>
<tr>
<td>Link aggregation groups (LAGs) over Virtual Chassis ports (VCPs)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.6R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
<tr>
<td>Role requirements for mixed EX4200 and EX4500 Virtual Chassis—master and backup can be any combination of EX4200 and EX4500 switches</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>11.4R1</td>
</tr>
</tbody>
</table>
## Table 60: Virtual Chassis Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role requirements for mixed EX4200 and EX4500 Virtual Chassis—master and backup must be either two EX4200 switches or two EX4500 switches</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>11.2R1</td>
<td>-</td>
</tr>
<tr>
<td>Role requirements for mixed EX4200 and EX4500 Virtual Chassis—master and backup must be two EX4500 switches</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>11.1R1</td>
<td>-</td>
</tr>
<tr>
<td>Member switch support maximum</td>
<td>4—12.2R1 (initial release)</td>
<td>10—12.2R1 (initial release)</td>
<td>10—9.0R1 (initial release)</td>
<td>10—13.2X50 - D10</td>
<td>10—11.4R1 (initial release)</td>
<td>10—12.2R1 (initial release)</td>
<td>10—11.1R1 (initial release)</td>
<td>4—12.1R1 (initial release)</td>
</tr>
<tr>
<td>Virtual Chassis fast failover</td>
<td>N.S.</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>N.S.</td>
<td>12.1R1</td>
<td>12.2R1</td>
<td>12.1R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Virtual Chassis split and merge</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.3R2</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
</tbody>
</table>

*NOTE: A mixed Virtual Chassis supports up to 10 member switches regardless of whether the switches are EX4200 switches, EX4500 switches, or EX4550 switches.*
Table 60: Virtual Chassis Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>Mixed EX4200, EX4500, and EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Chassis—Autoprovisioning of Virtual Chassis ports (VCPs)</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.5R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>N.S.</td>
</tr>
<tr>
<td>Virtual Chassis preprovisioning</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.0R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1</td>
<td>10.4R1</td>
</tr>
</tbody>
</table>
### Table 60: Virtual Chassis Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>EX2200 Virtual Chassis</th>
<th>EX3300 Virtual Chassis</th>
<th>EX4200 Virtual Chassis</th>
<th>EX4300 Virtual Chassis</th>
<th>EX4500 Virtual Chassis</th>
<th>EX4550 Virtual Chassis</th>
<th>EX8200 Virtual Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Chassis—SFP uplink port interconnection of member switches</td>
<td>12.2R1</td>
<td>11.3R1</td>
<td>9.2R1</td>
<td>13.2X50 - D10</td>
<td>11.1R1</td>
<td>12.2R1</td>
<td>11.1R1 (EX4200 to EX4200 and EX4500 to EX4500 only)</td>
</tr>
<tr>
<td><strong>NOTE:</strong> You can use SFP uplink port connections to interconnect EX4500 member switches into a Virtual Chassis without installing a Virtual Chassis module starting in Junos OS Release 11.4R1. An installed Virtual Chassis module is required in previous Junos OS releases.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XRE200 Hard Disk Drive (HDD) monitoring</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>
Related Documentation

- EX Series Switch Software Features Overview on page 27
- EX2200 Switches Hardware Overview
- EX3200 Switches Hardware Overview
- EX3300 Switches Hardware Overview
- EX4200 Switches Hardware Overview
- EX4300 Switches Hardware Overview
- EX4500 Switches Hardware Overview
- EX4550 Switches Hardware Overview
- EX6210 Switch Hardware Overview
- EX8208 Switch Hardware Overview
- EX8216 Switch Hardware Overview
- Line Card Model and Version Compatibility in an EX6200 Switch
- Line Card Model and Version Compatibility in an EX8200 Switch
- XRE200 External Routing Engine Hardware Overview
- Layer 3 Protocols Supported on EX Series Switches on page 2553
- Layer 3 Protocols Not Supported on EX Series Switches on page 2554
PART 3

System Setup

- Overview on page 111
- Configuration on page 115
- Administration on page 159
- Troubleshooting Procedures on page 379
CHAPTER 3

Overview

- Software Overview on page 111

Software Overview

- Understanding Software Infrastructure and Processes on page 111

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 111
- Junos OS Processes on page 112

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.

- Routing Engine—Provides three main functions:
  - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network
- Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

**Junos OS Processes**

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 61 on page 112 describes the primary Junos OS processes.

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis process</td>
<td>chassisd</td>
<td>Detects hardware on the system that is used to configure network interfaces. Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered. Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</td>
</tr>
<tr>
<td>Ethernet switching process</td>
<td>eswd</td>
<td>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces. Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>Forwarding process</td>
<td>pfem</td>
<td>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</td>
</tr>
<tr>
<td>Interface process</td>
<td>dcd</td>
<td>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</td>
</tr>
<tr>
<td>Management process</td>
<td>mgd</td>
<td>Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the switch. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</td>
</tr>
<tr>
<td>Routing protocol process</td>
<td>rpd</td>
<td>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</td>
</tr>
</tbody>
</table>
Related Documentation

- For more information about processes, see Junos OS Network Operations Guide
- For more information about basic system parameters, supported protocols, and software processes, see Junos OS System Basics Configuration Guide
Configuration

- Initial Configuration on page 115
- Configuration Statements on page 119

Initial Configuration

- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- Configuring Date and Time for the EX Series Switch (J-Web Procedure) on page 117
- Configuring System Identity for an EX Series Switch (J-Web Procedure) on page 118

Configuring the LCD Panel on EX Series Switches (CLI Procedure)

This topic applies to hardware devices in the EX Series product family, which includes switches and the XRE200 External Routing Engine, that support the LCD panel interface.

The LCD panel on the front panel of EX Series switches displays a variety of information about the switch in the Status menu and provides the Maintenance menu to allow you to perform basic operations such as initial setup and reboot. You can disable these menus or individual menu options if you do not want switch users to use them. You can also set a custom message that will be displayed on the panel.

This topic describes:

- Disabling or Enabling Menus and Menu Options on the LCD Panel on page 115
- Configuring a Custom Display Message on page 116

Disabling or Enabling Menus and Menu Options on the LCD Panel

By default, the Maintenance menu, the Status menu, and the options in those menus in the LCD panel are enabled. Users can configure and troubleshoot the switch using the Maintenance menu and view certain details about the switch using the Status menu.

If you do not want users to be able to use those menus or use some of the menu options, you can disable the menus or individual menu options. You can re-enable the menus or menu options.

Issue the `show chassis lcd` operational mode command to see which menus and menu options are currently enabled.
NOTE: On some platforms you must specify an FPC slot number in these commands. See the `lcd-menu` statement for details.

To disable a menu:

```
[edit]
user@switch# set chassis lcd-menu menu-item menu-name disable
```

To enable a menu:

```
[edit]
user@switch# delete chassis lcd-menu menu-item menu-name disable
```

To disable a menu option:

```
[edit]
user@switch# set chassis lcd-menu menu-item menu-option disable
```

To enable a menu option:

```
[edit]
user@switch# delete chassis lcd-menu menu-item menu-option disable
```

**Configuring a Custom Display Message**

You can configure the second line of the LCD to display a custom message temporarily for 5 minutes or permanently.

To display a custom message temporarily:

- On an EX3200 switch, a standalone EX3300 switch, a standalone EX4200 switch, a standalone EX4500 switch, an EX8200 switch, or an XRE200 External Routing Engine:
  
  ```
  user@switch> set chassis display message message
  ```

- On an EX3300, EX4200, or EX4500 switch in a Virtual Chassis configuration:
  
  ```
  user@switch> set chassis display message message fpc-slot slot-number
  ```

To display a custom message permanently:

- On an EX3200 switch, a standalone EX3300 switch, a standalone EX4200 switch, a standalone EX4500 switch, an EX8200 switch, or an XRE200 External Routing Engine:
  
  ```
  user@switch> set chassis display message message permanent
  ```

- On an EX3300, EX4200, or EX4500 switch in a Virtual Chassis configuration:
  
  ```
  user@switch> set chassis display message message fpc-slot slot-number permanent
  ```

**NOTE:** The buttons on the LCD panel are disabled when the LCD is configured to display a custom message.

To disable the display of the custom message:

```
user@switch> clear chassis display message
```

You can view the custom message by issuing the command `show chassis lcd`.
Configuring Date and Time for the EX Series Switch (J-Web Procedure)

To configure date and time on an EX Series switch:

1. Select Configure > System Properties > Date & Time.
2. To modify the information, click Edit. Enter information into the Edit Date & Time page as described in Table 62 on page 117.
3. Click one of the following options:
   - To apply the configuration, click OK.
   - To cancel your entries and return to the System Properties page, click Cancel.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

### Table 62: Date and Time Settings

<table>
<thead>
<tr>
<th>Time</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>Identifies the timezone that the switching platform is located in.</td>
<td>Select the appropriate time zone from the list.</td>
</tr>
</tbody>
</table>
| Set Time | Synchronizes the system time with that of the NTP server. You can also manually set the system time and date. | To immediately set the time, Click one of the following options:  
  - **Synchronize with PC time**—The switch synchronizes the time with that of the PC.  
  - **NTP Servers**—The switch sends a request to the NTP server and synchronizes the system time.  
  - **Manual**—A pop-up window allows you to select the current date and time from a list. |
To configure identification details for an EX Series switch:

1. Select **Configure > System Properties > System Identity**. The System Identity page displays configuration details.

2. To modify the configuration, click **Edit**. Enter information into the System Identity page as described in Table 63 on page 118.

**NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

### Table 63: System Identity Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Defines the hostname of the switching platform.</td>
<td>Type the hostname.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Defines the network or subnetwork that the machine belongs to.</td>
<td>Type the domain name.</td>
</tr>
<tr>
<td>Root Password</td>
<td>Sets the root password that user root can use to log in to the switching platform.</td>
<td>Type a plain-text password. The system encrypts the password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> After a root password has been defined, it is required when you log in to the J-Web user interface or the CLI.</td>
</tr>
<tr>
<td>Confirm Root Password</td>
<td>Verifies that the root password has been typed correctly.</td>
<td>Retype the password.</td>
</tr>
<tr>
<td>DNS Name Servers</td>
<td>Specifies a DNS server for the switching platform to use to resolve hostnames into addresses.</td>
<td>To add an IP address, click <strong>Add</strong>. To edit an IP address, click <strong>Edit</strong>. To delete an IP address, click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Domain Search</td>
<td>Specifies the domains to be searched.</td>
<td>To add a domain, click <strong>Add</strong>. To edit a domain, click <strong>Edit</strong>. To delete a domain, click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
Configuration Statements
arp (System)

Syntax

```
arp {
    aging-timer minutes;
    gratuitous-arp-delay seconds;
    gratuitous-arp-on-ifup;
    interfaces {
        interface-name {
            aging-timer minutes;
        }
    }
    passive-learning;
    purging;
}
```

For EX-Series switches:

```
arp {
    aging-timer minutes;
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify ARP options. You can enable backup VRRP routers to learn ARP requests for VRRP-IP to VRRP-MAC address translation. You can also set the time interval between ARP updates.

For EX-Series switches, set only the time interval between ARP updates.

Options

- **aging-timer**—Time interval in minutes between ARP updates. In environments where the number of ARP entries to update is high (for example, on routers only, metro Ethernet environments), increasing the time between updates can improve system performance.
- **passive-learning** (QFX-Series only)—Configure switches to learn the ARP mappings (IP-to-MAC address) for hosts sending the requests.

Default: 20 minutes

Range: 1 to 240 minutes

The remaining statements are explained separately.

Required Privilege

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS ARP Learning and Aging Options for Mapping IPv4 Network Addresses to MAC Addresses
- Junos OS Network Interfaces Library for Routing Devices
• For more information about ARP updates, see the Junos OS System Basics Configuration Guide.

authentication-key

Syntax  
authentication-key key-number type type value password;

Hierarchy Level  
[edit system ntp]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Configure Network Time Protocol (NTP) authentication keys so that the router or switch can send authenticated packets. If you configure the router or switch to operate in authenticated mode, you must configure a key.

Both the keys and the authentication scheme (MD5) must be identical between a set of peers sharing the same key number.

Options  
key-number—Positive integer that identifies the key.

type type—Authentication type. It can only be md5.

value password—The key itself, which can be from 1 through 8 ASCII characters. If the key contains spaces, enclose it in quotation marks.

Required Privilege Level  
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  
• Configuring NTP Authentication Keys
  • broadcast on page 124
  • peer on page 149
  • server on page 154
  • trusted-key on page 158
auxiliary

Syntax auxiliary {
  disable;
  insecure;
  type terminal-type:
  port-type (mini-usb | rj45);
}

Hierarchy Level [edit system ports]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the characteristics of the auxiliary port.
Remaining statement is explained separately.

Default disable is the default option.

Options disable—Disable the port.
insecure—Disable super user access or root logins to establish terminal connection.
type terminal-type—Type of terminal that is connected to the port.
Range: ansi, vt100, small-xterm, xterm
Default: The terminal type is unknown, and the user is prompted for the terminal type. The
remaining statement is explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation • Configuring the Junos OS to Set Console and Auxiliary Port Properties
boot-server (NTP)

Syntax  boot-server (address | hostname);

Hierarchy Level  [edit system ntp]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure the server that NTP queries when the router or switch boots to determine the local date and time.

When you boot the router or switch, it issues an ntpdate request, which polls a network server to determine the local date and time. You need to configure a server that the router or switch uses to determine the time when the router or switch boots. Otherwise, NTP will not be able to synchronize to a time server if the server’s time appears to be very far off of the local router’s or switch’s time. You can either configure an IP address or a hostname for the boot server. If you configure a hostname instead of an IP address, the ntpdate request resolves the hostname to an IP address when the router or switch boots up.

Options

• address—The IP address of an NTP boot server.
• hostname—The hostname of an NTP boot server.

Required Privilege Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Synchronizing and Coordinating Time Distribution Using NTP
**broadcast**

**Syntax**

```
broadcast address <key key-number> <version value> <ttl value>;
```

**Hierarchy Level**

```
[edit system ntp]
```

**Release Information**


**Description**

Configure the local router or switch to operate in broadcast mode with the remote system at the specified `address`. In this mode, the local router or switch sends periodic broadcast messages to a client population at the specified broadcast or multicast `address`. Normally, you include this statement only when the local router or switch is operating as a transmitter.

**Options**

- **address**—The broadcast address on one of the local networks or a multicast address assigned to NTP. You must specify an address, not a hostname. If the multicast address is used, it must be `224.0.1.1`.

- **key key-number**—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

  **Range:** Any unsigned 32-bit integer

- **ttl value**—(Optional) Time-to-live (TTL) value to use.

  **Range:** 1 through 255

  **Default:** 1

- **version value**—(Optional) Specify the version number to be used in outgoing NTP packets.

  **Range:** 1 through 4

  **Default:** 4

**Required Privilege**

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

**Related Documentation**

- *Configuring the NTP Time Server and Time Services*
**broadcast-client**

**Syntax**

broadcast-client;

**Hierarchy Level**

[edit system ntp]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure the local router or switch to listen for broadcast messages on the local network to discover other servers on the same subnet.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring the Router or Switch to Listen for Broadcast Messages Using NTP
**console (System Ports)**

**Syntax**

```console
console {
  disable;
  insecure;
  log-out-on-disconnect;
  type terminal-type;
}
```

**Hierarchy Level**

[edit system ports]

**Release Information**

Statement introduced before Junos OS Release 7.4.

*disable* option added in Junos OS Release 7.6.

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure the characteristics of the console port.

**Default**

The console port is enabled and its speed is 9600 baud.

**Options**

- **disable**—Disable console login connections.
- **insecure**—Disable root login connections to the console and auxiliary ports. Configuring the console port as insecure also prevents superusers and anyone with a user identifier (UID) of 0 from establishing terminal connections in multiuser mode. This option can be used to prevent a user from attempting password recovery by booting into single-user mode, if the user does not know the root password.

  **log-out-on-disconnect**—Log out the session when the data carrier on the console port is lost.

  **NOTE:** The *log-out-on-disconnect* option is not operational on MX80 routers. On MX80 routers you must manually log out from the console with the request system logout u0 command.

- **type terminal-type**—Type of terminal that is connected to the port.

  **Range:** ansi, vt100, small-xterm, xterm

  **Default:** The terminal type is unknown, and the user is prompted for the terminal type.

**Required Privilege**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Configuration the Junos OS to Set Console and Auxiliary Port Properties
default-address-selection

Syntax  default-address-selection;

Hierarchy Level  [edit system]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Use the loopback interface, lo0, as the source address for all locally generated IP packets when the packet is sent through a routed interface, but not when the packet is sent through a local interface such as fxp0. The lo0 interface is the interface to the router’s or switch’s Routing Engine.

Default  The default address is used as the source address for all locally generated IP packets on outgoing interfaces that are unnumbered. If an outgoing interface is numbered, the default address is chosen using the following sequence:

- The primary address on the loopback interface lo0 that is not 127.0.0.1 is used.
- The primary address for the primary interface or the preferred address (if configured) for the primary interface is used.

By default, the primary address on an interface is selected as the numerically lowest local address configured on the interface.

An interface’s primary address is used by default as the local address for broadcast and multicast packets sourced locally and sent out through the interface. An interface’s preferred address is the default local address used for packets sourced by the local router or switch to destinations on the subnet. By default, the numerically lowest local address configured for the interface is chosen as the preferred address on the subnet.

To configure a different primary address or preferred address, include the primary or preferred statement at the [edit interfaces interface-name unit logical-unit-number family family address address] or [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address] hierarchy levels.

For more information about default, primary, and preferred addresses for an interface, see “Configuring Default, Primary, and Preferred Addresses and Interfaces” in the Junos OS Network Interfaces Library for Routing Devices.

Required Privilege Level  system—To view this statement in the configuration.
  system-control—To add this statement to the configuration.

Related Documentation  • Configuring the Junos OS to Select a Fixed Source Address for Locally Generated TCP/IP Packets

  • Junos OS Network Interfaces Library for Routing Devices
**domain-name**

Syntax:  
```plaintext
domain-name domain-name;
```

Hierarchy Level:  
```plaintext
[edit system]
```

Release Information:  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description:  
Configure the name of the domain in which the router or switch is located. This is the default domain name that is appended to hostnames that are not fully qualified.

Options:  
```plaintext
domain-name—Name of the domain.
```

Required Privilege Level:  
```plaintext
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.
```

Related Documentation:  
- Configuring the Domain Name for the Router or Switch

---

**gre-path-mtu-discovery**

Syntax:  
```plaintext
(gre-path-mtu-discovery | no-gre-path-mtu-discovery);
```

Hierarchy Level:  
```plaintext
[edit system internet-options]
```

Release Information:  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description:  
Configure path MTU discovery for outgoing GRE tunnel connections:
- `gre-path-mtu-discovery`—Path MTU discovery is enabled.
- `no-gre-path-mtu-discovery`—Path MTU discovery is disabled.

Default:  
Path MTU discovery is enabled.

Required Privilege Level:  
```plaintext
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.
```

Related Documentation:  
- Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections
host-name

Syntax  
host-name hostname;

Hierarchy Level  
[edit system]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Set the hostname of the router or switch.

Options  
hostname—Name of the router or switch.

Required Privilege
Level  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

Related Documentation
• Configuring the Hostname of the Router or Switch

icmpv4-rate-limit

Syntax  
icmpv4-rate-limit  
  {  
    bucket-size seconds;  
    packet-rate pps;  
  }

Hierarchy Level  
[edit system internet-options]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Configure rate-limiting parameters for ICMPv4 messages sent.

Options  
bucket-size seconds—Number of seconds in the rate-limiting bucket.  
  Range: 0 through 4294967295 seconds  
  Default: 5

  packet-rate pps—Rate-limiting packets earned per second.  
  Range: 0 through 4294967295 pps  
  Default: 1000

Required Privilege
Level  
admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration.

Related Documentation
• Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages
icmpv6-rate-limit

Syntax
icmpv6-rate-limit {
  bucket-size seconds;
  packet-rate packet-rate;
}

Hierarchy Level [edit system internet-options]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure rate-limiting parameters for ICMPv6 messages sent.

Options
  bucket-size seconds—Number of seconds in the rate-limiting bucket.
  Range: 0 through 4294967295 seconds
  Default: 5

  packet-rate pps—Rate-limiting packets earned per second.
  Range: 0 through 4294967295 pps
  Default: 1000

Required Privilege Level
  admin—To view this statement in the configuration.
  admin-control—To add this statement to the configuration.

Related Documentation
  • Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages
**inet6-backup-router**

**Syntax**

```plaintext
inet6-backup-router address <destination destination-address>;
```

**Hierarchy Level**

```plaintext
[edit system]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Set a default router (running IP version 6 [IPv6]) to use while the local router or switch (running IPv6) is booting and if the routing protocol processes fail to start. The Junos OS removes the route to this router or switch as soon as the software starts.

**Options**

- **address**—Address of the default router.
- **destination destination-address**—(Optional) Destination address that is reachable through the backup router. You can include this option to achieve network reachability while loading, configuring, and recovering the router or switch, but without the risk of installing a default route in the forwarding table.

**Default:** All hosts (default route) are reachable through the backup router.

**Required Privilege Level**

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring a Backup Router
internet-options

Syntax  
```bash
internet-options {
  (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
  icmpv4-rate-limit bucket-size bucket-size packet-rate packet-rate;
  icmpv6-rate-limit bucket-size bucket-size packet-rate packet-rate;
  (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
  ipv6-duplicate-addr-detection-transmits;
  (ipv6-reject-zero-hop-limit | no-ipv6-reject-zero-hop-limit);
  (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
  ipv6-path-mtu-discovery-timeout;
  no-tcp-rfc1323;
  no-tcp-rfc1323-paws;
  (path-mtu-discovery | no-path-mtu-discovery);
  source-port upper-limit <upper-limit>;
  (source-quench | no-source-quench);
  tcp-drop-synfin-set;
  tcp-mss mss-value;
}
```

Hierarchy Level  [edit system]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure system IP options to protect against certain types of DoS attacks.

The remaining statements are explained separately.

Required Privilege Level  admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation  • Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages
• Configuring the Junos OS ICMPv6 Rate Limit for ICMPv6 Routing Engine Messages
• Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections
• Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections
• Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections
• Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts
• Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit
• Configuring the Junos OS to Ignore ICMP Source Quench Messages
• Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set
• Configuring the Junos OS to Disable TCP RFC 1323 Extensions
• Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension
• Configuring the Junos OS to Extend the Default Port Address Range
ipip-path-mtu-discovery

Syntax
(ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);

Hierarchy Level
[edit system internet-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure path MTU discovery for outgoing IP-IP tunnel connections:

- ipip-path-mtu-discovery—Path MTU discovery is enabled.
- no-ipip-path-mtu-discovery—Path MTU discovery is disabled.

Default
Path MTU discovery is enabled.

Required Privilege
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS for IP-IP Path MTU Discovery on IP-IP Tunnel Connections
- internet-options on page 132

ipv6-duplicate-addr-detection-transmits

Syntax
ipv6-duplicate-addr-detection-transmits;

Hierarchy Level
[edit system internet-options]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Control the number of attempts for IPv6 duplicate address detection.

The range of values supported for ipv6-duplicate-addr-detection-transmits is from 0 to 20.

Default
The default value is 3.

Required Privilege
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS for IPv6 Duplicate Address Detection Attempts
ipv6-path-mtu-discovery

Syntax  (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);

Hierarchy Level  [edit system internet-options]

Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description  Configure path MTU discovery for IPv6 packets:

•  ipv6-path-mtu-discovery—IPv6 path MTU discovery is enabled.
•  no-ipv6-path-mtu-discovery—IPv6 path MTU discovery is disabled.

Default  IPv6 path MTU discovery is enabled.

Required Privilege Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  • Configuring the Junos OS for IPv6 Path MTU Discovery

ipv6-path-mtu-discovery-timeout

Syntax  ipv6-path-mtu-discovery-timeout minutes;

Hierarchy Level  [edit system internet-options]

Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description  Set the IPv6 path MTU discovery timeout interval.

Options  minutes—IPv6 path MTU discovery timeout.
Default: 10 minutes

Required Privilege Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  • Configuring the Junos OS for IPv6 Path MTU Discovery
ipv6-reject-zero-hop-limit

Syntax  (ipv6-reject-zero-hop-limit | no-ipv6-reject-zero-hop-limit);

Hierarchy Level  [edit system internet-options]

Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description  Enable and disable rejecting incoming IPv6 packets with a zero hop limit value in their header.

Required Privilege Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  • Configuring the Junos OS for Acceptance of IPv6 Packets with a Zero Hop Limit
Syntax

EX3200, EX3300, EX4200, or EX4500 switch:

```plaintext
lcd-menu fpc slot-number {
  menu-item (menu-name | menu-option) <disable>;
}
```

EX6200 or EX8200 switch or XRE200 External Routing Engine:

```plaintext
lcd-menu {
  menu-item (menu-name | menu-option) <disable>;
}
```

Hierarchy Level
[edit chassis]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Disable or enable the Maintenance menu or the Status menu in the LCD panel.

Options

- none—(EX6200 and EX8200 switches and XRE200 External Routing Engines only) Disable or enable the specified menu or menu options.
- `fpc slot-number`—(EX3200, EX3300, EX4200, and EX4500 switches only) Disable or enable the specified menu or menu options, where `slot-number` is:
  - 0—On standalone switches.
  - 0–9—On a device in a Virtual Chassis. The value is the member ID of the device.

**NOTE:** This option is not available on an EX8200 Virtual Chassis. The LCD panel on an XRE200 External Routing Engine provides information for the XRE200 External Routing Engine only.

- `disable`—(Optional) Disable the specified menu.

The remaining statement is explained separately.

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-level—To add this statement to the configuration.

Related Documentation
- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
  - LCD Panel in EX3200 Switches
  - LCD Panel in EX3300 Switches
  - LCD Panel in EX4200 Switches
  - LCD Panel in EX4500 Switches
  - LCD Panel in an EX6200 Switch
- LCD Panel in an EX8200 Switch
- LCD Panel in an XRE200 External Routing Engine
**location (System)**

**Syntax**

```plaintext
location {
    altitude feet;
    building name;
    country-code code;
    floor number;
    hcoord horizontal-coordinate;
    lata service-area;
    latitude degrees;
    longitude degrees;
    npa-nxx number;
    postal-code postal-code;
    rack number;
    vcoord vertical-coordinate;
}
```

**Hierarchy Level**

[edit system]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure the system location in various formats.

**Options**

- **altitude feet**—Number of feet above sea level.
- **building name**—Name of building. The name of the building can be 1 to 28 characters in length. If the string contains spaces, enclose it in quotation marks (" ").
- **country-code code**—Two-letter country code.
- **floor number**—Floor in the building.
- **hcoord horizontal-coordinate**—Bellcore Horizontal Coordinate.
- **lata service-area**—Long-distance service area.
- **latitude degrees**—Latitude in degree format.
- **longitude degrees**—Longitude in degree format.
- **npa-nxx number**—First six digits of the phone number (area code and exchange).
- **postal-code postal-code**—Postal code.
- **rack number**—Rack number.
- **vcoord vertical-coordinate**—Bellcore Vertical Coordinate.

**Required Privilege Level**

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.
Related Documentation

- Configuring the Physical Location of the Router or Switch
**menu-item**

**Syntax**
```
menu-item (menu-name | menu-option) <disable>
```

**Hierarchy Level**
- [edit chassis lcd-menu],
- [edit chassis lcd-menu fpc slot-number]

**Release Information**
Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**
Disable or enable the Maintenance menu, the Status menu, or an individual option in one of those menus in the LCD panel.

On EX3200, EX3300, EX4200, and EX4500 switches, you use `menu-item` at the `[edit chassis lcd-menu fpc slot-number]` hierarchy level.

On EX6200 and EX8200 switches, and on XRE200 External Routing Engines, you use `menu-item` at the `[edit chassis lcd-menu]` hierarchy level.

**Options**
- `menu-name`—Name of the LCD menu:
  - maintenance-menu
  - status-menu

- `menu-option`—Specific option on one of the LCD menus. You must include the quotation marks when you type the option. Table 64 on page 141 describes the different menu options of the LCD menus supported on the switches.
Table 64: Menu Options of the LCD Menus Supported on the Switches

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu Options</th>
<th>Option Descriptions</th>
<th>Platforms Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>maintenance-menu</td>
<td>&quot;maintenance-menu halt-menu&quot;</td>
<td>System halt option</td>
<td>All switches except EX2200</td>
</tr>
<tr>
<td></td>
<td>&quot;maintenance-menu system-reboot&quot;</td>
<td>System reboot option</td>
<td>All switches except EX2200</td>
</tr>
<tr>
<td></td>
<td>&quot;maintenance-menu rescue-config&quot;</td>
<td>Load rescue option</td>
<td>All switches except EX2200</td>
</tr>
<tr>
<td></td>
<td>&quot;maintenance-menu vc-uplink-config&quot;</td>
<td>Request VC port option for a device in a Virtual Chassis configuration</td>
<td>EX3300, EX4200, and EX4500 switches and XRE200 External Routing Engines only</td>
</tr>
<tr>
<td></td>
<td>&quot;maintenance-menu factory-default&quot;</td>
<td>Factory default option</td>
<td>All switches except EX2200</td>
</tr>
<tr>
<td>status-menu</td>
<td>&quot;status-menu vcp-status&quot;</td>
<td>Virtual Chassis port (VCP) status for a device in a Virtual Chassis configuration</td>
<td>EX3300, EX4200, and EX4500 switches and XRE200 External Routing Engines only</td>
</tr>
<tr>
<td></td>
<td>&quot;status-menu sf-status1-menu&quot;</td>
<td>Status of the switch fabric on the Switch Fabric and Routing Engine (SRE) module in slot SRE0 on EX8208 switches</td>
<td>EX8208 and EX8216 switches only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status of the switch fabric on the Switch Fabric (SF) modules in slots SF0 and SF1 on EX8216 switches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;status-menu sf-status2-menu&quot;</td>
<td>Status of the switch fabric on the SRE module in slot SRE1 on EX8208 switches</td>
<td>EX8208 and EX8216 switches only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Status of the switch fabric on the SF modules in slots SF2–SF5 on EX8216 switches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;status-menu sf-status3-menu&quot;</td>
<td>Status of the switch fabric on the SF modules in slots SF6 and SF7 on EX8216 switches</td>
<td>EX8216 switches only</td>
</tr>
<tr>
<td></td>
<td>&quot;status-menu power-status&quot;</td>
<td>Status of the power supply or power supplies</td>
<td>EX3200, EX3300, EX4200, and EX4500 switches</td>
</tr>
</tbody>
</table>
### Table 64: Menu Options of the LCD Menus Supported on the Switches (continued)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Menu Options</th>
<th>Option Descriptions</th>
<th>Platforms Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&quot;status-menu psu-status1-menu&quot;</td>
<td>Status of the power supplies in slots P0 and P1</td>
<td>EX8208 and EX8216 switches only</td>
</tr>
<tr>
<td></td>
<td>&quot;status-menu psu-status2-menu&quot;</td>
<td>Status of the power supplies in slots P2–P5</td>
<td>EX8208 and EX8216 switches only</td>
</tr>
<tr>
<td></td>
<td>&quot;status-menu environ-menu&quot;</td>
<td>Status of the fan; current chassis temperature</td>
<td>All switches (except EX2200) and XRE200 External Routing Engine</td>
</tr>
<tr>
<td></td>
<td>&quot;status-menu show-version&quot;</td>
<td>The version of Junos OS loaded on the switch</td>
<td>All switches except EX2200</td>
</tr>
</tbody>
</table>

**Required Privilege**
- **view-level**—To view this statement in the configuration.
- **control-level**—To add this statement to the configuration.

**Related Documentation**
- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- LCD Panel in EX3200 Switches
- LCD Panel in EX3300 Switches
- LCD Panel in EX4200 Switches
- LCD Panel in EX4500 Switches
- LCD Panel in EX4550 Switches
- LCD Panel in an EX6200 Switch
- LCD Panel in an EX8200 Switch
- LCD Panel in an XRE200 External Routing Engine

**disable**—(Optional) Disable the specified menu.
multicast-client

Syntax  multicast-client <address>;

Hierarchy Level  [edit system ntp]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  For NTP, configure the local router or switch to listen for multicast messages on the local network to discover other servers on the same subnet.

Options  address—(Optional) One or more IP addresses. If you specify addresses, the router or switch joins those multicast groups.

Default:  224.0.1.1.

Required Privilege Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  • Configuring the Router or Switch to Listen for Multicast Messages Using NTP
no-multicast-echo

Syntax  
no-multicast-echo {  
  arp {  
    aging-timer minutes;  
    gratuitous-arp-delay seconds;  
    gratuitous-arp-on-ifup;  
    interfaces {  
      interface-name {  
        aging-timer minutes;  
      }  
    }  
    passive-learning;  
    purging;  
  }  
  host-name hostname;  
  location {  
    altitude feet;  
    building name;  
    country-code code;  
    floor number;  
    hcoord horizontal-coordinate;  
    lata service-area;  
    latitude degrees;  
    longitude degrees;  
    npa-nx number;  
    postal-code postal-code;  
    rack number;  
    vcoord vertical-coordinate;  
  }  
  license {  
    autoupdate URL;  
    renew before-expiration (number | interval number)  
  }  
}

Hierarchy Level  [edit system]

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  Disable the Routing Engine from responding to ICMP echo requests sent to multicast group addresses.

Default  The Routing Engine responds to ICMP echo requests sent to multicast group addresses.

Required Privilege Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
Related Documentation

- Configuring the Junos OS to Disable the Routing Engine Response to Multicast Ping Packets

no-ping-record-route

Syntax

no-ping-record-route;

Hierarchy Level

[edit system]

Release Information

Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the Junos OS to disable the reporting of the IP address in ping responses.

Required Privilege

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses

no-ping-time-stamp

Syntax

no-ping-time-stamp;

Hierarchy Level

[edit system]

Release Information

Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the Junos OS to disable the recording of timestamps in ping responses.

Required Privilege

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Configuring the Junos OS to Disable the Reporting of IP Address and Timestamps in Ping Responses
no-redirects (IPv4 Traffic)

Syntax  
no-redirects;

Hierarchy Level  
[edit system],  
[edit interfaces interface-name unit logical-unit-number family family]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.  
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description  
Stop protocol redirect messages for IPv4 traffic from being sent on the entire switch or on an interface on the router or switch.

To disable the sending of protocol redirect messages for the entire router or switch, include the no-redirects statement at the [edit system] hierarchy level.

To disable the sending of protocol redirect messages on a specific interface, include the no-redirects statement at the [edit interfaces interface-name unit logical-unit-number family family] hierarchy level.

Default  
The router or switch sends redirect messages.

Required Privilege Level  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

Related Documentation  
• Configuring the Junos OS to Disable Protocol Redirect Messages on the Router or Switch  
• Understanding the Protocol Redirect Mechanism on EX Series Switches  
• Configuring Junos OS to Disable Sending Protocol Redirect Messages on EX Series Switches (CLI Procedure)  
• Junos OS Network Interfaces Library for Routing Devices
no-tcp-rfc1323-paws

Syntax       no-tcp-rfc1323-paws;
Hierarchy Level       [edit system internet-options]
Release Information       Statement introduced before Junos OS Release 7.4.
                            Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description       Configure the Junos OS to disable the RFC 1323 Protection Against Wrapped Sequence
                            (PAWS) number extension.
Required Privilege Level       system—To view this statement in the configuration.
                                  system-control—To add this statement to the configuration.
Related Documentation       • Configuring the Junos OS to Disable the TCP RFC 1323 PAWS Extension

no-tcp-rfc1323

Syntax       no-tcp-rfc1323;
Hierarchy Level       [edit system internet-options]
Release Information       Statement introduced before Junos OS Release 7.4.
                            Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description       Configure the Junos OS to disable RFC 1323 TCP extensions.
Required Privilege Level       system—To view this statement in the configuration.
                                  system-control—To add this statement to the configuration.
Related Documentation       • Configuring the Junos OS to Disable TCP RFC 1323 Extensions
ntp

Syntax  
ntp [ 
    authentication-key number type value password; 
    boot-server address; 
    broadcast <address> <key key-number> <version value> <ttl value>; 
    broadcast-client; 
    multicast-client <address>; 
    peer address <key key-number> <version value> <prefer>; 
    server address <key key-number> <version value> <prefer>; 
    source-address source-address; 
    trusted-key [ key-numbers ]; 
  ]

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4. 
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure NTP on the router or switch.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration. 
system-control—To add this statement to the configuration.

Related Documentation • Synchronizing and Coordinating Time Distribution Using NTP

path-mtu-discovery

Syntax (path-mtu-discovery | no-path-mtu-discovery);

Hierarchy Level [edit system internet-options]

Release Information Statement introduced before Junos OS Release 7.4. 
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure path MTU discovery for outgoing Transmission Control Protocol (TCP) connections:

• path-mtu-discovery—Path MTU discovery is enabled.
• no-path-mtu-discovery—Path MTU discovery is disabled.

Default Path MTU discovery is enabled.

Required Privilege Level system—To view this statement in the configuration. 
system-control—To add this statement to the configuration.

Related Documentation • Configuring the Junos OS for Path MTU Discovery on Outgoing TCP Connections
peer (NTP)

Syntax peer address <key key-number> <version value> <prefer>;

Hierarchy Level [edit system ntp]


Description For NTP, configure the local router or switch to operate in symmetric active mode with the remote system at the specified address. In this mode, the local router or switch and the remote system can synchronize with each other. This configuration is useful in a network in which either the local router or switch or the remote system might be a better source of time.

Options address—Address of the remote system. You must specify an address, not a hostname.

key key-number—(Optional) All packets sent to the address include authentication fields that are encrypted using the specified key number.

Range: Any unsigned 32-bit integer

prefer—(Optional) Mark the remote system as the preferred host, which means that if all other factors are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

version value—(Optional) Specify the NTP version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation • Configuring the NTP Time Server and Time Services
**port-type**

**Syntax**  
port-type (mini-usb | rj45);

**Hierarchy Level**  
[edit system ports auxiliary]

**Release Information**  
Statement introduced in Junos OS Release 11.3 for EX Series switches.

**Description**  
(EX2200-C and EX4550 switch only) Set the RJ-45 console port or the Mini-USB console port as the active console port.

**Default**  
The RJ-45 console port is the active port.

**Options**  
mini-usb—Set the Mini USB type-B console port as the active console port.

rj45—Set the RJ-45 console port as the active console port.

**Required Privilege**

**Level**

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring the Console Port Type (CLI Procedure)
ports

Syntax

```
ports {
  auxiliary {
    disable;
    insecure;
    type terminal-type;
    port-type (mini-usb | rj45);
  }
  console {
    disable;
    insecure;
    log-out-on-disconnect;
    type terminal-type;
  }
}
```

Hierarchy Level
[
editsystem\]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure the properties of the console and auxiliary ports. The ports are located on the router's craft interface.

See the switch's hardware documentation for port locations.

The remaining statements are explained separately.

Required Privilege
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Set Console and Auxiliary Port Properties
### power

**Syntax**

```plaintext
power (off | on);
```

**Hierarchy Level**

```
[edit chassis fpc slot]
```

**Release Information**

Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

On an EX6200 or EX8200 switch, turn a specified Flexible PIC Concentrator (FPC) on or off. See “EX Series Switches Hardware and CLI Terminology Mapping” on page 389.

**NOTE:** On an EX6200 switch, the power statement has no effect when you configure it for an uplink port FPC on the Switch Fabric and Routing Engine (SRE) module. If you configure the statement for those FPCs, the configuration will be committed, but a message that informs you that the configuration has no effect is logged in the system log. You cannot turn the power on and off for these FPCs.

**Options**

- **on**—Turn on the specified FPC.
- **off**—Turn off the specified FPC.

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- Removing a Line Card from an EX6200 Switch
processes

Syntax

processes {
  process-name (enable | disable) failover (alternate-media | other-routing-engine);
  timeout seconds;
}

Hierarchy Level  [edit system]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure which Junos OS processes are running on the router or switch.

CAUTION: Never disable any of the software processes unless instructed to do so by a customer support engineer.

Default  All processes are enabled by default.

Options

(enable | disable)—(Optional) Enable or disable a specified process.

failover (alternate-media | other-routing-engine)—(Optional) For routers or switches with
redundant Routing Engines only, switch to backup media if a process fails repeatedly.
If a process fails four times within 30 seconds, the router or switch reboots from
the alternate media or the other Routing Engine.

process-name—One of the valid process names. You can obtain a complete list of process
names by using the CLI command completion feature. After specifying a process
name, command completion also indicates any additional options for that process.

timeout seconds—(Optional) How often the system checks the watchdog timer, in seconds.
If the watchdog timer has not been checked in the specified number of seconds, the
system reloads. If you set the time value too low, it is possible for the system to
reboot immediately after it loads.

Values: 15, 60, or 180

Default: 180 seconds (rounded up to 291 seconds by the Junos kernel)

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

• Disabling Junos OS Processes
server (NTP)

Syntax

server address <key key-number> <version value> <prefer>;

Hierarchy Level

[edit system ntp]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

For NTP, configure the local router or switch to operate in client mode with the remote system at the specified address. In this mode, the local router or switch can be synchronized with the remote system, but the remote system can never be synchronized with the local router or switch.

Options

address—Address of the remote system. You must specify an address, not a hostname.

key key-number—(Optional) Use the specified key number to encrypt authentication fields in all packets sent to the specified address.

Range: Any unsigned 32-bit integer

prefer—(Optional) Mark the remote system as preferred host, which means that if all other things are equal, this remote system is chosen for synchronization among a set of correctly operating systems.

version value—(Optional) Specify the version number to be used in outgoing NTP packets.

Range: 1 through 4

Default: 4

Required Privilege

Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

• Configuring the NTP Time Server and Time Services
**tcp-drop-synfin-set**

**Syntax**
tcp-drop-synfin-set;

**Hierarchy Level**
[edit system internet-options]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the router or switch to drop packets that have both the SYN and FIN bits set.

**Required Privilege**
- **Level**
  - admin—To view this statement in the configuration.
  - admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring the Junos OS to Enable the Router or Switch to Drop Packets with the SYN and FIN Bits Set
- TCP Headers with SYN and FIN Flags Set
traceoptions (SBC Configuration Process)

Syntax

```plaintext
traceoptions {
    file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
    flag flag;
}
```

Hierarchy Level

[edit system processes sbc-configuration-process]

Release Information

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description

Configure trace options for the session border controller (SBC) process of the border signaling gateway (BSG).

Options

- `file filename`—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory `/var/log`. You can include the following file options:
  - `files number`—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
    If you specify a maximum number of files, you must also specify a maximum file size with the `size` option and a filename.
    **Range:** 2 through 1000
    **Default:** 3 files
  - `match regex`—(Optional) Refine the output to include lines that contain the regular expression.
  - `no-world-readable`—(Optional) Disable unrestricted file access.
  - `size size`—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When the trace-file again reaches its maximum size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.
    **Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB.
    **Range:** 10 KB through 1 GB
    **Default:** 128 KB
  - `world-readable`—(Optional) Enable unrestricted file access.
**flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all** trace-level—Trace all SBC process operations.
- **common** trace-level—Trace common events.
- **configuration** trace-level—Trace configuration events.
- **device-monitor** trace-level—Trace device monitor events.
- **ipc** trace-level—Trace IPC events.
- **memory**—pool trace-level—Trace memory pool events.
- **trace-level**—Trace level options are related to the severity of the event being traced. When you choose a trace level, messages at that level and higher levels are captured. Enter one of the following trace levels as the **trace-level**:
  - **debug**—Log all code flow of control.
  - **error**—Log failures with a short-term effect.
  - **info**—Log summary for normal operations, such as the policy decisions made for a call.
  - **trace**—Log program trace START and EXIT macros.
  - **warning**—Log failure recovery events or failure of an external entity.
- **ui** trace-level—Trace user interface operations.

**Required Privilege**

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

**Related Documentation**

- See “Troubleshooting the IMSG” in the *Junos Multiplay Solutions Guide*
- *System Management Configuration Statements*
trusted-key

Syntax
trusted-key [ key-numbers ];

Hierarchy Level
[edit system ntp]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
For NTP, configure the keys you are allowed to use when you configure the local router or switch to synchronize its time with other systems on the network.

Options
key-numbers—One or more key numbers. Each key can be any 32-bit unsigned integer except 0.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• Configuring NTP Authentication Keys
  • authentication-key on page 121
  • broadcast on page 124
  • peer on page 149
  • server on page 154
CHAPTER 5

Administration

- Operational Commands on page 159

Operational Commands
# clear chassis display message

**Syntax**

<table>
<thead>
<tr>
<th>Syntax (TX Matrix Router)</th>
<th>clear chassis display message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax (TX Matrix Plus Router)</td>
<td>clear chassis display message</td>
</tr>
<tr>
<td>Syntax (QFabric Systems)</td>
<td>clear chassis display message</td>
</tr>
</tbody>
</table>

**Release Information**

- Command introduced in Junos OS Release 7.5.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

(M40e, M160, M320, T Series routers, EX Series, and QFabric systems only) Clear or stop a text message on the craft interface display, which is on the front of the router or switch or on the LCD panel display on the router or switch. The craft interface alternates the display of text messages with standard craft interface messages, switching between messages every 2 seconds. By default, on both the router and the switch, the text message is displayed for 5 minutes. The craft interface display has four 20-character lines. The LCD panel display has two 16-character lines, and text messages appear only on the second line.

**Options**

- **none**—Clear or stop a text message on the craft interface display.
- **interconnect-device name**—(QFabric systems only) (Optional) On a QFabric system, clear or stop a text message on the LCD panel display on the specified Interconnect device.
- **lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number. Replace number with the following values depending on the LCC configuration:
  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
**node-device name**—(QFabric systems only) (Optional) On a QFabric system, clear or stop a text message on the LCD panel display on the specified Node device in a Node group.

**scc**—(TX Matrix routers only) (Optional) Clear or stop a text message on the craft interface on the TX Matrix router (switch-card chassis).

**sfc number**—(TX Matrix Plus routers only) (Optional) Clear or stop a text message on the craft interface on the TX Matrix Plus router (or switch-fabric chassis). Replace number with 0.

**Required Privilege Level**

clear

**Related Documentation**

- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- set chassis display message on page 223
- show chassis craft-interface

**List of Sample Output**

clear chassis display message on page 161

**Output Fields**

See show chassis craft-interface for an explanation of output fields.

**Sample Output**

clear chassis display message

The following example displays and then clears the text message on the craft interface display:

```
user@host> show chassis craft-interface
Red alarm:   LED off, relay off
Yellow alarm: LED off, relay off
Host OK LED:  On
Host fail LED: Off
FPCs  0  1  2  3  4  5  6  7

|---------------------|
Green  .. *.. * * |
Red     ........   
LCD screen:
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NOC contact Dusty</td>
</tr>
<tr>
<td>(888) 526-1234</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
</tbody>
</table>

user@host> clear chassis display message

user@host> show chassis craft-interface
Red alarm:   LED off, relay off
Yellow alarm: LED off, relay off
Host OK LED:  On
Host fail LED: Off
FPCs  0  1  2  3  4  5  6  7

|---------------------|
Green  .. *.. * * |
Red     ........   
LCD screen:
```

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>host</th>
<th>Up: 017:05:47</th>
<th>Temperature OK</th>
</tr>
</thead>
</table>
clear system reboot

### Syntax

**Syntax**

```
clear system reboot
<both-routing-engines>
```

**Syntax (EX Series Switches)**

```
clear system reboot
<all-members>
<both-routing-engines>
<local>
<member member-id>
```

**Syntax (TX Matrix Router)**

```
clear system reboot
<both-routing-engines>
<all-chassis | all-lcc | lcc number | scc>
```

**Syntax (TX Matrix Plus Router)**

```
clear system reboot
<both-routing-engines>
<all-chassis | all-lcc | lcc number | sfc number>
```

**Syntax (QFX Series)**

```
clear system reboot
<infrastructure name>
<interconnect-device name>
<node-group name>
```

### Release Information

- **Command introduced before Junos OS Release 7.4.**
- **Command introduced in Junos OS Release 9.0 for EX Series switches.**
- **sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.**
- **Command introduced in Junos OS Release 11.1 for the QFX Series.**

### Description

Clear any pending system software reboots or halts. When issued on a TX Matrix router without any options, the default behavior clears all pending system software reboots or halts on all T640 routers connected to the TX Matrix router. When issued on a TX Matrix Plus router without any options, the default behavior clears all pending system software reboots or halts on all T1600 or T4000 routers connected to the TX Matrix Plus router.

### Options

- **none**—Clear all pending system software reboots or halts.
  - **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Clear all halt or reboot requests for all the Routing Engines in the chassis.
  - **all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, clear all halt or reboot requests for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, clear all halt or reboot requests on the l connected T1600 or T4000 LCCs.
  - **all-members**—(EX4200 switches only) (Optional) Clear all halt or reboot requests on all members of the Virtual Chassis configuration.
  - **both-routing-engines**—(Systems with multiple Routing Engines) (Optional) Clear all halt or reboot requests on both Routing Engines. On a TX Matrix router, clear both Routing Engines on all chassis connected to the TX Matrix router. Likewise, on a TX Matrix
Plus router, clear both Routing Engines on all chassis connected to the TX Matrix Plus router.

**infrastructure name**—(QFabric systems) (Optional) Clear all halt or reboot requests on the fabric control Routing Engines or fabric manager Routing Engines.

**interconnect-device name**—(QFabric systems) (Optional) Clear all halt or reboot requests on the Interconnect device.

**lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, clear all halt or reboot requests for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, clear all halt or reboot requests for a specific router that is connected to the TX Matrix Plus router. Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(EX4200 switches only) (Optional) Clear all halt or reboot requests on the local Virtual Chassis member.

**member member-id**—(EX4200 switches only) (Optional) Clear all halt or reboot requests on the specified member of the Virtual Chassis configuration. Replace `member-id` with a value from 0 through 9.

**node-group name**—(QFabric systems) (Optional) Clear all halt or reboot requests on the Node group.

**scc**—(TX Matrix routers only) (Optional) Clear all halt or reboot requests for the TX Matrix router (or switch-card chassis).

**sfc number**—(TX Matrix Plus routers only) (Optional) Clear all halt or reboot requests for the TX Matrix Plus router. Replace `number` with 0.

**Required Privilege Level**

- maintenance

**Related Documentation**

- [request system reboot on page 191](#)
- [request system reboot](#)
- [Rebooting and Halting a QFX Series Product](#)
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)
List of Sample Output

- clear system reboot on page 166
- clear system reboot (TX Matrix Router) on page 166
- clear system reboot (QFX Series) on page 166

Output Fields

- When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear system reboot

```
user@host> clear system reboot
reboot requested by root at Sat Dec 12 19:37:34 1998
[process id 17855]
Terminating...
```

clear system reboot (TX Matrix Router)

```
user@host> clear system reboot
scc-re0:
---------------------------------------------------------------
No shutdown/reboot scheduled.
lcc0-re0:
---------------------------------------------------------------
No shutdown/reboot scheduled.
lcc2-re0:
---------------------------------------------------------------
No shutdown/reboot scheduled.
```

clear system reboot (QFX Series)

```
user@switch> clear system reboot node-group node1
No shutdown/reboot scheduled.
```
configure

Syntax

configure
<dynamic>
<exclusive>
<private>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Enter configuration mode. When this command is entered without any optional keywords, everyone can make configuration changes and commit all changes made to the configuration.

Options
none—Enter configuration mode.

dynamic—(Optional) Configure routing policies and certain routing policy objects in a dynamic database that is not subject to the same verification required in the standard configuration database. As a result, the time it takes to commit changes to the dynamic database is much shorter than for the standard configuration database. You can then reference these policies and policy objects in routing policies you configure in the standard database.

exclusive—(Optional) Lock the candidate configuration for as long as you remain in configuration mode, allowing you to make changes without interference from other users. Other users can enter and exit configuration mode, but they cannot change the configuration.

private—(Optional) Allow multiple users to edit different parts of the configuration at the same time and to commit only their own changes, or to roll back without interfering with one another's changes. You cannot commit changes in configure private mode when another user is in configure exclusive mode.

Additional Information
For more information about the different methods of entering configuration mode and the restrictions that apply, see the Junos OS Administration Library for Routing Devices.

Required Privilege
configure

Related Documentation
• show configuration on page 264

List of Sample Output
configure on page 168

Output Fields
When you enter this command, you are placed in configuration mode and the system prompt changes from hostname> to hostname#.
Sample Output

```
configure

user@host> configure
Entering configuration mode
[edit]
user@host#
```
op

Syntax

```
Syntax
op filename
<detail>
<argument-name argument-value>
<key (md5 | sha-256 | sha1) key-value
<url url>
```

Release Information

Command introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 9.0 for EX Series switches.
key option introduced in Junos OS Release 10.0.
url option introduced in Junos OS Release 10.0.

Description

Execute an op script stored in one of the following locations:

- On the router or switch in the `/var/db/scripts/op` directory
- At a remote URL

Options

detail—(Optional) Display detailed output.

`argument-name argument-value`—(Optional) Specify one or more arguments to the script. For each argument you include on the command line, you must specify a corresponding value for the argument.

`key (md5 | sha-256 | sha1) key-value`—(Optional) With the `<url>` option, specify a checksum hash to verify the integrity of the script. You can include the `<key>` option if the checksum statement is included at the `[edit system scripts op file filename]` hierarchy level.

`url url`—(Optional) Specify a URL where the script is located.

Additional Information

For more information about Junos op scripts, see the *Junos OS Automation Library*.

Required Privilege

```
Level
maintenance
```

Related Documentation

- **Executing an Op Script** in the *Junos OS Automation Library*
- **Executing an Op Script from a Remote Site** in the *Junos OS Automation Library*

- `checksum`
- `file checksum md5 on page 532`
- `file checksum sha-256 on page 534`
- `file checksum sha1 on page 533`

List of Sample Output

```
List of Sample Output
op on page 170
op url on page 170
```

Output Fields

When you enter this command, you are provided feedback on the status of your request.
Sample Output

op

user@host> op script1 interface ge-0/2/0.0 protocol inet

op url

user@host> op url https://www.juniper.net/fa/2009-04-01.01.slax key md5 8de24d09e1d90b2581bb937d2a5ad590 interface ge-0/2/0.0 protocol inet
request chassis pic

Syntax

request chassis pic (offline | online) fpc-slot slot-number pic-slot slot-number

Syntax (ACX4000 Series Routers)

request chassis pic (offline | online) fpc-slot slot-number pic-slot slot-number

Syntax (TX Matrix and TX Matrix Plus Routers)

request chassis pic (offline | online) fpc-slot slot-number pic-slot slot-number <lcc number>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.3 for ACX4000 Routers.

Description

Control the operation of the PIC.

NOTE: The request chassis pic (offline | online) fpc-slot slot-number pic-slot slot-number command is not supported for built-in PICs on MX Series routers.

To view a list of built-in PICs on the router or switch chassis, use the show chassis hardware command.

NOTE: T1600 routers and TX Matrix Plus routers with 100-Gigabit Ethernet PICs require two adjacent PIC slots, 0 and 1, for each PIC. Therefore, only online and offline command options to PIC slot 0 are allowed. Use of the online and offline command options for PIC slot 1 with the described router and PIC combination is not allowed.

NOTE: In T Series routers, when the PIC state is set from offline to online or vice-versa before the processing is complete for the previous command, you are provided feedback on the status of your request. The following sample messages are displayed if you try to set a PIC offline or online:

user@switch> request chassis pic fpc-slot 1 pic-slot 0 online
fpc 1 pic 0 online initiated, use "show chassis fpc pic-status" to verify

user@switch> request chassis pic fpc-slot 1 pic-slot 0 online
FPC 1 PIC 0 already transitioning to online

When the same PIC is set to a different state while the transition is in progress, you are provided feedback on the status of your request.

user@switch> request chassis pic fpc-slot 1 pic-slot 0 offline
FPC 1, PIC 0 already transitioning to online. Please retry later.
Options

- **offline**—Take the PIC offline.
- **online**—Bring the PIC online.
- **fpc-slot slot-number**—Flexible PIC Concentrator (FPC) slot number. Replace `slot-number` with a value appropriate for your router or switch:
  - ACX4000 routers—1 or 2.
  - EX Series switches:
    - EX3200 switches and EX4200 standalone switches—0.
    - EX4200 switches in a Virtual Chassis configuration—0 through 9 (switch’s member ID).
    - EX8208 switches—0 through 7 (line card).
    - EX8216 switches—0 through 15 (line card).
  - M5, M7i, M10, and M10i routers—0 or 1.
  - M20 routers—0 through 3.
  - M40 and M40e routers—0 through 7.
  - M120 routers—0 through 5.
  - M160 routers—0 through 7.
  - M320 routers—0 through 7.
  - MX 5, MX10, and MX40 routers—0 or 1.
  - MX80 routers—0 or 1.
  - MX240 routers—0 through 2
  - MX480 routers—0 through 5
  - MX2020 routers—0 through 19.
  - MX2010 routers—0 through 9.
  - MX960 routers—0 through 11.
  - PTX5000 routers—0 or 1.
  - T Series routers—0 through 7.
  - TX Matrix and TX Matrix Plus routers only—On a TX Matrix router, if you specify the number of the T640 router by using the **lcc number** option (the recommended method), replace `slot-number` with a value from 0 through 7. Otherwise, replace `slot-number` with a value from 0 through 31.
    - Likewise, on a TX Matrix Plus router, if you specify the **number** of the T1600 or T4000 router by using the lcc number option (the recommended method), replace `slot-number` with a value from 0 through 7. Otherwise, for the FPC slot number, replace `slot-number` with a value from 0 through 31. On a TX Matrix Plus router with 3D SIBs to assign the FPC slot number, replace `slot-number` with a value from 0 through 63. For example, the following commands have the same result:
user@host> request chassis pic fpc-slot 1 lcc 1 pic-slot 0 offline
user@host> request chassis pic fpc-slot 9 pic-slot 0 offline

**pic-slot slot-number**—PIC slot number.
- EX3200 and EX4200 switches—0 for built-in network interfaces and 1 for interfaces on uplink modules.
- EX8208 and EX8216 switches—0.
- M Series routers—0, 1, 2, or 3
- MX960 router—**slot-number** corresponds to the slot number of the Packet Forwarding Engine.
- PTX5000 routers—0 or 1.
- T320 router—0 or 1.
- T640 router—0, 1, 2, or 3.
- TI600 router —0, 1, 2, or 3.
- T4000 router—0, 1, 2, or 3.

**lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.
Replace number with the following values depending on the LCC configuration:
- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SiBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SiBs in a routing matrix.

**Required Privilege Level**
- maintenance

**Related Documentation**
- *show chassis hardware*
- *show chassis pic on page 1056*
- *Configuring the PIC Type*

**List of Sample Output**
- request chassis pic on page 174

**Output Fields**
- When you enter this command, you are provided feedback on the status of your request.
Sample Output
request chassis pic

user@host> request chassis pic-slot 0 online fpc-slot 0
FPC 0, PIC 0 is already online
### request chassis routing-engine master

**Syntax**

```bash
request chassis routing-engine master (acquire | release | switch)
<force>
<no-confirm>
```

**Syntax (TX Matrix Routers)**

```bash
request chassis routing-engine master (acquire | release | switch) (lcc number | scc | all-chassis)
<force>
<no-confirm>
```

**Syntax (TX Matrix Plus Routers)**

```bash
request chassis routing-engine master (acquire | release | switch) (lcc number | sfc | all-chassis | all-lcc)
<force>
<no-confirm>
```

**Syntax (MX Series Routers)**

```bash
request chassis routing-engine master (acquire | release | switch)
<all-members>
<force>
<local>
<member member-id>
<no-confirm>
```

**Syntax (MX104 3D Universal Edge Routers)**

```bash
request chassis routing-engine master (acquire | release | switch)
<no-confirm>
```

**Syntax (MX2010 and MX2020 3D Universal Edge Routers)**

```bash
request chassis routing-engine master (acquire | release | switch <check>)
<no-confirm>
```

**Syntax (QFX Series)**

```bash
request chassis routing-engine master (release | switch)
<check>
<interconnect-device name>
<node-group name>
<no-confirm>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- `all-chassis` option added in Junos OS Release 8.0.
- `sfc` option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.3 for QFX Series.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
- Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

**Description**

For routers or switches with multiple Routing Engines, control which Routing Engine is the master.

---

**CAUTION:** (Routing matrix based on the TX Matrix or TX Matrix Plus routers only) Within the routing matrix, we recommend that all Routing Engines run...
the same Junos OS Release. If you run different releases on the Routing Engines and a change in mastership occurs on any backup Routing Engine in the routing matrix, one or all routers (in a routing matrix based on the TX Matrix router or in a routing matrix based on a TX Matrix Plus router) might become logically disconnected from the TX Matrix router and cause data loss. For more information, see the TX Matrix Router Hardware Guide or the Junos OS High Availability Library for Routing Devices.

**NOTE:** Successive graceful Routing Engine switchover events must be a minimum of 240 seconds (4 minutes) apart after both Routing Engines have come up.

If the router or switch displays a warning message similar to “Standby Routing Engine is not ready for graceful switchover. Packet Forwarding Engines that are not ready for graceful switchover might be reset,” do not attempt switchover. If you choose to proceed with switchover, only the Packet Forwarding Engines that were not ready for graceful switchover are reset. None of the Flexible PIC concentrators (FPCs) should spontaneously restart. We recommend that you wait until the warning no longer appears and then proceed with the switchover.

You will receive an error message stating “Command aborted. Not ready for mastership switch, try after n seconds” when this command is re-entered before 240 seconds have elapsed on EX Series switches.

**NOTE:** On a QFabric system, to avoid traffic loss on the network Node group, switch mastership of the routing engine to the backup routing engine, and then reboot.

**Options**

- **acquire**—Attempt to become the master Routing Engine.
- **release**—Request that the other Routing Engine become the master.
- **switch**—Toggle mastership between Routing Engines.

The acquire, release, and switch options have the following suboptions:

- **all-chassis**—(TX Matrix and TX Matrix Plus routers only) On a routing matrix composed of a TX Matrix router and the attached T640 routers, switch mastership on all the Routing Engines in the routing matrix. Likewise, on a routing matrix composed of a TX Matrix Plus router and the attached T1600 or T4000 routers, switch mastership on all the Routing Engines in the routing matrix.
**all-lcc**—(TX Matrix Plus routers only) Request to acquire mastership for all line-card chassis (LCC).

**all-members**—(MX Series routers only) (Optional) Control Routing Engine mastership on the Routing Engines in all member routers of the Virtual Chassis configuration.

**check**—(QFabric systems, MX240, MX480, MX960, MX2010, and MX2020 routers only) (Optional) Available only with the `switch` option. Check graceful switchover status of the standby Routing Engine before toggling mastership between Routing Engines.

**interconnect-device name**—(QFabric systems only) (Optional) Control Routing Engine mastership on the Routing Engines on an Interconnect device.

**lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number. Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(MX Series routers only) (Optional) Control Routing Engine mastership on the Routing Engines in the local Virtual Chassis member.

**member member-id**—(MX Series routers only) (Optional) Control Routing Engine mastership on the Routing Engines of the specified member in the Virtual Chassis Configuration. Replace `member-id` with a value of 0 or 1.

**no-confirm**—(Optional) Do not request confirmation for the switch.

**node-group name**—(QFabric systems only) (Optional) Control Routing Engine mastership on the Routing Engines on a Node group.

**scc**—(TX Matrix routers only) TX Matrix (switch-card chassis).

**sfc**—(TX Matrix Plus routers only) TX Matrix Plus router (or switch-fabric chassis).

**force**—(Optional) Available only with the `acquire` option. Force the change to a new master Routing Engine.

---

**NOTE:** The force option is not supported on the MX104 router.
Because both Routing Engines are always running, the transition from one to the other as the master Routing Engine is immediate. However, the changeover interrupts communication to the System and Switch Board (SSB). The SSB takes several seconds to reinitialize the Flexible PIC Concentrators (FPCs) and restart the PICs. Interior gateway protocol (IGP) and BGP convergence times depend on the specific network environment.

By default, the Routing Engine in slot 0 (RE0) is the master and the Routing Engine in slot 1 (RE1) is the backup. To change the default master Routing Engine, include the routing-engine statement at the [edit chassis redundancy] hierarchy level in the configuration. For more information, see the Junos OS Administration Library for Routing Devices.

To have the backup Routing Engine become the master Routing Engine, use the request chassis routing-engine master switch command. If you use this command to change the master and then restart the chassis software for any reason, the master reverts to the default setting.

NOTE: Although the configurations on the two Routing Engines do not have to be the same and are not automatically synchronized, we recommend making both configurations the same.

Required Privilege Level
 maintenance

Related Documentation
- show chassis routing-engine on page 1070
- Configuring Routing Engine Redundancy
- Switching the Global Master and Backup Roles in a Virtual Chassis Configuration

List of Sample Output
request chassis routing-engine master acquire on page 178
request chassis routing-engine master switch on page 178

Sample Output
request chassis routing-engine master acquire

user@host> request chassis routing-engine master acquire
warning: Traffic will be interrupted while the PFE is re-initialized
warning: The other routing engine's file system could be corrupted
Reset other routing engine and become master ? [yes,no] (no)

request chassis routing-engine master switch

user@host> request chassis routing-engine master switch
warning: Traffic will be interrupted while the PFE is re-initialized
Toggle mastership between Routing Engines? [yes,no] (no) yes
Resolving mastership...
Complete. The other Routing Engine becomes the master.

Switch mastership back to the local Routing Engine:

user@host> request chassis routing-engine master switch

warning: Traffic will be interrupted while the PFE is re-initialized

Toggle mastership between routing engines? [yes,no] (no) yes
Resolving mastership...
Complete. The local routing engine becomes the master.
# request system halt

**Syntax**

```plaintext
request system halt
<at time>
<backup-routing-engine>
<both-routing-engines>
<other-routing-engine>
<in minutes>
<media (compact-flash | disk | removable-compact-flash | usb)>
<message "text">
```

**Syntax (EX Series Switches)**

```plaintext
request system halt
<all-members>
<at time>
<backup-routing-engine>
<both-routing-engines>
<in minutes>
<local>
<media (external | internal)>
<member member-id>
<message "text">
<other-routing-engine>
<slice slice>
```

**Syntax (PTX Series)**

```plaintext
request system halt
<at time>
<backup-routing-engine>
<both-routing-engines>
<other-routing-engine>
<in minutes>
<media (compact-flash | disk)>
<message "text">
```

**Syntax (TX Matrix Router)**

```plaintext
request system halt
<all-lcc | lcc number | lcc number>
<at time>
<backup-routing-engine>
<both-routing-engines>
<other-routing-engine>
<in minutes>
<media (compact-flash | disk)>
<message "text">
```

**Syntax (TX Matrix Plus Router)**

```plaintext
request system halt
<all-chassis | all-lcc | lcc number | sfc number>
<at time>
<backup-routing-engine>
<both-routing-engines>
<other-routing-engine>
<in minutes>
<media (compact-flash | disk)>
<message "text">
```
Syntax (MX Series Router)
request system halt
<all-members>
<at time>
<backup-routing-engine>
<both-routing-engines>
<in minutes>
<local>
<media (external | internal)>
<member member-id>
<message "text">
<other-routing-engine>

Syntax (QFX Series)
request system halt
<all-members>
<at time>
<director-device director-device-id>
<in minutes>
<local>
<media>
<member member-id>
<message "text">
<slice slice>

Release Information
Command introduced before Junos OS Release 7.4.
other-routing-engine option introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
director-device option introduced for QFabric systems in Junos OS Release 12.2.

Description
Stop the router or switch software.

NOTE: When you issue this command on an individual component in a QFabric system, you will receive a warning that says “Hardware-based members will halt, Virtual Junos Routing Engines will reboot.” If you want to halt only one member of a Node group, use the member option from the Node group CLI. You cannot issue this command from the QFabric CLI.

Options
none—Stop the router or switch software immediately.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Halt all chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, halt all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, halt all T1600 or T4000 routers connected to the TX Matrix Plus router.

all-members—(EX4200 switches and MX Series routers only) (Optional) Halt all members of the Virtual Chassis configuration.
at time — (Optional) Time at which to stop the software, specified in one of the following ways:

- now—Stop the software immediately. This is the default.
- +minutes—Number of minutes from now to stop the software.
- yymmdthhm—Absolute time at which to stop the software, specified as year, month, day, hour, and minute.
- hh:mm—Absolute time on the current day at which to stop the software.

backup-routing-engine — (Optional) Halt the backup Routing Engine. This command halts the backup Routing Engine, regardless from which Routing Engine the command is executed. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is halted. If you issue the command from the backup Routing Engine, the backup Routing Engine is halted.

both-routing-engines— (Optional) Halt both Routing Engines at the same time.

director-device director-device-id— (QFabric systems only) Halt a specific Director device.

lcc number— (TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, halt a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, halt a specific router that is connected to the TX Matrix Plus router.

Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local— (EX4200 switches and MX Series routers only) (Optional) Halt the local Virtual Chassis member.

in minutes— (Optional) Number of minutes from now to stop the software. This option is an alias for the at +minutes option.

media (compact-flash | disk | removable-compact-flash | usb) — (Optional) Boot medium for the next boot. (The options removable-compact-flash and usb pertain to J Series routers only.)

media (external | internal) — (EX Series and QFX Series switches and MX Series routers only) (Optional) Halt the boot media:

- external—Halt the external mass storage device.
- **internal**—Halt the internal flash device.

**member member-id**—(EX4200 switches and MX Series routers only) (Optional) Halt the specified member of the Virtual Chassis configuration. For EX4200 switches, replace `member-id` with a value from 0 through 9. For an MX Series Virtual Chassis, replace `member-id` with a value of 0 or 1.

**message "text"**—(Optional) Message to display to all system users before stopping the software.

**other-routing-engine**—(Optional) Halt the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is halted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is halted.

**scc**—(TX Matrix routers only) (Optional) Halt the TX Matrix router (or switch-card chassis).

**sfc number**—(TX Matrix Plus routers only) (Optional) Halt the TX Matrix Plus router (or switch-fabric chassis). Replace `number` with 0.

**slice slice**—(EX Series and QFX Series switches only) (Optional) Halt a partition on the boot media. This option has the following suboptions:
  - 1—Halt partition 1.
  - 2—Halt partition 2.
  - **alternate**—Reboot from the alternate partition.

**Additional Information**

On the M7i router, the `request system halt` command does not immediately power down the Packet Forwarding Engine. The power-down process can take as long as 5 minutes.

On a TX Matrix router and TX Matrix Plus router if you issue the `request system halt` command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are halted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are halted.

**NOTE:** If you have a router or switch with two Routing Engines and you want to shut the power off to the router or switch or remove a Routing Engine, you must first halt the backup Routing Engine (if it has been upgraded), and then halt the master Routing Engine. To halt a Routing Engine, issue the `request system halt` command. You can also halt both Routing Engines at the same time by issuing the `request system halt both-routing-engines` command.

**Required Privilege Level**

- maintenance

**Related Documentation**

- `clear system reboot` on page 163
- request system power-off on page 187
- Rebooting and Halting a QFX Series Product
- Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output

- request system halt on page 185
- request system halt (In 2 Hours) on page 185
- request system halt (Immediately) on page 185
- request system halt (At 1:20 AM) on page 185

Output Fields

When you enter this command, you are provided feedback on the status of your request.
Sample Output
request system halt

user@host> request system halt
Halt the system ? [yes,no] (no) yes

*** FINAL System shutdown message from root@section2 ***
System going down IMMEDIATELY
Terminated
...
syncing disks... 11 8 done
The operating system has halted.
Please press any key to reboot.

request system halt (In 2 Hours)

The following example, which assumes that the time is 5 PM (1700), illustrates three different ways to request that the system stop 2 hours from now:

user@host> request system halt at +120
user@host> request system halt in 120
user@host> request system halt at 19:00

request system halt (Immediately)

user@host> request system halt at now

request system halt (At 1:20 AM)

To stop the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

user@host> request system halt at yymmdh120
request system halt at 120
Halt the system at 120? [yes,no] (no) yes
request system logout

Syntax  
request system logout (pid pid | terminal terminal | user username)  
<all>

Release Information
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Log out users from the router or switch and the configuration database. If a user held the configure exclusive lock, this command clears the exclusive lock.

Options
all—(Optional) Log out all sessions owned by a particular PID, terminal session, or user.  
(On a TX Matrix or TX Matrix Plus router, this command is broadcast to all chassis.)  

pid pid—Log out the user session using the specified management process identifier (PID). The PID type must be management process.  

terminal terminal—Log out the user for the specified terminal session.  

user username—Log out the specified user.

Required Privilege
configure

Related Documentation
• Junos OS Administration Library for Routing Devices

List of Sample Output
request system logout on page 186

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
request system logout

user@host> request system logout user tammy all  
Connection closed by foreign host.
## request system power-off

**Syntax**
```
request system power-off
<both-routing-engines>
<other-routing-engine>
<at time>
<in minutes>
<media (compact-flash | disk | removable-compact-flash | usb)>
<message "text"/>
```

### Syntax (EX Series Switches)
```
request system power-off
<all-members>
<at time>
<both-routing-engines>
<in minutes>
<local>
<media (external | internal)>
<message member-member-id>
<message "text"/>
<other-routing-engine>
<slice slice>
```

### Syntax (TX Matrix Router)
```
request system power-off
<all-chassis | all-lcc | lcc number | scc>
<both-routing-engines>
<other-routing-engine>
<at time>
<in minutes>
<media (compact-flash | disk)>
<message "text"/>
```

### Syntax (TX Matrix Plus Router)
```
request system power-off
<all-chassis | all-lcc | lcc number | sfc number>
<both-routing-engines>
<other-routing-engine>
<at time>
<in minutes>
<media (compact-flash | disk)>
<message "text"/>
```

### Syntax (MX Series Router)
```
request system power-off
<all-members>
<at time>
<both-routing-engines>
<in minutes>
<local>
<media (external | internal)>
<message member-member-id>
<message "text"/>
<other-routing-engine>
```

### Syntax (QFX Series)
```
request system power-off
<at time>
```
Release Information
Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Power off the software.

NOTE: When you issue this command on an individual component in a QFabric system, you will receive a warning that says “Hardware-based members will halt, Virtual Junos Routing Engines will reboot.” If you want to halt only one member, use the member option. You cannot issue this command from the QFabric CLI.

Options
none—Power off the router or switch software immediately.

all-chassis—(Optional) (TX Matrix and TX Matrix Plus router only) Power off all Routing Engines in the chassis.

all-lcc—(Optional) (TX Matrix and TX Matrix Plus router only) On a TX Matrix router, power off all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, power off all T1600 routers (or line-card chassis) connected to the TX Matrix Plus router.

all-members—(EX4200 switches and MX Series routers only) (Optional) Power off all members of the Virtual Chassis configuration.

at time—(Optional) Time at which to power off the software, specified in one of the following ways:

  • now—Power off the software immediately. This is the default.
  • +minutes—Number of minutes from now to power off the software.
  • yymmdthhmm—Absolute time at which to power off the software, specified as year, month, day, hour, and minute.
  • hh:mm—Absolute time on the current day at which to power off the software.

both-routing-engines—(Optional) Power off both Routing Engines at the same time.

in minutes—(Optional) Number of minutes from now to power off the software. This option is an alias for the at +minutes option.

lcc number—(Optional) (TX Matrix and TX Matrix Plus router only) On a TX Matrix router, power off a T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, power off a specific router that is connected to the TX Matrix Plus router.
Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Power off the local Virtual Chassis member.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Boot medium for the next boot. (The options removable-compact-flash and usb pertain to the J Series routers only.)

media (external | internal)—(EX Series and QFX Series switches and MX Series routers only) (Optional) Power off the boot media:
- external—Power off the external mass storage device.
- internal—Power off the internal flash device.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Power off the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

message "text"—(Optional) Message to display to all system users before powering off the software.

other-routing-engine—(Optional) Power off the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is halted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is halted.

scc—(Optional) (TX Matrix router only) Power off only the master Routing Engine or the backup Routing Engine on the TX Matrix router (or switch-card chassis). If you issue the command from the master Routing Engine, the master SCC is powered off. If you issue the command from the backup Routing Engine, the backup SCC is powered off.

sfc number—(Optional) (TX Matrix Plus router only) Power off only the master Routing Engine or the backup Routing Engine on the TX Matrix Plus router (or switch-fabric chassis). If you issue the command from the master Routing Engine, the master SFC is powered off. If you issue the command from the backup Routing Engine, the backup SFC is powered off. Replace number with zero.
slice slice—(EX Series and QFX Series switches only) (Optional) Power off a partition on the boot media. This option has the following suboptions:
  • 1—Power off partition 1.
  • 2—Power off partition 2.
  • alternate—Reboot from the alternate partition.

Additional Information
On a routing matrix composed of a TX Matrix router and T640 routers, if you issue the request system power-off command on the TX Matrix master Routing Engine, all the master Routing Engines connected to the routing matrix are powered off. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are powered off.

Likewise, on a routing matrix composed of a TX Matrix Plus router and T1600 routers, if you issue the request system power-off command on the TX Matrix Plus master Routing Engine, all the master Routing Engines connected to the routing matrix are powered off. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are powered off.

If you issue the request system power-off both-routing-engines command on the TX Matrix or TX Matrix Plus router, all the Routing Engines on the routing matrix are powered off.

Required Privilege
Level
maintenance

List of Sample Output
request system power-off on page 190

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system power-off

user@host> request system power-off message "This router will be powered off in 30 minutes. Please save your data and log out immediately."
warning: This command will not halt the other routing-engine. If planning to switch off power, use the both-routing-engines option.
Power Off the system? [yes,no] (no) yes

*** FINAL System shutdown message from remote@nutmeg ***
System going down IMMEDIATELY

This router will be powered off in 30 minutes. Please save your data and log out immediately.

Shutdown NOW!
[pid 5177]
request system reboot

Syntax  
request system reboot  
<at time>  
<both-routing-engines>  
<in minutes>  
<media (compact-flash | disk | removable-compact-flash | usb)>  
<message "text">  
<other-routing-engine>

Syntax (EX Series Switches)  
request system reboot  
<all-members>  
<at time>  
<both-routing-engines>  
<in minutes>  
<local>  
<media (external | internal)>  
<member member-id>  
<message "text">  
<other-routing-engine>  
<slice slice>

Syntax (TX Matrix Router)  
request system reboot  
<all-chassis | all-lcc | lcc number | scc>  
<at time>  
<both-routing-engines>  
<in minutes>  
<media (compact-flash | disk)>  
<message "text">  
<other-routing-engine>  

Syntax (TX Matrix Plus Router)  
request system reboot  
<all-chassis | all-lcc | lcc number | sfc number>  
<at time>  
<both-routing-engines>  
<in minutes>  
<media (compact-flash | disk)>  
<message "text">  
<other-routing-engine>  
<partition (1 | 2 | alternate)>

Syntax (MX Series Router)  
request system reboot  
<all-members>  
<at time>  
<both-routing-engines>  
<in minutes>  
<local>  
<media (external | internal)>  
<member member-id>  
<message "text">  
<other-routing-engine>

Release Information  
Command introduced before Junos OS Release 7.4.
Option **other-routing-engine** introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Option **both-routing-engines** introduced in Junos OS Release 12.1.

**Description**
Reboot the software.

**Options**

- **none**—Reboot the software immediately.
- **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.
- **all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.
- **all-members**—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.
- **at time**—(Optional) Time at which to reboot the software, specified in one of the following ways:
  - **now**—Stop or reboot the software immediately. This is the default.
  - **+minutes**—Number of minutes from now to reboot the software.
  - **yymmddhhmm**—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
  - **hh:mm**—Absolute time on the current day at which to stop the software, specified in 24-hour time.
- **both-routing-engines**—(Optional) Reboot both Routing Engines at the same time.
- **in minutes**—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at +minutes** option.
- **lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.
  Replace **number** with the following values depending on the LCC configuration:
  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
local—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the local Virtual Chassis member.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Boot medium for next boot. (The options removable-compact-flash and usb pertain to the J Series routers only.)

media (external | internal)—(EX Series switches and MX Series routers only) (Optional) Reboot the boot media:

  • external—Reboot the external mass storage device.
  • internal—Reboot the internal flash device.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

message "text”—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition—(TX Matrix Plus routers only) (Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

  • 1—Reboot from partition 1.
  • 2—Reboot from partition 2.
  • alternate—Reboot from the alternate partition.

scc—(TX Matrix routers only) (Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

sfc number—(TX Matrix Plus routers only) (Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace number with 0.
	slice slice—(EX Series switches only) (Optional) Reboot a partition on the boot media. This option has the following suboptions:

  • 1—Power off partition 1.
  • 2—Power off partition 2.
  • alternate—Reboot from the alternate partition.
Additional Information

Reboot requests are recorded in the system log files, which you can view with the `show log` command (see `show log`). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the `show system processes` command (see `show system processes`).

On a TX Matrix or TX Matrix Plus router, if you issue the `request system reboot` command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.

---

**NOTE:** Before issuing the `request system reboot` command on a TX Matrix Plus router with no options or the all-chassis, all-lcc, lcc `number`, or sfc options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the `request system reboot` command.

---

**NOTE:** To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

---

**Required Privilege Level**

maintenance

**Related Documentation**

- clear system reboot on page 163
- request system halt on page 180
- request system reboot
- *Rebooting and Halting a QFX Series Product*
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

**List of Sample Output**

- request system reboot on page 195
- request system reboot (at 2300) on page 195
- request system reboot (in 2 Hours) on page 195
- request system reboot (Immediately) on page 195
- request system reboot (at 1:20 AM) on page 195

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.
Sample Output
request system reboot

user@host> request system reboot
Reboot the system ? [yes,no] (no)

request system reboot (at 2300)

user@host> request system reboot at 2300 message?Maintenance time? 
Reboot the system ? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00

request system reboot (in 2 Hours)
The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00

request system reboot (Immediately)

user@host> request system reboot at now

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
**request system reboot**

**Syntax**

```plaintext
request system reboot
<all-members | local | member member-id>
<at time>
<in minutes>
<media (external | internal)>
<message “text”>
<slice (1 | 2 | alternate)>
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches. Option `partition` changed to `slice` in Junos OS Release 10.0 for EX Series switches.

**Description**

Reboot the Junos OS.

Reboot requests are recorded in the system log files, which you can view with the `show log` command. You can view the process names with the `show system processes` command.

**Options**

- **none**—Reboots the software immediately.
- **all-members | local | member member-id**—(EX4200 switch only) (Optional) Specify which member of the Virtual Chassis to reboot:
  - **all-members**—Reboots each switch that is a member of the Virtual Chassis.
  - **local**—Reboots the local switch, meaning the switch you are logged into, only.
  - **member member-id**—Reboots the specified member switch of the Virtual Chassis.
- **at time**—(Optional) Time at which to reboot the software, specified in one of the following ways:
  - **+minutes**—Number of minutes from now to reboot the software.
  - **hh:mm**—Absolute time on the current day at which to reboot the software, specified in 24-hour time.
  - **now**—Stop or reboot the software immediately. This is the default.
  - **yymmdthhmm**—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.

- **in minutes**—(Optional) Number of minutes from now to reboot the software. This option is an alias for the `at +minutes` option.
- **media (external | internal)**—(Optional) Boot medium for the next boot. The external option reboots the switch using a software package stored on an external boot source, such as a USB flash drive. The internal option reboots the switch using a software package stored in an internal memory source.
- **message “text”**—(Optional) Message to display to all system users before rebooting the software.
slice (1 | 2 | alternate)—(Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

- 1—Reboot from partition 1.
- 2—Reboot from partition 2.
- alternate—Reboot from the alternate partition, which is the partition that did not boot the switch at the last bootup.

Required Privilege Level

maintenance

Related Documentation

- clear system reboot on page 163

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

user@host> request system reboot
Reboot the system? [yes,no] (no)

request system reboot (at 2300)

user@host> request system reboot at 2300 message?Maintenance time!? Reboot the system? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

user@host> request system reboot at+120
user@host> request system reboot in 120
user@host> request system reboot at 19:00

request system reboot (immediately)

user@host> request system reboot at now

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
request system scripts convert

Syntax
```
request system scripts convert (slax-to-xslt | xslt-to-slax) source source/filename
destination destination/ <filename> <partial> <version (1.0 | 1.1)>
```

Release Information
Command introduced in Junos OS Release 8.2.
Command introduced in Junos OS Release 9.0 for EX Series switches.
partial and version options added in Junos OS Release 12.2.

Description
Convert an Extensible Stylesheet Language Transformations (XSLT) script to Stylesheet Language, Alternative syntax (SLAX), or convert a SLAX script to XSLT.

Options
```
destination destination/ <filename>—Specify a destination for the converted file.
```
Optionally, you can specify a filename for the converted file. If you do not specify a filename, the software assigns one automatically. The default destination filename is `SLAX-Conversion-Temp` or `slax-temp` depending on the Junos OS release, with a randomly generated, five-character, alpha-numeric extension. For example, the software converts a source file called `test.xsl` to `slax-temp.kWwQk`. The software converts a source file called `test1.slax` to `slax-temp.zN61h`.

```
partial—(Optional) Convert partial script input.
```

```
slax-to-xslt—Convert a SLAX script to XSLT.
```

```
source source/filename—Specify a source file that you want to convert.
```

```
version—(Optional) Specify the SLAX version listed in the version statement of the generated script for XSLT-to-SLAX conversions. Acceptable values are 1.0 and 1.1. The default is 1.1.
```

```
xslt-to-slax—Convert an XSLT script to SLAX.
```

Required Privilege Level
maintenance

Related Documentation
- Converting Scripts Between SLAX and XSLT

List of Sample Output
request system scripts convert slax-to-xslt on page 198
request system scripts convert xslt-to-slax on page 199

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
request system scripts convert slax-to-xslt
```
user@host> request system scripts convert slax-to-xslt source /var/db/scripts/op/script1.slax
destination /var/db/scripts/op
conversion complete
```
request system scripts convert xslt-to-slax

user@host> request system scripts convert xslt-to-slax source /var/db/scripts/commit/script1.xsl
destination /var/db/scripts/commit partial version 1.0
conversion complete
**request system scripts refresh-from commit**

**Syntax**

```
request system scripts refresh-from commit file file-name url url-path
```

**Release Information**

Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Automatically download the initial Junos OS configuration and a set of standard commit scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:

```
<request-script-refresh-from>
  <type>commit</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

**Options**

- `file file-name` — Name of the file to be downloaded.
- `url url-path` — URL of the file to be downloaded.

**Required Privilege Level**

maintenance

**Related Documentation**

- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- *Junos OS NETCONF XML Management Protocol Guide*

**List of Sample Output**

```
request system scripts refresh-from commit file config.txt url http://host1.juniper.net on page 200
```

**Sample Output**

```
user@switch> request system scripts refresh-from commit file config.txt url http://host1.juniper.net
http://host1.juniper.net
user@switch>
```
request system scripts refresh-from event

Syntax

request system scripts refresh-from event file file-name url url-path

Release Information


Description

Automatically download the initial Junos OS configuration and a set of standard event scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:

```
<request-script-refresh-from>
  <type>event</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

Options

- **file file-name**—Name of the file to be downloaded.
- **url url-path**—URL of the file to be downloaded.

Required Privilege

- Level: maintenance

Related Documentation

- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Junos OS NETCONF XML Management Protocol Guide

List of Sample Output

request system scripts refresh-from event file config.txt url http://host1.juniper.net on page 201

Sample Output

```
user@switch> request system scripts refresh-from event file config.txt url http://host1.juniper.net
```

Copyright © 2013, Juniper Networks, Inc.
**request system scripts refresh-from op**

**Syntax**
```
request system scripts refresh-from op file file-name url url-path
```

**Release Information**
Command introduced in Junos OS Release 10.1 for EX Series switches.

**Description**
Automatically download the initial Junos OS configuration and a set of standard op scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:

```
<request-script-refresh-from>
  <type>op</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

**Options**
- **file file-name**—Name of the file to be downloaded.
- **url url-path**—URL of the file to be downloaded.

**Required Privilege Level**
maintenance

**Related Documentation**
- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Junos OS NETCONF XML Management Protocol Guide

**List of Sample Output**
```
request system scripts refresh-from op file config.txt url http://host1.juniper.net
```

**Sample Output**
```
user@switch> request system scripts refresh-from op file config.txt url http://host1.juniper.net
user@switch>
```
request system storage cleanup

Syntax
request system storage cleanup <dry-run>

Syntax (EX Series Switches)
request system storage cleanup
<all-members>
<dry-run>
<local>
<member member-id>

Syntax (MX Series Router)
request system storage cleanup
<all-members>
<dry-run>
<local>
<member member-id>

Syntax (QFX Series)
request system storage cleanup
<component (serial number | UUID | all)>
<director-group name>
<dry-run>
<infrastructure name>
<interconnect-device name>
<name-tag name-tag>
<node-group name>
<prune>
<qfabric (component name) | dry-run | name-tag | repository)>
<repository (core | log)>

Release Information
Command introduced in Junos OS Release 7.4.
dry-run option introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Free storage space on the router or switch by rotating log files and proposing a list of files for deletion. User input is required for file deletion. On a QFabric system, you can delete debug files located on individual devices or on the entire QFabric system.

Options
all-members—(EX4200 switches and MX Series routers only) (Optional) Delete files on the Virtual Chassis master Routing Engine only.

custom (UUID | serial number | all)—(QFabric systems only) (Optional) Delete files located on individual QFabric system devices or on the entire QFabric system.

director-group name—(QFabric systems only) (Optional) Delete files on the Director group.

NOTE: To delete files on the other members of the Virtual Chassis configuration, log in to each backup Routing Engine and delete the files using the request system storage cleanup local command.
**dry-run**—(Optional) List files proposed for deletion (without deleting them).


**interconnect-device name**—(QFabric systems only) (Optional) Delete files on the Interconnect device.

**local**—(EX4200 switches and MX Series routers only) (Optional) Delete files on the local Virtual Chassis member.

**member member-id**—(EX4200 switches and MX Series routers only) (Optional) Delete files on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace `member-id` with a value from 0 through 9. For an MX Series Virtual Chassis, replace `member-id` with a value of 0 or 1.

**name-tag name-tag**—(QFabric systems only) (Optional) Delete debug files that match a specific regular expression.

**node-group name**—(QFabric systems only) (Optional) Delete files on the Node group.

**prune**—(QFabric systems only) (Optional) Delete debug files located in either the core or log debug repositories of a QFabric system device.

**qfabric component name**—(QFabric systems only) (Optional) Delete debug files located in the debug repositories of a QFabric system device.

**repository (core | log)**—(QFabric systems only) (Optional) Specify the repository on the QFabric system device for which you want to delete debug files.

**Additional Information**
If logging is configured and being used, the **dry-run** option rotates the log files. In that case, the output displays the message “Currently rotating log files, please wait.” If no logging is currently under way, the output displays only a list of files to delete.

**Required Privilege Level**
maintenance

**List of Sample Output**
request system storage cleanup dry-run on page 205
request system storage cleanup on page 206
request system storage cleanup director-group (QFabric Systems) on page 206
request system storage cleanup infrastructure device-name (QFabric Systems) on page 208
request system storage cleanup interconnect-device device-name (QFabric Systems) on page 209
request system storage cleanup node-group group-name (QFabric Systems) on page 210
request system storage cleanup qfabric component device-name (QFabric Systems) on page 211
request system storage cleanup qfabric component device-name repository core (QFabric Systems) on page 211
request system storage cleanup qfabric component all (QFabric Systems) on page 211
Output Fields  

Table 65 on page 205 describes the output fields for the request system storage cleanup command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of files to delete:</td>
<td>Shows list of files available for deletion.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the core-dump file.</td>
</tr>
<tr>
<td>Date</td>
<td>Last core-dump file modification date and time.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the core-dump file.</td>
</tr>
<tr>
<td>Directory to delete:</td>
<td>Shows list of directories available for deletion.</td>
</tr>
<tr>
<td>Repository scope:</td>
<td>Repository where core-dump files and log files are stored. The core-dump files are located in the core repository, and the log files are located in the log repository. The default Repository scope is shared since both the core and log repositories are shared by all of the QFabric system devices.</td>
</tr>
<tr>
<td>Repository head:</td>
<td>Name of the top-level repository location.</td>
</tr>
<tr>
<td>Repository name:</td>
<td>Name of the repository: core or log.</td>
</tr>
<tr>
<td>Creating list of debug artifacts to be removed under:</td>
<td>Shows location of files available for deletion.</td>
</tr>
<tr>
<td>List of debug artifacts to be removed under:</td>
<td>Shows list of files available for deletion.</td>
</tr>
</tbody>
</table>

Sample Output

request system storage cleanup dry-run

user@host> request system storage cleanup dry-run
Currently rotating log files, please wait.
This operation can take up to a minute.

List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.4K</td>
<td>Mar 8 15:00</td>
<td>/var/log/messages.1.gz</td>
</tr>
<tr>
<td>7245B</td>
<td>Feb 5 15:00</td>
<td>/var/log/messages.3.gz</td>
</tr>
<tr>
<td>11.8K</td>
<td>Feb 22 13:00</td>
<td>/var/log/messages.2.gz</td>
</tr>
<tr>
<td>3926B</td>
<td>Mar 16 13:57</td>
<td>/var/log/messages.0.gz</td>
</tr>
<tr>
<td>3962B</td>
<td>Feb 22 12:47</td>
<td>/var/log/sampled.1.gz</td>
</tr>
<tr>
<td>4146B</td>
<td>Mar 8 12:20</td>
<td>/var/log/sampled.0.gz</td>
</tr>
<tr>
<td>4708B</td>
<td>Dec 21 11:39</td>
<td>/var/log/sampled.2.gz</td>
</tr>
<tr>
<td>7068B</td>
<td>Jan 16 18:00</td>
<td>/var/log/messages.4.gz</td>
</tr>
<tr>
<td>13.7K</td>
<td>Dec 27 22:00</td>
<td>/var/log/messages.5.gz</td>
</tr>
<tr>
<td>890B</td>
<td>Feb 22 17:22</td>
<td>/var/tmp/sampled.pkts</td>
</tr>
</tbody>
</table>
request system storage cleanup

user@host> request system storage cleanup
Currently rotating log files, please wait.
This operation can take up to a minute.

List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.4K</td>
<td>Mar 8 15:00</td>
<td>/var/log/messages.1.gz</td>
</tr>
<tr>
<td>7245B</td>
<td>Feb 5 15:00</td>
<td>/var/log/messages.3.gz</td>
</tr>
<tr>
<td>11.8K</td>
<td>Feb 22 13:00</td>
<td>/var/log/messages.2.gz</td>
</tr>
<tr>
<td>3926B</td>
<td>Mar 16 13:57</td>
<td>/var/log/messages.0.gz</td>
</tr>
<tr>
<td>11.6K</td>
<td>Mar 8 15:00</td>
<td>/var/log/messages.5.gz</td>
</tr>
<tr>
<td>7254B</td>
<td>Feb 5 15:00</td>
<td>/var/log/messages.6.gz</td>
</tr>
<tr>
<td>12.9K</td>
<td>Feb 22 13:00</td>
<td>/var/log/messages.8.gz</td>
</tr>
<tr>
<td>3726B</td>
<td>Mar 16 13:57</td>
<td>/var/log/messages.7.gz</td>
</tr>
<tr>
<td>3962B</td>
<td>Feb 22 12:47</td>
<td>/var/log/sampled.1.gz</td>
</tr>
<tr>
<td>4146B</td>
<td>Mar 8 12:20</td>
<td>/var/log/sampled.0.gz</td>
</tr>
<tr>
<td>4708B</td>
<td>Dec 21 11:39</td>
<td>/var/log/sampled.2.gz</td>
</tr>
<tr>
<td>7068B</td>
<td>Jan 16 18:00</td>
<td>/var/log/messages.4.gz</td>
</tr>
<tr>
<td>13.7K</td>
<td>Dec 27 22:00</td>
<td>/var/log/messages.5.gz</td>
</tr>
<tr>
<td>890B</td>
<td>Feb 22 17:22</td>
<td>/var/tmp/sampled.pkts</td>
</tr>
</tbody>
</table>

Delete these files? [yes,no] (yes)

request system storage cleanup director-group (QFabric Systems)

user@switch> request system storage cleanup director-group
List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:16:29</td>
<td>/tmp/2064.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:07:34</td>
<td>/tmp/30804.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:13:41</td>
<td>/tmp/26792.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:13:39</td>
<td>/tmp/26432.sfcauth</td>
</tr>
<tr>
<td>0</td>
<td>2011-11-07 07:45:40</td>
<td>/tmp/cluster_cleanup.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 07:36:29</td>
<td>/tmp/clustat.28019.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 07:36:29</td>
<td>/tmp/clustat.x.28019.log</td>
</tr>
<tr>
<td>9.6M</td>
<td>2011-11-07 05:30:24</td>
<td>/tmp/sfc.2.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:28:11</td>
<td>/tmp/mgd-init.1320672491.log</td>
</tr>
<tr>
<td>248K</td>
<td>2011-11-07 05:19:24</td>
<td>/tmp/cn_monitor.20111107-045111.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:17:18</td>
<td>/tmp/clustat.3401.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:17:18</td>
<td>/tmp/clustat_x.3401.log</td>
</tr>
<tr>
<td>8.0K</td>
<td>2011-11-07 04:58:25</td>
<td>/tmp/mgd-init.1320670633.log</td>
</tr>
<tr>
<td>0</td>
<td>2011-11-07 04:54:01</td>
<td>/tmp/mysql_db_install_5.1.37.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:52:08</td>
<td>/tmp/cn_send.log</td>
</tr>
<tr>
<td>0</td>
<td>2011-11-07 04:52:00</td>
<td>/tmp/init_eth0.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:49:35</td>
<td>/tmp/install_interfaces.sh.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:48:15</td>
<td>/tmp/bootstrap.sh.log</td>
</tr>
<tr>
<td>38M</td>
<td>2011-11-07 04:42:42</td>
<td>/tmp/cn_monitor.20111104-110308.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:38:47</td>
<td>/tmp/clustat.30913.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:38:47</td>
<td>/tmp/clustat_x.30913.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 04:38:03</td>
<td>/tmp/dcf_upgrade.sh.remove.log</td>
</tr>
</tbody>
</table>
List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0K</td>
<td>2011-11-10 05:47:47</td>
<td>/tmp/5713.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 05:14:32</td>
<td>/tmp/14494.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 05:11:47</td>
<td>/tmp/9978.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 05:09:37</td>
<td>/tmp/6128.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 05:04:28</td>
<td>/tmp/29703.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 11:59:10</td>
<td>/tmp/12131.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 11:36:08</td>
<td>/tmp/32415.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 11:30:30</td>
<td>/tmp/22406.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 11:24:37</td>
<td>/tmp/12131.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 10:48:42</td>
<td>/tmp/12687.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 09:27:20</td>
<td>/tmp/31082.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 07:33:58</td>
<td>/tmp/14633.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 05:08:25</td>
<td>/tmp/15447.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 04:12:29</td>
<td>/tmp/26874.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 04:12:27</td>
<td>/tmp/26713.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 03:49:17</td>
<td>/tmp/17691.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 01:32:23</td>
<td>/tmp/5716.sfcauth</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 00:08:17</td>
<td>/tmp/sfcsnmpd.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-10 07:57:50</td>
<td>/tmp/cluster_cleanup.log</td>
</tr>
<tr>
<td>824K</td>
<td>2011-11-07 07:38:37</td>
<td>/tmp/cn_monitor.20111107-053643.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 07:36:30</td>
<td>/tmp/clustat.18399.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 07:36:30</td>
<td>/tmp/clustat.x.18399.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 07:35:47</td>
<td>/tmp/command_lock.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:39:54</td>
<td>/tmp/mdg-init.1320673194.log</td>
</tr>
<tr>
<td>92K</td>
<td>2011-11-07 05:19:25</td>
<td>/tmp/cn_monitor.20111107-050412.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:17:20</td>
<td>/tmp/clustat.30115.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:17:20</td>
<td>/tmp/clustat.x.30115.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:08:07</td>
<td>/tmp/mdg-init.1320671241.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:04:57</td>
<td>/tmp/cn_send.log</td>
</tr>
<tr>
<td>0</td>
<td>2011-11-07 05:04:52</td>
<td>/tmp/init_eth0.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:02:38</td>
<td>/tmp/install_interfaces.sh.log</td>
</tr>
<tr>
<td>4.0K</td>
<td>2011-11-07 05:01:19</td>
<td>/tmp/bootstrap.sh.log</td>
</tr>
<tr>
<td>160K</td>
<td>2011-11-07 05:00:47</td>
<td>/tmp/bootstrap_cleanup.log</td>
</tr>
</tbody>
</table>
Directory to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1398</td>
<td>Nov 8 19:03</td>
<td>/var/log/default-log-messages.0.gz</td>
</tr>
<tr>
<td>5602B</td>
<td>Nov 8 19:03</td>
<td>/var/log/messages.0.gz</td>
</tr>
<tr>
<td>28.4K</td>
<td>Nov 8 10:15</td>
<td>/var/log/messages.1.gz</td>
</tr>
<tr>
<td>35.2K</td>
<td>Nov 7 13:45</td>
<td>/var/log/messages.2.gz</td>
</tr>
<tr>
<td>2078</td>
<td>Nov 7 16:02</td>
<td>/var/log/wtmp.0.gz</td>
</tr>
<tr>
<td>278</td>
<td>Nov 7 12:14</td>
<td>/var/log/wtmp.1.gz</td>
</tr>
<tr>
<td>184.4M</td>
<td>Nov 7 12:16</td>
<td>/var/sw/pkg/jinstall-dc-re-11.3I20111104_1216_dc-builder-domestic-signed.tgz</td>
</tr>
<tr>
<td>124.0K</td>
<td>Nov 7 15:59</td>
<td>/var/tmp/gres-tp/env.dat</td>
</tr>
<tr>
<td>0</td>
<td>Nov 7 12:57</td>
<td>/var/tmp/gres-tp/lock</td>
</tr>
<tr>
<td>155B</td>
<td>Nov 7 16:02</td>
<td>/var/tmp/krt_genconfig_filter.txt</td>
</tr>
<tr>
<td>0</td>
<td>Nov 7 12:35</td>
<td>/var/tmp/last_ccif_update</td>
</tr>
<tr>
<td>1217B</td>
<td>Nov 7 12:15</td>
<td>/var/tmp/loader.conf.preinstall</td>
</tr>
<tr>
<td>184.4M</td>
<td>Nov 6 07:11</td>
<td>/var/tmp/mchassis-install.tgz</td>
</tr>
<tr>
<td>10.8M</td>
<td>Nov 7 12:16</td>
<td>/var/tmp/preinstall/bootstrap-install-11.3I20111104_1216_dc-builder.tar</td>
</tr>
<tr>
<td>57.4K</td>
<td>Nov 7 12:16</td>
<td>/var/tmp/preinstall/configs-11.3I20111104_1216_dc-builder.tgz</td>
</tr>
<tr>
<td>259B</td>
<td>Nov 7 12:16</td>
<td>/var/tmp/preinstall/install.conf</td>
</tr>
<tr>
<td>734.3K</td>
<td>Nov 4 13:46</td>
<td>/var/tmp/preinstall/jboot-dc-re-11.3I20111104_1216_dc-builder.tgz</td>
</tr>
<tr>
<td>177.8M</td>
<td>Nov 7 12:16</td>
<td></td>
</tr>
</tbody>
</table>
request system storage cleanup interconnect-device device-name (QFabric Systems)

user@switch> request system storage cleanup interconnect IC-WS001
re1:

List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11B</td>
<td>Nov 7</td>
<td>/var/jail/tmp/alarmd.ts</td>
</tr>
<tr>
<td>128B</td>
<td>Nov 8</td>
<td>/var/log/default-log-messages.0.gz</td>
</tr>
<tr>
<td>9965B</td>
<td>Nov 8</td>
<td>/var/log/messages.0.gz</td>
</tr>
<tr>
<td>15.8K</td>
<td>Nov 8</td>
<td>/var/log/messages.1.gz</td>
</tr>
<tr>
<td>15.8K</td>
<td>Nov 8</td>
<td>/var/log/messages.2.gz</td>
</tr>
<tr>
<td>15.7K</td>
<td>Nov 8</td>
<td>/var/log/messages.3.gz</td>
</tr>
<tr>
<td>15.8K</td>
<td>Nov 8</td>
<td>/var/log/messages.4.gz</td>
</tr>
<tr>
<td>15.7K</td>
<td>Nov 8</td>
<td>/var/log/messages.5.gz</td>
</tr>
<tr>
<td>18.7K</td>
<td>Nov 7</td>
<td>/var/log/messages.6.gz</td>
</tr>
<tr>
<td>17.6K</td>
<td>Nov 7</td>
<td>/var/log/messages.7.gz</td>
</tr>
<tr>
<td>58.3K</td>
<td>Nov 7</td>
<td>/var/log/messages.8.gz</td>
</tr>
<tr>
<td>20.3K</td>
<td>Nov 7</td>
<td>/var/log/messages.9.gz</td>
</tr>
<tr>
<td>90B</td>
<td>Nov 7</td>
<td>/var/log/wtmp.0.gz</td>
</tr>
<tr>
<td>57B</td>
<td>Nov 7</td>
<td>/var/log/wtmp.1.gz</td>
</tr>
<tr>
<td>124.0K</td>
<td>Nov 7</td>
<td>/var/tmp/gres-tp/env.dat</td>
</tr>
<tr>
<td>0B</td>
<td>Nov 7</td>
<td>/var/tmp/gres-tp/lock</td>
</tr>
<tr>
<td>12.0K</td>
<td>Nov 7</td>
<td>/var/tmp/if-rtsdb/env.lck</td>
</tr>
<tr>
<td>132.0K</td>
<td>Nov 7</td>
<td>/var/tmp/if-rtsdb/env.mem</td>
</tr>
<tr>
<td>2688.0K</td>
<td>Nov 7</td>
<td>/var/tmp/if-rtsdb/shm_usr1.mem</td>
</tr>
<tr>
<td>2048.0K</td>
<td>Nov 7</td>
<td>/var/tmp/if-rtsdb/shm_usr2.mem</td>
</tr>
<tr>
<td>730B</td>
<td>Nov 7</td>
<td>/var/tmp/juniper.conf.gz</td>
</tr>
<tr>
<td>155B</td>
<td>Nov 7</td>
<td>/var/tmp/krt_gencfg_filter.txt</td>
</tr>
<tr>
<td>0B</td>
<td>Nov 7</td>
<td>/var/tmp/rtsdb/if-rtsdb</td>
</tr>
</tbody>
</table>

re0:

List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11B</td>
<td>Nov 7</td>
<td>/var/jail/tmp/alarmd.ts</td>
</tr>
<tr>
<td>128B</td>
<td>Nov 8</td>
<td>/var/log/default-log-messages.0.gz</td>
</tr>
<tr>
<td>16.7K</td>
<td>Nov 8</td>
<td>/var/log/messages.0.gz</td>
</tr>
<tr>
<td>22.2K</td>
<td>Nov 8</td>
<td>/var/log/messages.1.gz</td>
</tr>
<tr>
<td>18.4K</td>
<td>Nov 8</td>
<td>/var/log/messages.2.gz</td>
</tr>
<tr>
<td>21.6K</td>
<td>Nov 8</td>
<td>/var/log/messages.3.gz</td>
</tr>
<tr>
<td>17.9K</td>
<td>Nov 8</td>
<td>/var/log/messages.4.gz</td>
</tr>
<tr>
<td>19.4K</td>
<td>Nov 8</td>
<td>/var/log/messages.5.gz</td>
</tr>
<tr>
<td>18.2K</td>
<td>Nov 8</td>
<td>/var/log/messages.6.gz</td>
</tr>
<tr>
<td>20.4K</td>
<td>Nov 8</td>
<td>/var/log/messages.7.gz</td>
</tr>
<tr>
<td>21.4K</td>
<td>Nov 8</td>
<td>/var/log/messages.8.gz</td>
</tr>
<tr>
<td>21.0K</td>
<td>Nov 8</td>
<td>/var/log/messages.9.gz</td>
</tr>
<tr>
<td>19.9K</td>
<td>Nov 8</td>
<td>/var/log/snmp-traps.0.gz</td>
</tr>
<tr>
<td>2038B</td>
<td>Nov 8</td>
<td>/var/log/wtmp.0.gz</td>
</tr>
<tr>
<td>578</td>
<td>Nov 7</td>
<td>/var/log/wtmp.1.gz</td>
</tr>
<tr>
<td>124.0K</td>
<td>Nov 7</td>
<td>/var/tmp/gres-tp/env.dat</td>
</tr>
</tbody>
</table>
request system storage cleanup node-group group-name (QFabric Systems)

user@switch> request system storage cleanup node-group NW-NG-0

List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>126B</td>
<td>Nov 8 19:07</td>
<td>/var/log/default-log-messages.0.gz</td>
</tr>
<tr>
<td>179B</td>
<td>Nov 7 13:32</td>
<td>/var/log/install.0.gz</td>
</tr>
<tr>
<td>22.9K</td>
<td>Nov 8 19:07</td>
<td>/var/log/messages.0.gz</td>
</tr>
<tr>
<td>26.5K</td>
<td>Nov 8 17:30</td>
<td>/var/log/messages.1.gz</td>
</tr>
<tr>
<td>20.5K</td>
<td>Nov 8 13:15</td>
<td>/var/log/messages.2.gz</td>
</tr>
<tr>
<td>33.2K</td>
<td>Nov 7 17:45</td>
<td>/var/log/messages.3.gz</td>
</tr>
<tr>
<td>35.5K</td>
<td>Nov 7 15:45</td>
<td>/var/log/messages.4.gz</td>
</tr>
<tr>
<td>339B</td>
<td>Nov 8 17:08</td>
<td>/var/log/wtmp.0.gz</td>
</tr>
<tr>
<td>124.0K</td>
<td>Nov 8 17:08</td>
<td>/var/tmp/gres-tp/env.dat</td>
</tr>
<tr>
<td>0B</td>
<td>Nov 7 12:39</td>
<td>/var/tmp/gres-tp/lock</td>
</tr>
<tr>
<td>12.0K</td>
<td>Nov 7 12:59</td>
<td>/var/tmp/if-rtsdb/env.lck</td>
</tr>
<tr>
<td>132.0K</td>
<td>Nov 7 15:55</td>
<td>/var/tmp/if-rtsdb/shm_usr1.mem</td>
</tr>
<tr>
<td>2688.0K</td>
<td>Nov 7 15:41</td>
<td>/var/tmp/if-rtsdb/shm_usr2.mem</td>
</tr>
<tr>
<td>2048.0K</td>
<td>Nov 7 15:41</td>
<td>/var/tmp/if-rtsdb/trace.mem</td>
</tr>
<tr>
<td>727B</td>
<td>Nov 7 15:54</td>
<td>/var/tmp/juniper.conf.gz</td>
</tr>
<tr>
<td>155B</td>
<td>Nov 7 15:55</td>
<td>/var/tmp/krt_gencfg_filter.txt</td>
</tr>
<tr>
<td>0B</td>
<td>Nov 7 15:41</td>
<td>/var/tmp/rtbsd/if-rtsdb</td>
</tr>
</tbody>
</table>

EE3093:

List of files to delete:

<table>
<thead>
<tr>
<th>Size</th>
<th>Date</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>118B</td>
<td>Nov 8 17:33</td>
<td>/var/jail/tmp/alarmd.ts</td>
</tr>
<tr>
<td>119B</td>
<td>Nov 8 19:08</td>
<td>/var/log/default-log-messages.0.gz</td>
</tr>
<tr>
<td>180B</td>
<td>Nov 7 17:41</td>
<td>/var/log/install.0.gz</td>
</tr>
<tr>
<td>178B</td>
<td>Nov 7 13:32</td>
<td>/var/log/install.1.gz</td>
</tr>
<tr>
<td>2739B</td>
<td>Nov 8 19:08</td>
<td>/var/log/messages.0.gz</td>
</tr>
<tr>
<td>29.8K</td>
<td>Nov 8 18:45</td>
<td>/var/log/messages.1.gz</td>
</tr>
<tr>
<td>31.8K</td>
<td>Nov 8 17:15</td>
<td>/var/log/messages.2.gz</td>
</tr>
<tr>
<td>20.6K</td>
<td>Nov 8 16:00</td>
<td>/var/log/messages.3.gz</td>
</tr>
<tr>
<td>15.4K</td>
<td>Nov 8 10:15</td>
<td>/var/log/messages.4.gz</td>
</tr>
<tr>
<td>15.4K</td>
<td>Nov 8 02:15</td>
<td>/var/log/messages.5.gz</td>
</tr>
<tr>
<td>25.5K</td>
<td>Nov 7 20:45</td>
<td>/var/log/messages.6.gz</td>
</tr>
<tr>
<td>48.0K</td>
<td>Nov 7 17:45</td>
<td>/var/log/messages.7.gz</td>
</tr>
<tr>
<td>32.8K</td>
<td>Nov 7 13:45</td>
<td>/var/log/messages.8.gz</td>
</tr>
<tr>
<td>684B</td>
<td>Nov 8 17:02</td>
<td>/var/log/wtmp.0.gz</td>
</tr>
<tr>
<td>588B</td>
<td>Nov 7 12:40</td>
<td>/var/log/wtmp.1.gz</td>
</tr>
<tr>
<td>124.0K</td>
<td>Nov 7 17:34</td>
<td>/var/tmp/gres-tp/env.dat</td>
</tr>
</tbody>
</table>
request system storage cleanup qfabric component device-name (QFabric Systems)

user@switch> request system storage cleanup qfabric component A0001/YA0197
Repository type: regular
Repository head: /pbstorage
Creating list of debug artifacts to be removed under:
/pbstorage/rdumps/A0001/YA0197
Removing debug artifacts ... (press control C to abort)
Removing /pbstorage/rdumps/A0001/YA0197/cosd.core.0.0.05162011123308.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/cosd.core.1.0.05162011123614.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/cosd.core.2.0.05162011123920.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/livekcore.05132011163930.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/vmcore.05132011120528.gz ... done
Removing /pbstorage/rdumps/A0001/YA0197/vmcore.kz ... done
Creating list of debug artifacts to be removed under: /pbstorage/rlogs/A0001/YA0197
Removing debug artifacts ... (press control C to abort)
Removing /pbstorage/rlogs/A0001/YA0197/kdumpinfo.05132011120528 ... done
Removing /pbstorage/rlogs/A0001/YA0197/kernel.tarball.0.1039.05122011234415.tgz ... done
Removing /pbstorage/rlogs/A0001/YA0197/kernel.tarball.1.1039.05132011175544.tgz ... done
Removing /pbstorage/rlogs/A0001/YA0197/tnetd.tarball.0.1057.05162011124500.gz ... done
Removing /pbstorage/rlogs/A0001/YA0197/tnetd.tarball.1.1057.05162011124543.tgz ... done

request system storage cleanup qfabric component device-name repository core (QFabric Systems)

user@switch> request system storage cleanup qfabric component EE3093 repository core
Repository scope: shared
Repository head: /pdbdata/export
Repository name: core
Creating list of debug artifacts to be removed under: /pdbdata/export/rdumps/EE3093
NOTE: core repository under /pdbdata/export/rdumps/EE3093 empty

request system storage cleanup qfabric component all (QFabric Systems)

user@switch> request system storage cleanup qfabric component all
Repository scope: shared
Repository head: /pdbdata/export
Creating list of debug artifacts to be removed under: /pdbdata/export/rdumps
NOTE: core repository under /pdbdata/export/rdumps/all empty
Creating list of debug artifacts to be removed under: /pdbdata/export/rlogs
List of debug artifacts to clean up ... (press control C to abort)
/ppdbdata/export/rlogs/73747cd8-0710-11e1-b6a4-00e081c5297e/install-11072011125819.log
/ppdbdata/export/rlogs/77116f18-0710-11e1-a2a0-00e081c5297e/install-11072011125819.log
/ppdbdata/export/rlogs/7d7871a-0710-11e1-878e-00e081c5297e/install-11072011125932.log
/ppdbdata/export/rlogs/BBAK0394/install-11072011121532.log
/ppdbdata/export/rlogs/E3093/install-11072011121536.log
/ppdbdata/export/rlogs/W5001/YN5999/install-11072011121644.log
/ppdbdata/export/rlogs/W5001/YW3803/install-11072011122429.log
/ppdbdata/export/rlogs/d0afda1e-0710-11e1-a1d0-00e081c5297e/install-11072011125930.log
restart

Syntax
restart
<gracefully | immediately | soft>

Syntax (ACX Series Routers)
restart

Syntax (EX Series Switches)
restart
<autoinstallation | chassis-control | class-of-service | database-replication | dhcp | dhcp-service | diameter-service | dot1x-protocol | ethernet-link-fault-management | ethernet-switching | event-processing | firewall | general-authentication-service | interface-control | kernel-replication | l2-learning | lACP | license-service | link-management | lldpd-service | mib-process | mountd-service | multicast-snooping | pgm | redundancy-interface-process | remote-operations | routing | secure-neighbor-discovery | service-deployment | sflow-service | snmp | vrrp | web-management>

Syntax (Routing Matrix)
restart
<adaptive-services | audit-process | chassis-control | class-of-service | disk-monitoring | dynamic-flow-capture | ecc-error-logging | event-processing | firewall | interface-control | ipsec-key-management | kernel-replication | l2-learning | l2tp-service | lACP | link-management | mib-process | pgm | pic-services-logging | pki-service | ppp | pppoe | redundancy-interface-process | remote-operations | routing | logical-system-name | sampling | service-deployment | snmp>
<all | all-lcc | lcc number>
<gracefully | immediately | soft>

**Syntax (J Series Routing Platform)**
restart
<adaptive-services | audit-process | chassis-control | class-of-service | dhcp | dialer-services | dlsw | event-processing | firewall | interface-control | ipsec-key-management | isdn-signaling | l2-learn | l2tp-service | mib-process | network-access-service | pgm | ppp | pppoe | remote-operations | routing logical-system logical-system-name | sampling | service-deployment | snmp | usb-control | web-management>
<gracefully | immediately | soft>

**Syntax (TX Matrix Routers)**
restart
<adaptive-services | audit-process | chassis-control | class-of-service | dhcp-service | diameter-service | disk-monitoring | dynamic-flow-capture | ecc-error-logging | event-processing | firewall | interface-control | ipsec-key-management | kernel-replication | l2-learn | l2tp-service | lacp | link-management | mib-process | pgm | ppp | pppoe | redundancy-interface-process | remote-operations | routing logical-system logical-system-name | sampling | service-deployment | snmp | statistics-service>
<all-chassis | all-lcc | lc number | scc>
<gracefully | immediately | soft>

**Syntax (TX Matrix Plus Routers)**
restart
<adaptive-services | audit-process | chassis-control | class-of-service | dhcp-service | diameter-service | disk-monitoring | dynamic-flow-capture | ecc-error-logging | event-processing | firewall | interface-control | ipsec-key-management | kernel-replication | l2-learn | l2tp-service | lacp | link-management | mib-process | pgm | ppp | pppoe | redundancy-interface-process | remote-operations | routing logical-system logical-system-name | sampling | service-deployment | snmp | statistics-service>
<all-chassis | all-lcc | all-sfc | lc number | sfc number>
<gracefully | immediately | soft>

**Syntax (MX Series Routers)**
restart
<all-members>
<gracefully | immediately | soft>
<local>
<member member-id>
**Syntax (J Series Routers)**
```
restart <adaptive-services | audit-process | chassis-control | class-of-service | dhcp | dhcp-service |
       | dialer-services | diameter-service | dlsw | event-processing | firewall | interface-control |
       | ipsec-key-management | isdn-signaling | l2ald | l2-learning | l2tp-service | mib-process |
       | network-access-service | pgm | ppp | pppoe | remote-operations | routing <logical-system logical-system-name> | sampling | service-deployment | snmp | usb-control |
       | web-management>
       <gracefully | immediately | soft>
```

**Syntax (QFX Series)**
```
restart <adaptive-services | audit-process | chassis-control | class-of-service | dialer-services |
       | diameter-service | dlsw | ethernet-connectivity | event-processing | fibre-channel | firewall |
       | general-authentication-service | igmp-host-services | interface-control |
       | ipsec-key-management | isdn-signaling | l2ald | l2-learning | l2tp-service | mib-process |
       | named-service | network-access-service | ntrace-process | pgm | ppp | pppoe |
       | redundancy-interface-process | remote-operations | logical-system-name> | routing | sampling | secure-neighbor-discovery | service-deployment | snmp | usb-control |
       | web-management>
       <gracefully | immediately | soft>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- Command introduced in Junos OS Release 12.2 for ACX Series routers.

Options added:
- `dynamic-flow-capture` in Junos OS Release 7.4.
- `dlsw` in Junos OS Release 7.5.
- `event-processing` in Junos OS Release 7.5.
- `ppp` in Junos OS Release 7.5.
- `l2ald` in Junos OS Release 8.0.
- `link-management` in Release 8.0.
- `pgcp-service` in Junos OS Release 8.4.
- `sbc-configuration-process` in Junos OS Release 9.5.
- `services pgcp gateway` in Junos OS Release 9.6.
- `sfc` and `all-sfc` for the TX Matrix Router in Junos OS Release 9.6.

**Description**
Restart a Junos OS process.

---

**CAUTION:** Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router or switch to drop calls and interrupt transmission, resulting in possible loss of data.

**Options**
- `none`—Same as `gracefully`. 

---

Copyright © 2013, Juniper Networks, Inc.
**adaptive-services**—(Optional) Restart the configuration management process that manages the configuration for stateful firewall, Network Address Translation (NAT), intrusion detection services (IDS), and IP Security (IPsec) services on the Adaptive Services PIC.

**all-chassis**—(TX Matrix and TX Matrix Plus routers only) (Optional) Restart the software process on all chassis.

**all-lcc**—(TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process on all T640 routers connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process on all T1600 routers connected to the TX Matrix Plus router.

**all-members**—(MX Series routers only) (Optional) Restart the software process for all members of the Virtual Chassis configuration.

**all-sfc**—(TX Matrix Plus routers only) (Optional) For a TX Matrix Plus router, restart the software processes for the TX Matrix Plus router (or switch-fabric chassis).

**ancpd-service**—(Optional) Restart the Access Node Control Protocol (ANCP) process, which works with a special Internet Group Management Protocol (IGMP) session to collect outgoing interface mapping events in a scalable manner.

**application-identification**—(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.

**audit-process**—(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, analyzing, and tracking usage patterns, for billing a user based on the amount of time or type of services accessed.

**auto-configuration**—(Optional) Restart the Interface Auto-Configuration process.

**autoinstallation**—(EX Series switches only) (Optional) Restart the autoinstallation process.

**captive-portal-content-delivery**—(Optional) Restart the HTTP redirect service by specifying the location to which a subscriber’s initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber.

**ce-l2tp-service**—(M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Universal Edge Layer 2 Tunneling Protocol (L2TP) process, which establishes L2TP tunnels and Point-to-Point Protocol (PPP) sessions through L2TP tunnels.

**chassis-control**—(Optional) Restart the chassis management process.

**class-of-service**—(Optional) Restart the class-of-service (CoS) process, which controls the router’s or switch’s CoS configuration.

**clksyncd-service**—(Optional) Restart the external clock synchronization process, which uses synchronous Ethernet (SyncE).
database-replication—(EX Series switches and MX Series routers only) (Optional) Restart the database replication process.

datapath-trace-service—(Optional) Restart the packet path tracing process.

dhcp—(J Series routers and EX Series switches only) (Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.

dhcp-service—(Optional) Restart the Dynamic Host Configuration Protocol process.

dialer-services—(J Series routers and EX Series switches only) (Optional) Restart the ISDN dial-out process.

diameter-service—(Optional) Restart the diameter process.

disk-monitoring—(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.

dlsw—(J Series routers and QFX Series only) (Optional) Restart the data link switching (DLSw) service.

dot1x-protocol—(EX Series switches only) (Optional) Restart the port-based network access control process.

dynamic-flow-capture—(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on Monitoring Services III PICs.

ecc-error-logging—(Optional) Restart the error checking and correction (ECC) process, which logs ECC parity errors in memory on the Routing Engine.

ethernet-connectivity-fault-management—(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.

ethernet-link-fault-management—(EX Series switches and MX Series routers only) (Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.

ethernet-switching—(EX Series switches only) (Optional) Restart the Ethernet switching process.

event-processing—(Optional) Restart the event process (eventd).

fibre-channel—(QFX Series only) (Optional) Restart the Fibre Channel process.

firewall—(Optional) Restart the firewall management process, which manages the firewall configuration and enables accepting or rejecting packets that are transiting an interface on a router or switch.
general-authentication-service—(EX Series switches and MX Series routers only) (Optional) Restart the general authentication process.

generously—(Optional) Restart the software process.

iccp-service—(Optional) Restart the Inter-Chassis Communication Protocol (ICCP) process.

idp-policy—(Optional) Restart the intrusion detection and prevention (IDP) protocol process.

immediately—(Optional) Immediately restart the software process.

interface-control—(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.

ipsec-key-management—(Optional) Restart the IPsec key management process.

isdn-signaling—(J Series routers and QFX Series only) (Optional) Restart the ISDN signaling process, which initiates ISDN connections.

kernel-replication—(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.

l2-learning—(Optional) Restart the Layer 2 address flooding and learning process.

l2cpd-service—(Optional) Restart the Layer 2 Control Protocol process, which enables features such as Layer 2 protocol tunneling and nonstop bridging.

l2tp-service—(M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Layer 2 Tunneling Protocol (L2TP) process, which sets up client services for establishing Point-to-Point Protocol (PPP) tunnels across a network and negotiating Multilink PPP if it is implemented.

l2tp-universal-edge—(MX Series routers only) (Optional) Restart the L2TP process, which establishes L2TP tunnels and PPP sessions through L2TP tunnels.

l2tp—(Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link to allow their link aggregation control instances to reach agreement on the identity of the LAG to which the link belongs, and then to move the link to that LAG, and to enable the transmission and reception processes for the link to function in an orderly manner.

lcc number—(TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process for a specific T640 router that is connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process for a specific router that is connected to the TX Matrix Plus router.
Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**license-service**—(EX Series switches only) (Optional) Restart the feature license management process.

**link-management**—(TX Matrix and TX Matrix Plus routers and EX Series switches only) (Optional) Restart the Link Management Protocol (LMP) process, which establishes and maintains LMP control channels.

**lldpd-service**—(EX Series switches only) (Optional) Restart the Link Layer Discovery Protocol (LLDP) process.

**local**—(MX Series routers only) (Optional) Restart the software process for the local Virtual Chassis member.

**local-policy-decision-function**—(Optional) Restart the process for the Local Policy Decision Function, which regulates collection of statistics related to applications and application groups and tracking of information about dynamic subscribers and static interfaces.

**mac-validation**—(Optional) Restart the Media Access Control (MAC) validation process, which configures MAC address validation for subscriber interfaces created on demux interfaces in dynamic profiles on MX Series routers.

**member member-id**—(MX Series routers only) (Optional) Restart the software process for a specific member of the Virtual Chassis configuration. Replace *member-id* with a value of 0 or 1.

**mib-process**—(Optional) Restart the Management Information Base (MIB) version II process, which provides the router's MIB II agent.

**mobile-ip**—(Optional) Restart the Mobile IP process, which configures Junos OS Mobile IP features.

**mountd-service**—(EX Series switches and MX Series routers only) (Optional) Restart the service for NFS mount requests.

**mpls-traceroute**—(Optional) Restart the MPLS Periodic Traceroute process.

**mspd**—(Optional) Restart the Multiservice process.
multicast-snooping—(EX Series switches and MX Series routers only) (Optional) Restart the multicast snooping process, which makes Layer 2 devices, such as VLAN switches, aware of Layer 3 information, such as the media access control (MAC) addresses of members of a multicast group.

named-service—(Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.

network-access-service—(J Series routers and QFX Series only) (Optional) Restart the network access process, which provides the router's Challenge Handshake Authentication Protocol (CHAP) authentication service.

nfsd-service—(Optional) Restart the Remote NFS Server process, which provides remote file access for applications that need NFS-based transport.

packet-triggered-subscribers—(Optional) Restart the packet-triggered subscribers and policy control (PTSP) process, which allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device.

peer-selection-service—(Optional) Restart the Peer Selection Service process.

pgcp-service—(Optional) Restart the pgcpd service process running on the Routing Engine. This option does not restart pgcpd processes running on mobile station PICs. To restart pgcpd processes running on mobile station PICs, use the `services pgcp gateway` option.

pgm—(Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.

pic-services-logging—(Optional) Restart the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.

pki-service—(Optional) Restart the PKI Service process.

ppp—(Optional) Restart the Point-to-Point Protocol (PPP) process, which is the encapsulation protocol process for transporting IP traffic across point-to-point links.

ppp-service—(Optional) Restart the Universal Edge PPP process, which is the encapsulation protocol process for transporting IP traffic across Universal Edge routers.

pppoe—(Optional) Restart the Point-to-Point Protocol over Ethernet (PPPoE) process, which combines PPP that typically runs over broadband connections with the Ethernet link-layer protocol that allows users to connect to a network of hosts over a bridge or access concentrator.

protected-system-domain-service—(Optional) Restart the Protected System Domain (PSD) process.

redundancy-interface-process—(Optional) Restart the ASP redundancy process.
remote-operations—(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.

root-system-domain-service—(Optional) Restart the Root System Domain (RSD) service.

routing—(ACX Series routers, QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the routing protocol process.

routing <logical-system logical-system-name>—(Optional) Restart the routing protocol process, which controls the routing protocols that run on the router or switch and maintains the routing tables. Optionally, restart the routing protocol process for the specified logical system only.

sampling—(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.

sbc-configuration-process—(Optional) Restart the session border controller (SBC) process of the border signaling gateway (BSG).

scc—(TX Matrix routers only) (Optional) Restart the software process on the TX Matrix router (or switch-card chassis).

sdk-service—(Optional) Restart the SDK Service process, which runs on the Routing Engine and is responsible for communications between the SDK application and Junos OS. Although the SDK Service process is present on the router, it is turned off by default.

secure-neighbor-discovery—(QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.

sfc number—(TX Matrix Plus routers only) (Optional) Restart the software process on the TX Matrix Plus router (or switch-fabric chassis). Replace number with 0.

service-deployment—(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.

services—(Optional) Restart a service.

services pgcp gateway gateway-name—(Optional) Restart the pgcpd process for a specific border gateway function (BGF) running on an MS-PIC. This option does not restart the pgcpd process running on the Routing Engine. To restart the pgcpd process on the Routing Engine, use the pgcp-service option.

sflow-service—(EX Series switches only) (Optional) Restart the flow sampling (sFlow technology) process.

snmp—(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router’s or switch’s SNMP master agent.
**soft**—(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.

**static-subscribers**—(Optional) Restart the static subscribers process, which associates subscribers with statically configured interfaces and provides dynamic service activation and activation for these subscribers.

**statistics-service**—(Optional) Restart the process that manages the Packet Forwarding Engine statistics.

**subscriber-management**—(Optional) Restart the Subscriber Management process.

**subscriber-management-helper**—(Optional) Restart the Subscriber Management Helper process.

**tunnel-oam**—(Optional) Restart the Tunnel OAM process, which enables the Operations, Administration, and Maintenance of Layer 2 tunneled networks. Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 PDUs across the provider’s cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain.

**usb-control**—(J Series routers and MX Series routers only) (Optional) Restart the USB control process.

**vrrp**—(ACX Series routers, EX Series switches, and MX Series routers only) (Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.

**web-management**—(J Series routers, QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the Web management process.

**Required Privilege Level**

reset

**Related Documentation**

- Overview of Junos OS CLI Operational Mode Commands

**List of Sample Output**

restart interfaces on page 222

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```
**set chassis display message**

**Syntax**

```
set chassis display message "message"
<permanent>
```

**Syntax (TX Matrix Router)**

```
set chassis display message "message" (lcc number | scc)
<permanent>
```

**Syntax (TX Matrix Plus Router)**

```
set chassis display message "message " (fpc-slot slot-number | lcc number | sfc number)
<permanent>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
**sfc** option for TX Matrix Plus router introduced in Junos OS Release 9.6.

**Description**

Display or stop a text message on the craft interface display, which is on the front of the router, or on the LCD panel display on the switch. The craft interface alternates the display of text messages with standard craft interface messages three times, switching between messages every 60 seconds.

---

**NOTE:** On T Series routers, when this command is executed with the `permanent` option, the display of the text message alternates with that of the standard craft interface message continuously every 60 seconds.

By default, on both the router and the switch, the text message is displayed for 5 minutes. The craft interface display has four 20-character lines. The LCD panel display has two 16-character lines, and text messages appear only on the second line.

**Options**

"message"—Message to display. On the craft interface display, if the message is longer than 20 characters, it wraps onto the next line. If a word does not fit on one line, the entire word moves down to the next line. Any portion of the message that does not fit on the display is truncated. An empty pair of quotation marks (" ") deletes the text message from the craft interface display. On the LCD panel display, the message is limited to 16 characters.

**fpc-slot slot-number**—(TX Matrix Plus routers and EX4200 and QFX Series only) On the router or switch, display the text message on the craft interface for a specific Flexible PIC Concentrator (FPC). Replace `slot-number` with a value from 0 through 31. On the switch, display the text message for a specific member of a Virtual Chassis, where `fpc-slot slot-number` corresponds to the member ID. Replace `slot-number` with a value from 0 through 9. On the QFX Series, the `slot-number` is always 0. On a TX Matrix Plus router with 3D SIBs replace `slot-number` with a value from 0 through 63.

**lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.
Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**permanent**—(Optional) Display a text message on the craft interface display or LCD panel display permanently.

**scc**—(TX Matrix routers only) Display the text message on the craft interface display of the TX Matrix router (switch-card chassis).

**sfc number**—(TX Matrix Plus routers only) Display the text message on the craft interface display of the TX Matrix Plus router (or switch-fabric chassis).

**Required Privilege Level**

clear

**Related Documentation**

- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- clear chassis display message on page 160
- show chassis craft-interface
- Understanding the Implementation of System Log Messages on the QFabric System

**List of Sample Output**

- set chassis display message (Creating) on page 224
- set chassis display message (Deleting) on page 225

**Output Fields**

See *show chassis craft-interface* for an explanation of output fields.

**Sample Output**

**set chassis display message (Creating)**

The following example shows how to set the display message and verify the result:

```
user@host> set chassis display message "NOC contact Dusty (888) 555-1234"
message sent

user@host> show chassis craft-interface
Red alarm: LED off, relay off
Yellow alarm: LED off, relay off
Host OK LED: On
Host fail LED: Off
FPCs 0 1 2 3 4 5 6 7
-------------------------------
Green .. *.. * *
Red ........
```
set chassis display message (Deleting)

The following example shows how to delete the display message and verify that the message is removed:

```
user@host> set chassis display message ""
message sent

user@host> show chassis craft-interface
Red alarm: LED off, relay off
Yellow alarm: LED off, relay off
Host OK LED: On
Host fail LED: Off
FPCs  0  1  2  3  4  5  6  7
-------------------------------
Green  .. *.. * *.
Red    ........
LCD screen:
                  +---------------------+
| host              |
| Up: 0+17:05:47    |
| Temperature OK    |
                  +---------------------+
```
set date

Syntax

```
set date (date-time ntp <key authentication-key number> <servers> <source-address source-address>)
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
key option introduced in Junos OS Release 12.1R2

Description

Set the date and time.

Options

- **date-time**—Date and time. Enter this string inside quotation marks.
- **ntp**—Use a Network Time Protocol (NTP) server to synchronize the current date and time setting on the router or switch.
- **key authentication-key number**—(Optional) Specify a key number to authenticate the NTP server used to synchronize the date and time. You must specify the same key number used to authenticate the server configured at the `edit system ntp authentication-key number` hierarchy level.
- **servers**—(Optional) Specify the IP address of one or more NTP servers.
- **source-address source-address**—Specify the source address that the router or switch uses to contact the remote NTP server.

Required Privilege Level

```
view
```

Related Documentation

- Setting the Date and Time

List of Sample Output

```
set date on page 226
```

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
set date

user@host> set date ntp
21 Apr 17:22:02 ntpdate[3867]: step time server 172.17.27.46 offset 8.759252 sec
```

### show chassis fan

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show chassis fan</code></td>
<td>Show information about the fan tray and fans.</td>
</tr>
</tbody>
</table>

**Syntax (ACX4000 Series Router)**

- `show chassis fan`

**Syntax (MX Series Router)**

- `<all-members>`
- `<local>`
- `<member member-id>`

**Syntax (T Series Routers)**

- `show chassis fan`

**Syntax (MX104, MX2010, and MX2020 3D Universal Edge Router)**

- `show chassis fan`

**Syntax (QFabric Systems)**

- `<interconnect-device name>`

**Syntax (TX Matrix Router)**

- `show chassis fan`
- `<lcc number | scc>`

**Syntax (TX Matrix Plus Router)**

- `show chassis fan`
- `<lcc number | sfc number>`

**Release Information**

- Command introduced in Junos OS Release 10.0 on MX Series 3D Universal Edge Routers, M120 routers, and M320 routers, T320 routers, T640 routers, T1600 routers, TX Matrix Routers, and TX Matrix Plus routers.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- Command introduced in Junos OS Release 11.4 for EX Series switches.
- Command introduced in Junos OS Release 12.3 for PTX5000 Packet Transport Routers.
- Command introduced in Junos OS Release 12.1 for T4000 routers.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for ACX Series Routers.
- Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

**Description**

(T Series routers, TX Matrix routers, TX Matrix Plus routers, M120 routers, M320 routers, MX104 routers, MX2010 routers, MX2020 routers, MX Series 3D Universal Edge Routers, QFX3008-I Interconnect devices, EX Series switches, and PTX Series Packet Transport Routers only) Show information about the fan tray and fans.

**Options**

- `all-members`—(MX Series routers only) (Optional) Display information about the fan tray and fans for all members of the Virtual Chassis configuration.
- `local`—(MX Series routers only) (Optional) Display information about the fan tray and fans for the local Virtual Chassis member.
**member member-id**—(MX Series routers only) (Optional) Display information about the fan tray and fans for the specified member of the Virtual Chassis configuration. For an MX Series Virtual Chassis, replace `member-id` variable with a value 0 or 1.

**interconnect-device name**—(QFX3000-G QFabric systems only) (Optional) Display information about the fan tray and fans for the specified QFX3008-I Interconnect device.

**lcc number**—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display information about the fan tray and fans for the specified T640 router (line-card chassis) that is connected to a TX Matrix router. On a TX Matrix Plus router, display information about the fan tray and fans for the specified router (line-card chassis) that is connected to a TX Matrix Plus router. Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**scc**—(TX Matrix routers only) (Optional) Display information about the fan tray and fans for the TX Matrix router (switch-card chassis).

**stc number**—(TX Matrix Plus routers only) (Optional) Display information about the fan tray and fans for the TX Matrix Plus router (switch-fabric chassis). Replace `number` variable with 0.

**Required Privilege Level**

- **view**

**List of Sample Output**

- show chassis fan on page 229
- show chassis fan (QFabric Systems) on page 230
- show chassis fan (EX Series Switches) on page 231
- show chassis fan (T320 Router) on page 231
- show chassis fan (T640 Router) on page 232
- show chassis fan (T1600 Router) on page 232
- show chassis fan (T4000 Core Router) on page 233
- show chassis fan (TX Matrix Router) on page 233
- show chassis fan (TX Matrix Plus Router) on page 234
- show chassis fan (TX Matrix Plus Router with 3D SIBs) on page 235
- show chassis fan (PTX5000 Packet Transport Router) on page 237
- show chassis fan (MX104 Router) on page 238
- show chassis fan (MX2010 Router) on page 238
- show chassis fan (MX2020 Router) on page 238
Table 66 on page 229 lists the output fields for the `show chassis fan` command. Output fields are listed in the approximate order in which they appear.

**Table 66: show chassis fan Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
<td>Fan item identifier.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the fan:</td>
</tr>
<tr>
<td></td>
<td>• OK — Fan is running properly and within the normal range.</td>
</tr>
<tr>
<td></td>
<td>• Check — Fan is in Check state because of some fault or alarm condition.</td>
</tr>
<tr>
<td>RPM</td>
<td>Fan speed in revolutions per minute (RPM).</td>
</tr>
<tr>
<td>% RPM</td>
<td>Percentage of the fan speed being used.</td>
</tr>
<tr>
<td>Measurement</td>
<td>Fan speed status based on different chassis cooling requirements:</td>
</tr>
<tr>
<td></td>
<td>• Spinning at high speed</td>
</tr>
<tr>
<td></td>
<td>• Spinning at intermediate speed</td>
</tr>
<tr>
<td></td>
<td>• Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>• Spinning at low speed (except EX Series switches)</td>
</tr>
<tr>
<td></td>
<td>Fan speed in revolutions per minute (RPM) for each fan in the fan tray.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
user@host> show chassis fan

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Tray Fan 1</td>
<td>OK</td>
<td>3790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 2</td>
<td>OK</td>
<td>3769</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 3</td>
<td>OK</td>
<td>3769</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 4</td>
<td>OK</td>
<td>3790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 5</td>
<td>OK</td>
<td>3790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 6</td>
<td>OK</td>
<td>3790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 7</td>
<td>OK</td>
<td>3790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 8</td>
<td>OK</td>
<td>3769</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 9</td>
<td>OK</td>
<td>3769</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 10</td>
<td>OK</td>
<td>3790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Tray Fan 11</td>
<td>OK</td>
<td>3790</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
```
show chassis fan (QFabric Systems)

```
user@host> show chassis fan interconnect-device interconnect1
```

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFT 0 Fan 0</td>
<td>OK</td>
<td>2849</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>TFT 0 Fan 1</td>
<td>OK</td>
<td>2821</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>TFT 0 Fan 2</td>
<td>OK</td>
<td>2735</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>TFT 0 Fan 3</td>
<td>OK</td>
<td>2815</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>TFT 0 Fan 4</td>
<td>OK</td>
<td>2828</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>TFT 0 Fan 5</td>
<td>OK</td>
<td>2863</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>BFT 1 Fan 0</td>
<td>OK</td>
<td>2941</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>BFT 1 Fan 1</td>
<td>OK</td>
<td>3008</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>BFT 1 Fan 2</td>
<td>OK</td>
<td>3073</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>BFT 1 Fan 3</td>
<td>OK</td>
<td>2925</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>BFT 1 Fan 4</td>
<td>OK</td>
<td>2863</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>BFT 1 Fan 5</td>
<td>OK</td>
<td>2933</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 0 Rotor 0</td>
<td>OK</td>
<td>15472</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 0 Rotor 1</td>
<td>OK</td>
<td>14477</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 1 Rotor 0</td>
<td>OK</td>
<td>15561</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 1 Rotor 1</td>
<td>OK</td>
<td>14210</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 2 Rotor 0</td>
<td>OK</td>
<td>16167</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 2 Rotor 1</td>
<td>OK</td>
<td>14248</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 3 Rotor 0</td>
<td>OK</td>
<td>16463</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 0 Fan 3 Rotor 1</td>
<td>OK</td>
<td>14099</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 0 Rotor 0</td>
<td>OK</td>
<td>15083</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 0 Rotor 1</td>
<td>OK</td>
<td>13533</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 1 Rotor 0</td>
<td>OK</td>
<td>16071</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 1 Rotor 1</td>
<td>OK</td>
<td>14400</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 2 Rotor 0</td>
<td>OK</td>
<td>15517</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 2 Rotor 1</td>
<td>OK</td>
<td>14210</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 3 Rotor 0</td>
<td>OK</td>
<td>16413</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 1 Fan 3 Rotor 1</td>
<td>OK</td>
<td>14400</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 0 Rotor 0</td>
<td>OK</td>
<td>15297</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 0 Rotor 1</td>
<td>OK</td>
<td>14634</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 1 Rotor 0</td>
<td>OK</td>
<td>15561</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 1 Rotor 1</td>
<td>OK</td>
<td>14285</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 2 Rotor 0</td>
<td>OK</td>
<td>15835</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 2 Rotor 1</td>
<td>OK</td>
<td>14400</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 3 Rotor 0</td>
<td>OK</td>
<td>15789</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 2 Fan 3 Rotor 1</td>
<td>OK</td>
<td>14323</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 0 Rotor 0</td>
<td>OK</td>
<td>16314</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 0 Rotor 1</td>
<td>OK</td>
<td>14876</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 1 Rotor 0</td>
<td>OK</td>
<td>15835</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 1 Rotor 1</td>
<td>OK</td>
<td>14323</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 2 Rotor 0</td>
<td>OK</td>
<td>16265</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 2 Rotor 1</td>
<td>OK</td>
<td>14594</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 3 Rotor 0</td>
<td>OK</td>
<td>16071</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 3 Fan 3 Rotor 1</td>
<td>OK</td>
<td>14323</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 4 Fan 0 Rotor 0</td>
<td>OK</td>
<td>15652</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 4 Fan 0 Rotor 1</td>
<td>OK</td>
<td>14438</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 4 Fan 1 Rotor 0</td>
<td>OK</td>
<td>16167</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>SFT 4 Fan 1 Rotor 1</td>
<td>OK</td>
<td>14555</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
show chassis fan (EX Series Switches)

user@host> show chassis fan

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan 1</td>
<td>OK</td>
<td>3477</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 2</td>
<td>OK</td>
<td>3477</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 3</td>
<td>OK</td>
<td>3479</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 4</td>
<td>OK</td>
<td>3508</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 5</td>
<td>OK</td>
<td>3517</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 6</td>
<td>OK</td>
<td>3531</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 7</td>
<td>OK</td>
<td>3439</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 8</td>
<td>OK</td>
<td>3424</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 9</td>
<td>OK</td>
<td>3413</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 10</td>
<td>OK</td>
<td>3439</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 11</td>
<td>OK</td>
<td>3446</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 12</td>
<td>OK</td>
<td>3432</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

show chassis fan (T320 Router)

user@host> show chassis fan

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>2850</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>2820</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>2970</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>2790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>2640</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>2790</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>2520</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>2610</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>2550</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
Bottom Right Front fan   OK       2610    Spinning at normal speed
Bottom Right Middle fan   OK       2880    Spinning at normal speed
Bottom Right Rear fan     OK       2790    Spinning at normal speed
Rear Tray Top fan         OK       2130    Spinning at normal speed
Rear Tray Second fan      OK       2190    Spinning at normal speed
Rear Tray Middle fan      OK       2250    Spinning at normal speed
Rear Tray Fourth fan      OK       2220    Spinning at normal speed
Rear Tray Bottom fan      OK       2280    Spinning at normal speed

show chassis fan (T640 Router)

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>3450</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Top fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Second fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Third fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fourth fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fifth fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Sixth fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Seventh fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Bottom fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

show chassis fan (T1600 Router)

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>3450</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Top fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Second fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Third fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fourth fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fifth fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Sixth fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Seventh fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Bottom fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
### show chassis fan (T4000 Core Router)

```bash
user@host> show chassis fan
```

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>5220</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>5160</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>5190</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>5160</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>6030</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>6090</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>6090</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>6030</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>6060</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>6060</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Top fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Second fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Third fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Fourth fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Fifth fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Sixth fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Seventh fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
<tr>
<td>Rear Tray Bottom fan</td>
<td>OK</td>
<td>10000</td>
<td>Spinning at high speed</td>
</tr>
</tbody>
</table>

### show chassis fan (TX Matrix Router)

```bash
user@host> show chassis fan
```

For `scc-re0:`

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>3450</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Top fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Second fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Third fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fourth fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fifth fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Sixth fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Seventh fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Bottom fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

For `lcc2-re0:`

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>3450</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>3450</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

---

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>3360</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>3480</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Top fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Second fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Third fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fourth fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Fifth fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Sixth fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Seventh fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray Bottom fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

show chassis fan (TX Matrix Plus Router)

user@host> show chassis fan
sfc0-re0:

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan Tray 0 Fan 1</td>
<td>OK</td>
<td>4350</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 2</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 3</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 4</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 5</td>
<td>OK</td>
<td>4350</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 6</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 1</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 2</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 3</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 4</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 5</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 6</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 1</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 2</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 3</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 4</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 5</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 6</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 7</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 8</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 9</td>
<td>OK</td>
<td>4350</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 1</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 2</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 3</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 4</td>
<td>OK</td>
<td>4440</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 5</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 6</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 7</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 8</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 9</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 1</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 2</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 3</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 4</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 5</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 6</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 7</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 8</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 9</td>
<td>OK</td>
<td>4410</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
### show chassis fan (TX Matrix Plus Router with 3D SIBs)

```
user@host> show chassis fan
```

### lcc0-re0:

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan Tray 0 Fan 1</td>
<td>OK</td>
<td>4350</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 2</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 3</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 4</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 5</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 6</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 7</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 8</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 9</td>
<td>OK</td>
<td>4380</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

### sfc0-re0:

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan Tray 1 Fan 1</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 2</td>
<td>OK</td>
<td>4860</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 3</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 4</td>
<td>OK</td>
<td>4800</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 5</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 6</td>
<td>OK</td>
<td>4770</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 7</td>
<td>OK</td>
<td>4800</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 8</td>
<td>OK</td>
<td>4770</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 9</td>
<td>OK</td>
<td>4770</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 1</td>
<td>OK</td>
<td>4800</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 2</td>
<td>OK</td>
<td>4800</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 3</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 4</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 5</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 6</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 7</td>
<td>OK</td>
<td>4800</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 8</td>
<td>OK</td>
<td>4830</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 9</td>
<td>OK</td>
<td>4800</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Fan Tray 3 Fan 1          OK       4860    Spinning at normal speed
Fan Tray 3 Fan 2          OK       4860    Spinning at normal speed
Fan Tray 3 Fan 3          OK       4800    Spinning at normal speed
Fan Tray 3 Fan 4          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 5          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 6          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 7          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 8          OK       4800    Spinning at normal speed
Fan Tray 3 Fan 9          OK       4800    Spinning at normal speed
Fan Tray 4 Fan 1          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 2          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 3          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 4          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 5          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 6          OK       4860    Spinning at normal speed
Fan Tray 4 Fan 7          OK       4800    Spinning at normal speed
Fan Tray 4 Fan 8          OK       4860    Spinning at normal speed
Fan Tray 4 Fan 9          OK       4770    Spinning at normal speed
Fan Tray 5 Fan 1          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 2          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 3          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 4          OK       4800    Spinning at normal speed
Fan Tray 5 Fan 5          OK       4800    Spinning at normal speed
Fan Tray 5 Fan 6          OK       4800    Spinning at normal speed
Fan Tray 5 Fan 7          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 8          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 9          Check    2010

Fan Tray 3 Fan 1          OK       4860    Spinning at normal speed
Fan Tray 3 Fan 2          OK       4860    Spinning at normal speed
Fan Tray 3 Fan 3          OK       4800    Spinning at normal speed
Fan Tray 3 Fan 4          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 5          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 6          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 7          OK       4830    Spinning at normal speed
Fan Tray 3 Fan 8          OK       4800    Spinning at normal speed
Fan Tray 3 Fan 9          OK       4800    Spinning at normal speed
Fan Tray 4 Fan 1          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 2          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 3          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 4          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 5          OK       4830    Spinning at normal speed
Fan Tray 4 Fan 6          OK       4860    Spinning at normal speed
Fan Tray 4 Fan 7          OK       4800    Spinning at normal speed
Fan Tray 4 Fan 8          OK       4860    Spinning at normal speed
Fan Tray 4 Fan 9          OK       4770    Spinning at normal speed
Fan Tray 5 Fan 1          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 2          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 3          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 4          OK       4800    Spinning at normal speed
Fan Tray 5 Fan 5          OK       4800    Spinning at normal speed
Fan Tray 5 Fan 6          OK       4800    Spinning at normal speed
Fan Tray 5 Fan 7          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 8          OK       4830    Spinning at normal speed
Fan Tray 5 Fan 9          OK       4830    Spinning at normal speed

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>3450</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 1 (Top)</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 2</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 3</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 4</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 5</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 6</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 7</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 8</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 9</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 10</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 11</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 12</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 13</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 14</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 15</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 16 (Bottom)</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Item</td>
<td>Status</td>
<td>RPM</td>
<td>Measurement</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------</td>
<td>-----</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>3450</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>3390</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>3420</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 1 (Top)</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 2</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 3</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 4</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 5</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 6</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 7</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 8</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 9</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 10</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 11</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 12</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 13</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 14</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 15</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Rear Tray fan 16 (Bottom)</td>
<td>OK</td>
<td>7740</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

show chassis fan (PTX5000 Packet Transport Router)

```
user@host> show chassis fan
```

```
user@host> show chassis fan
```

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>% RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan Tray 0 Fan 1</td>
<td>OK</td>
<td>29%</td>
<td>2700 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 2</td>
<td>OK</td>
<td>29%</td>
<td>2700 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 3</td>
<td>OK</td>
<td>29%</td>
<td>2742 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 4</td>
<td>OK</td>
<td>29%</td>
<td>2700 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 5</td>
<td>OK</td>
<td>30%</td>
<td>2828 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 6</td>
<td>OK</td>
<td>30%</td>
<td>2828 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 7</td>
<td>OK</td>
<td>29%</td>
<td>2700 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 8</td>
<td>OK</td>
<td>30%</td>
<td>2785 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 9</td>
<td>OK</td>
<td>30%</td>
<td>2828 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 10</td>
<td>OK</td>
<td>30%</td>
<td>2828 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 11</td>
<td>OK</td>
<td>30%</td>
<td>2785 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 12</td>
<td>OK</td>
<td>30%</td>
<td>2828 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 13</td>
<td>OK</td>
<td>31%</td>
<td>2871 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 14</td>
<td>OK</td>
<td>30%</td>
<td>2828 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 1</td>
<td>OK</td>
<td>42%</td>
<td>3033 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 2</td>
<td>OK</td>
<td>42%</td>
<td>3066 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 3</td>
<td>OK</td>
<td>43%</td>
<td>3099 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 4</td>
<td>OK</td>
<td>43%</td>
<td>3166 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 5</td>
<td>OK</td>
<td>45%</td>
<td>3266 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 6</td>
<td>OK</td>
<td>43%</td>
<td>3133 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 1</td>
<td>OK</td>
<td>29%</td>
<td>2099 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 2</td>
<td>OK</td>
<td>30%</td>
<td>2199 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 3</td>
<td>OK</td>
<td>30%</td>
<td>2166 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 4</td>
<td>OK</td>
<td>33%</td>
<td>2399 RPM</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
### show chassis fan (MX104 Router)

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>% RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan 1</td>
<td>OK</td>
<td>29%</td>
<td>2133 RPM</td>
</tr>
<tr>
<td>Fan 2</td>
<td>OK</td>
<td>32%</td>
<td>2366 RPM</td>
</tr>
</tbody>
</table>

### show chassis fan (MX2010 Router)

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>% RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan Tray 0 Fan 1</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 2</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 3</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 4</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 5</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 6</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
</tbody>
</table>

### show chassis fan (MX2020 Router)

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>% RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan Tray 0 Fan 1</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 2</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 3</td>
<td>OK</td>
<td>36%</td>
<td>3240 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 4</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 5</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 6</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 1</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 2</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 3</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 4</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 5</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 6</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 1</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 2</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 3</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 4</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 5</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 6</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 1</td>
<td>OK</td>
<td>38%</td>
<td>3480 RPM</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 2</td>
<td>OK</td>
<td>40%</td>
<td>3600 RPM</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 3</td>
<td>OK</td>
<td>40%</td>
<td>3600 RPM</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 4</td>
<td>OK</td>
<td>40%</td>
<td>3600 RPM</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 5</td>
<td>OK</td>
<td>40%</td>
<td>3600 RPM</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 6</td>
<td>OK</td>
<td>37%</td>
<td>3360 RPM</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
show chassis fan (ACX4000 Router)

user@host > show chassis fan

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>RPM</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan 1</td>
<td>OK</td>
<td>4140</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan 2</td>
<td>OK</td>
<td>4200</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
**show chassis firmware**

**Syntax**
```
show chassis firmware
```

**Syntax (TX Matrix Routers)**
```
show chassis firmware
<lcc number | scc>
```

**Syntax (TX Matrix Plus Routers)**
```
show chassis firmware
<lcc number | sfc number>
```

**Syntax (MX Series Routers)**
```
show chassis firmware
<all-members>
<local>
<member member-id>
```

**Syntax (MX104, MX2010, and MX2020 3D Universal Edge Routers)**
```
show chassis firmware
```

**Syntax (QFX Series)**
```
show chassis firmware
interconnect-device name
node-device name
```

**Syntax (ACX Series Universal Access Routers)**
```
show chassis firmware
```

**Syntax (EX Series Switches)**
```
show chassis firmware
<detail>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.4 for EX Series switches.
- sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced for EX8200 switches in Junos OS Release 10.2 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for QFX Series.
- Command introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for ACX4000 Universal Access Routers.
- Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

**Description**
- On routers and switches, display the version levels of the firmware running on the System Control Board (SCB), Switching and Forwarding Module (SFM), System and Switch Board (SSB), Forwarding Engine Board (FEB), Flexible PIC Concentrators (FPCs), and Routing Engines. On a TX Matrix Plus router, display the version levels of the firmware running on the FPCs and the Switch Processor Mezzanine Board (SPMBs).
- On EX2200, EX3200, and EX4200 switches, and the QFX Series, display the version levels of the firmware running on the switch. On an EX8208 switch, display the version
levels of the firmware running on the Switch Fabric and Routing Engine (SRE) modules and on the line cards (shown as FPCs). On an EX8216 switch, display the version levels of the firmware running on the Routing Engine (RE) modules and on the line cards (shown as FPCs).

**Options**

- **none**—Display the version levels of the firmware running. For an EX4200 switch that is a member of a Virtual Chassis, display version levels for all members. For a TX Matrix router, display version levels for the firmware on the TX Matrix router and on all the T640 routers connected to the TX Matrix router. For a TX Matrix Plus router, display version levels for the firmware on the TX Matrix Plus router and on all the routers connected to the TX Matrix Plus router.

- **all-members**—(MX Series routers only) (Optional) Display the version levels of the firmware running for all members of the Virtual Chassis configuration.

- **interconnect-device name**—(QFabric systems) (Optional) Display the version levels of the firmware running on the Interconnect device.

- **lcc number**—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display version levels for the firmware on a specified T640 router (line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, display the version levels for the firmware on a specified router (line-card chassis) that is connected to the TX Matrix Plus router.

  Replace `number` with the following values depending on the LCC configuration:

  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

- **local**—(MX Series routers only) (Optional) Display the version levels of the firmware running for the local Virtual Chassis member.

- **member member-id**—(MX Series routers only) (Optional) Display the version levels of the firmware running for the specified member of the Virtual Chassis configuration. Replace `member-id` with a value of 0 or 1.

- **node-device**—(QFabric systems only) (Optional) Display the version levels of the firmware running on the Node device.

- **scc**—(TX Matrix router only) (Optional) Display version levels for the firmware on the TX Matrix router (switch-card chassis).

- **sfc number**—(TX Matrix Plus router only) (Optional) Display version levels for the firmware on the TX Matrix Plus router (or switch-fabric chassis). Replace `number` with 0.
**detail**—(EX3200, EX3300, EX4200, and EX4500 standalone and Virtual Chassis member switches only) (Optional) Display version levels of the firmware running on the switch for its programmable hardware components.

**Required Privilege**

**Level**

view

**Related Documentation**

- Upgrading the HSM Firmware

**List of Sample Output**

- show chassis firmware (M10 Router) on page 243
- show chassis firmware (M20 Router) on page 243
- show chassis firmware (M40 Router) on page 243
- show chassis firmware (M120 Router) on page 244
- show chassis firmware (M160 Router) on page 244
- show chassis firmware (MX104 Router) on page 244
- show chassis firmware (MX240 Router) on page 244
- show chassis firmware (MX480 Router) on page 244
- show chassis firmware (MX960 Router) on page 245
- show chassis firmware (MX2010 Router) on page 245
- show chassis firmware (MX2020 Router) on page 245
- show chassis firmware (MX240, MX480, MX960 Router with Application Services Modular Line Card) on page 246
- show chassis firmware (EX4200 Switch) on page 246
- show chassis firmware (EX8200 Switch) on page 246
- show chassis firmware lcc (TX Matrix Router) on page 247
- show chassis firmware scc (TX Matrix Router) on page 247
- show chassis firmware (TX Matrix Plus Router) on page 247
- show chassis firmware lcc (TX Matrix Plus Router) on page 248
- show chassis firmware sfc (TX Matrix Plus Router) on page 249
- show chassis firmware (QFX Series) on page 249
- show chassis firmware interconnect-device (QFabric System) on page 249
- show chassis firmware (ACX2000 Universal Access Router) on page 249
- show chassis firmware detail (EX3300 Switch) on page 250
- show chassis firmware (MX Routers with Media Services Blade [MSB]) on page 250

**Output Fields**

Table 67 on page 242 lists the output fields for the show chassis firmware command. Output fields are listed in the approximate order in which they appear.

**Table 67: show chassis firmware Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part</td>
<td>(MX Series, MX2010, and MX2020 routers) Chassis part name.</td>
</tr>
<tr>
<td>Type</td>
<td>(MX Series, MX2010, and MX2020 routers) Type of firmware: On routers: ROM or O/S. On switches: uboot or loader.</td>
</tr>
</tbody>
</table>
Table 67: show chassis firmware Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC</td>
<td>(detail option only) Number of FPC. For a standalone switch, the value is 0. For a Virtual Chassis configuration, value in the range of 0-9; refers to the member ID assigned to the switch.</td>
</tr>
<tr>
<td>AFEB</td>
<td>(MX104 routers) Version of the compact Forwarding Engine Board.</td>
</tr>
<tr>
<td>Boot</td>
<td>(detail option only) Version of the SYSPLD.</td>
</tr>
<tr>
<td>PoE</td>
<td>(detail option only) Version of the PoE firmware.</td>
</tr>
<tr>
<td>PFE-&lt;number&gt;</td>
<td>(detail option only) Version of the PFE used in the switch.</td>
</tr>
<tr>
<td>PHY-</td>
<td>(detail option only) Version of the physical layer device (PHY) used in the switch.</td>
</tr>
<tr>
<td>microcode</td>
<td>(detail option only) Microcode of the physical layer devices (PHY) used in the switch.</td>
</tr>
<tr>
<td>uboot</td>
<td>(detail option only) Version of the u-boot used in the switch.</td>
</tr>
<tr>
<td>loader</td>
<td>(detail option only) Version of the loader used in the switch.</td>
</tr>
</tbody>
</table>

Sample Output

show chassis firmware (M10 Router)

user@host> show chassis firmware
Part                       Type       Version
Forwarding engine board    ROM        Juniper ROM Monitor Version 4.1b2
                           O/S        Version 4.1I1 by tlim on 2000-04-24 11:27

show chassis firmware (M20 Router)

user@host> show chassis firmware
Part                       Type       Version
System switch board        ROM        Juniper ROM Monitor Version 3.4b26
                           O/S        Version 3.41I6 by smackie on 2000-02-29 2
FPC 1                      ROM        Juniper ROM Monitor Version 3.0b1
                           O/S        Version 3.4I4 by smackie on 2000-02-25 21
FPC 2                      ROM        Juniper ROM Monitor Version 3.0b1
                           O/S        Version 3.4I4 by smackie on 2000-02-25 21

show chassis firmware (M40 Router)

user@host> show chassis firmware
Part                       Type       Version
System control board       ROM        Juniper ROM Monitor Version 2.0i126Copyri
show chassis firmware (M120 Router)

```plaintext
user@host> show chassis firmware
Part                     Type       Version
FPC 0                    ROM        Juniper ROM Monitor Version 4.0b2
O/S        Version 4.0I1 by tlim on 2000-02-29 11:56
FPC 1                    ROM        Juniper ROM Monitor Version 4.0b2
O/S        Version 4.0I1 by tlim on 2000-02-29 11:56
FPC 2                    ROM        Juniper ROM Monitor Version 4.0b3
O/S        Version 4.0I1 by tlim on 2000-02-29 11:56
```

show chassis firmware (M160 Router)

```plaintext
user@host> show chassis firmware
Part                     Type       Version
SFM 0                    ROM        Juniper ROM Monitor Version 4.0b2
O/S        Version 4.0I1 by tlim on 2000-02-29 11:50
SFM 1                    ROM        Juniper ROM Monitor Version 4.0b2
O/S        Version 4.0I1 by tlim on 2000-02-29 11:50
FPC 0                    ROM        Juniper ROM Monitor Version 4.0b2
O/S        Version 4.0I1 by tlim on 2000-02-29 11:56
FPC 1                    ROM        Juniper ROM Monitor Version 4.0b2
O/S        Version 4.0I1 by tlim on 2000-02-29 11:56
FPC 2                    ROM        Juniper ROM Monitor Version 4.0b2
O/S        Version 4.0I1 by tlim on 2000-02-29 11:56
```

show chassis firmware (MX104 Router)

```plaintext
user@host> show chassis firmware
Part                     Type       Version
FPC 0                    ROM        Juniper ROM Monitor Version 13.1b24
O/S        Version 13.2-20130514.1 by builder on 2013-
FPC 1                    ROM        Juniper ROM Monitor Version 13.1b24
O/S        Version 13.2-20130514.1 by builder on 2013-
FPC 2                    ROM        Juniper ROM Monitor Version 13.1b24
O/S        Version 13.2-20130514.1 by builder on 2013-
AFEB                     ROM        Juniper ROM Monitor Version 13.1b24
O/S        Version 13.2-20130514.1 by builder on 2013-
```

show chassis firmware (MX240 Router)

```plaintext
user@host> show chassis firmware
Part                     Type       Version
FPC 1                    ROM        Juniper ROM Monitor Version 8.3b1
O/S        Version 9.0-20080103.0 by builder on 2008-0
FPC 2                    ROM        Juniper ROM Monitor Version 8.3b1
O/S        Version 9.0-20080103.0 by builder on 2008-0
```

show chassis firmware (MX480 Router)

```plaintext
user@host> show chassis firmware
Part                     Type       Version
FPC 1                    ROM        Juniper ROM Monitor Version 8.3b1
O/S        Version 9.0-20070916.3 by builder on 2007-0
### show chassis firmware (MX960 Router)

```
user@host> show chassis firmware
<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 4</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 8.0b8</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 8.2159 by artem on 2006-10-31 19:22</td>
</tr>
<tr>
<td>FPC 7</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 8.2b1</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 8.2-20061026.1 by builder on 2006-1</td>
</tr>
</tbody>
</table>
```

### show chassis firmware (MX2010 Router)

```
user@host> show chassis firmware
<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 12.3b1</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.1b3</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 2</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.1b3</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 3</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.1b3</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 4</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 5</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 6</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.4b1</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 7</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.1b3</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 8</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.4b1</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>FPC 9</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>SPMB 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 12.1b1</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
<tr>
<td>SPMB 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 12.1b1</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20121220.0 by builder on 2012-</td>
</tr>
</tbody>
</table>
```

### show chassis firmware (MX2020 Router)

```
user@host> show chassis firmware
<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 2</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 3</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 4</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 5</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 6</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 7</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 8</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
<tr>
<td>FPC 9</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 10.0b39</td>
</tr>
<tr>
<td></td>
<td>0/S</td>
<td>Version 12.3-20130415.0 by builder on 2013-</td>
</tr>
</tbody>
</table>
```
show chassis firmware (MX240, MX480, MX960 Router with Application Services Modular Line Card)

user@host> show chassis firmware

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 12.2I21 by manish on 2012-06-19 17:27:42</td>
</tr>
</tbody>
</table>

show chassis firmware (EX4200 Switch)

user@switch> show chassis firmware

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>uboot</td>
<td>U-Boot 1.1.6 (Feb 6 2008 - 11:27:42)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.1</td>
</tr>
<tr>
<td>FPC 1</td>
<td>uboot</td>
<td>U-Boot 1.1.6 (Feb 6 2008 - 11:27:42)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.1</td>
</tr>
<tr>
<td>FPC 2</td>
<td>uboot</td>
<td>U-Boot 1.1.6 (Feb 6 2008 - 11:27:42)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.1</td>
</tr>
</tbody>
</table>

show chassis firmware (EX8200 Switch)

user@switch> show chassis firmware

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>U-Boot</td>
<td>U-Boot 1.1.6 (Mar 25 2009 - 06:13:12)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.2</td>
</tr>
<tr>
<td>FPC 3</td>
<td>U-Boot</td>
<td>U-Boot 1.1.6 (Dec 4 2009 - 13:17:34)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.2</td>
</tr>
<tr>
<td>FPC 5</td>
<td>U-Boot</td>
<td>U-Boot 1.1.6 (Mar 25 2009 - 06:13:12)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.2</td>
</tr>
<tr>
<td>FPC 7</td>
<td>U-Boot</td>
<td>U-Boot 1.1.6 (Feb 6 2009 - 05:31:46)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.2</td>
</tr>
<tr>
<td>Routing Engine 0</td>
<td>U-Boot</td>
<td>U-Boot 1.1.6 (Mar 25 2009 - 06:13:12)</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.2</td>
</tr>
</tbody>
</table>
Routing Engine 1  U-Boot  U-Boot 1.1.6 (Mar 25 2009 - 06:13:12) 2.4.0  Loader  FreeBSD/PowerPC U-Boot bootstrap loader 2.2

**show chassis firmware lcc (TX Matrix Router)**

```
user@host> show chassis firmware lcc 0
lcc0-re0:
--------------------------------------------------------------------------
Part                     Type       Version
FPC 1                    ROM        Juniper ROM Monitor Version 6.4b18
O/S        Version 7.0-20040804.0 by builder on 2004-0
FPC 2                    ROM        Juniper ROM Monitor Version 6.4b20
O/S        Version 7.0-20040804.0 by builder on 2004-0
SPMB 0                   ROM        Juniper ROM Monitor Version 6.4b18
O/S        Version 7.0-20040804.0 by builder on 2004-0
```

**show chassis firmware scc (TX Matrix Router)**

```
user@host> show chassis firmware scc
scc-re0:
--------------------------------------------------------------------------
Part                     Type       Version
SPMB 0                   ROM        Juniper ROM Monitor Version 6.4b18
O/S        Version 7.0-20040804.0 by builder on 2004-0
```

**show chassis firmware (TX Matrix Plus Router)**

```
user@host> show chassis firmware
sfc0-re0:
--------------------------------------------------------------------------
Part                     Type       Version
Global FPC 4
Global FPC 6
Global FPC 7
Global FPC 12
Global FPC 14
Global FPC 15
Global FPC 20
Global FPC 21
Global FPC 22
Global FPC 23
Global FPC 24
Global FPC 25
Global FPC 26
Global FPC 28
Global FPC 29
Global FPC 31
SPMB 0                   ROM        Juniper ROM Monitor Version 9.5b1
O/S        Version 9.6-20090507.0 by builder on 2009-0
SPMB 1                   ROM        Juniper ROM Monitor Version 9.5b1
O/S        Version 9.6-20090507.0 by builder on 2009-0
lcc0-re1:
--------------------------------------------------------------------------
Part                     Type       Version
FPC 4                    ROM        Juniper ROM Monitor Version 9.0b2
O/S        Version 9.6-20090507.0 by builder on 2009-0
FPC 6                    ROM        Juniper ROM Monitor Version 9.0b2
O/S        Version 9.6-20090507.0 by builder on 2009-0
FPC 7                    ROM        Juniper ROM Monitor Version 9.0b2
O/S        Version 9.6-20090507.0 by builder on 2009-0
```
### show chassis firmware lcc (TX Matrix Plus Router)

```
user@host> show chassis firmware lcc 0
lcc0-rel:

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 4</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 5</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 6</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 7</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>SPMB 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5bl</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>SPMB 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5bl</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
</tbody>
</table>
```

### show chassis firmware lcc2 (TX Matrix Plus Router)

```
user@host> show chassis firmware lcc 2
lcc2-rel:

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 4</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 5</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 6</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 7</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 7.5b4</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>SPMB 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5bl</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>SPMB 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5bl</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
</tbody>
</table>
```

### show chassis firmware lcc3 (TX Matrix Plus Router)

```
user@host> show chassis firmware lcc 3
lcc3-rel:

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 2</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 4</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 7.5b4</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 5</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>FPC 7</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>SPMB 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5bl</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
<tr>
<td>SPMB 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5bl</td>
</tr>
<tr>
<td></td>
<td>O/S</td>
<td>Version 9.6-20090507.0 by builder on 2009-0</td>
</tr>
</tbody>
</table>
```
show chassis firmware sfc (TX Matrix Plus Router)

```
user@host> show chassis firmware sfc
sfc0-re0:
```

<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global FPC 4</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 6</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 7</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 12</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 14</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 15</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 20</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 21</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 22</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 23</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 24</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 25</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 26</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 28</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 29</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>Global FPC 31</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.0b2</td>
</tr>
<tr>
<td>SPMB 0</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5b1</td>
</tr>
<tr>
<td>SPMB 1</td>
<td>ROM</td>
<td>Juniper ROM Monitor Version 9.5b1</td>
</tr>
</tbody>
</table>

show chassis firmware (QFX Series)

```
user@switch> show chassis firmware
```

```
Part                     Type       Version
FPC 0                     U-Boot     U-Boot 1.1.1.6 (Sep 15 2010 - 02:11:11) 1.0.5
Routing Engine 0          Loader     FreeBSD/MIPS U-Boot bootstrap loader 0.1
```

show chassis firmware interconnect-device (QFabric System)

```
user@switch> show chassis firmware interconnect-device interconnect1
```

```
Part                     Type       Version
Routing Engine 0          U-Boot     U-Boot 1.1.6 (May 10 2011 - 04:52:59) 1.1.1
Routing Engine 1          U-Boot     U-Boot 1.1.6 (May 10 2011 - 04:52:59) 1.1.1
```

show chassis firmware (ACX2000 Universal Access Router)

```
user@switch> show chassis firmware
```

```
Part                     Type       Version
FPC                      0/S        Version 12.2I13 by jisjoy on 2012-05-29 06:249
FEB                      0/S        Version 12.2I13 by jisjoy on 2012-05-29 06:
show chassis firmware detail (EX3300 Switch)

```
user@switch> show chassis firmware detail
FPC 0
  Boot SYSPLD             3
  PoE firmware            4.1.6
  PFE-0                   3
  PFE-1                   3
  PHY
    microcode            0x514
    Boot Firmware
    uboot                U-Boot 1.1.6 (Aug 21 2011 - 01:45:26)   1.0.0
    loader               FreeBSD/arm U-Boot loader 1.0
``` 

show chassis firmware (MX Routers with Media Services Blade [MSB])

```
user@switch> show chassis firmware
Part                     Type       Version
FPC 1                    ROM        Juniper ROM Monitor Version 12.1b1
                         O/S       Version 12.2I21 by manish on 2012-06-19 17:
### show chassis lcd

**show chassis lcd (EX Series)**

```
show chassis lcd
  <fpc-slot fpc-slot-number>
  <menu (all-members | local | member member-id) >>
```

**show chassis lcd (QFX Series and QFabric Systems)**

```
show chassis lcd
  <fpc-slot fpc-slot-number>
  <interconnect-device device-id>
  <node-device device-id>
```

### Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

*menu* option introduced in Junos OS Release 10.2 for EX Series switches.

Command introduced in Junos OS Release 11.1 for the QFX Series.

Command introduced in Junos OS Release 13.1 for QFabric systems.

### Description

Display the information that appears on the LCD panel of EX3200, EX3300, EX4200, EX4500, EX6200, and EX8200 switches, XRE200 External Routing Engines, QFX Series standalone switches, and Interconnect devices and Node devices within a QFabric system. Display the status of the currently selected port parameter of the Status LED for each network port on the device.

### Options

**none**—Display the information that appears on the LCD panel (for any EX Series member switch in a Virtual Chassis or for XRE200 External Routing Engines, display the information for all Virtual Chassis members). Display the status of the currently selected port parameter of the Status LED for each network port.

**fpc-slot <fpc-slot-number>**—(Optional) Display the information as follows:

- (EX3200, EX3300, EX4200, and EX4500 switches, or the QFX Series) Display the information that appears on the LCD panel for either an FPC slot with no *fpc-slot-number* value specified or for the FPC slot specified by *fpc-slot 0*. *fpc-slot* refers to the switch itself and 0 is the only valid value for *fpc-slot-number*. Output for these options is the same as for the *none* option.

  Also display the status of the currently selected port parameter of the Status LED for each network port.

- (EX Series Virtual Chassis member switches or XRE200 External Routing Engines) If no *fpc-slot-number* value is specified, display the information that appears on the LCD panel for all members of the Virtual Chassis. Output for this option is the same as for the *none* option. If the *fpc-slot-number* value is specified (it equals the *member-id* value), display the information for the specified member.

  Also display the status of the currently selected port parameter of the Status LED for each network port.

- (EX6200 or EX8200 switches)—Display the information that appears on the LCD panel for the line card in the line-card slot specified by the *fpc-slot-number* value.

  Also display the status of the currently selected port parameter of the Status LED for each network port.
interconnect-device device-id—(QFabric systems only) (Optional) Display the front panel contents and LED status of all the ports on the Interconnect device.

menu—(Optional) Display the names of the menus and menu options that are currently enabled on the LCD panel.

menu all-members—(EX Series Virtual Chassis member switches or XRE200 External Routing Engines) (Optional) Display the names of the menus and menu options that are currently enabled on the LCD panel for all Virtual Chassis members.

menu local—(EX Series Virtual Chassis member switches or XRE200 External Routing Engines) (Optional) Display the names of the menus and menu options that are currently enabled on the LCD panel for the Virtual Chassis member from which you issued the command.

menu member member-id—(EX Series Virtual Chassis member switches or XRE200 External Routing Engines) (Optional) Display the names of the menus and menu options that are currently enabled on the LCD panel for the specified Virtual Chassis member.

dnode-device device-id—(QFabric systems only) (Optional) Display the front panel contents and LED status of all the ports on the Node device.

Required Privilege

Level view

Related Documentation

- LCD Panel in EX3200 Switches
- LCD Panel in EX4200 Switches
- LCD Panel in EX4500 Switches
- LCD Panel in an EX8200 Switch
- LCD Panel in an XRE200 External Routing Engine
- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- set chassis display message on page 223

List of Sample Output

- show chassis lcd (Two-Member EX4200 Virtual Chassis) on page 253
- show chassis lcd fpc-slot 1 (EX4200 Virtual Chassis) on page 255
- show chassis lcd (EX8200 Switch) on page 255
- show chassis lcd fpc-slot 2 (EX8200 Switch) on page 257
- show chassis lcd menu (EX4200 Switch) on page 257
- show chassis lcd menu (EX8200 Switch) on page 257
- show chassis lcd (QFX3500 Switches) on page 258
- show chassis lcd (XRE200 External Routing Engine in EX8200 Virtual Chassis) on page 258
- show chassis lcd interconnect-device (QFabric Systems) on page 261
- show chassis lcd node-device (QFabric Systems) on page 263

Output Fields

Table 68 on page 253 lists the output fields for the show chassis lcd command. Output fields are listed in the approximate order in which they appear.
### Table 68: show chassis lcd Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>member number</strong> (XRE200 External Routing Engine)</td>
<td>Member ID of the device whose content is being displayed.</td>
</tr>
<tr>
<td><strong>Front panel contents for slot</strong></td>
<td>FPC slot number of the switch whose content is being displayed. The number is always 0, except for EX4200 switches in a Virtual Chassis, where it is the member ID value. On EX6200 switches, EX8200 switches, and XRE200 External Routing Engines, no slot number is displayed. On XRE200 External Routing Engines, this field appears under the <strong>member number</strong> field for each member device in the EX8200 Virtual Chassis.</td>
</tr>
</tbody>
</table>
| **LCD screen** | The first line displays the hostname (for Virtual Chassis members, displays the member ID, the current role, and hostname; for EX8200 switches, displays RE and the hostname). The second line displays the currently selected port parameter of the Status LED and the alarms counter. The Status LED port parameters are:  
  - ADM—Administrative  
  - SPD—Speed  
  - DPX—Duplex  
  - POE—Power over Ethernet (EX3200 and EX4200 switches only) |
| **LEDs status** | Current state of the Alarms, System, and Master LEDs (chassis status LEDs). |
| **Interface** | Names of the interfaces on the switch. |
| **LED (ADM/SPD/DPX/POE)** | State of the currently selected port parameter of the Status LED for the interface. The Status LED port parameters are:  
  **NOTE:** The XRE200 External Routing Engine always displays the **NA** parameter. The QFX Series products do not have any of the port parameters listed below.  
  - ADM—Administrative  
  - SPD—Speed  
  - DPX—Duplex  
  - NA—Not applicable.  
  - POE—Power over Ethernet |
| **fpc** | On standalone EX Series and QFX Series switches, always 0. On EX Series Virtual Chassis member switches, member ID of the Virtual Chassis member whose LCD menu is displayed. |

---

**Sample Output**

*show chassis lcd* (Two-Member EX4200 Virtual Chassis)

```
user@switch> show chassis lcd
Front panel contents for slot: 0
-------------------------------
LCD screen:
  00:BK switch1
  LED: SPD ALARM 00
```
LEDs status:
  Alarms LED: Off
  System LED: Green
  Master LED: Off

<table>
<thead>
<tr>
<th>Interface</th>
<th>LED(ADM/SPD/DPX/POE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/11</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/12</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/13</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/14</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/15</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/16</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/17</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/18</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/19</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/20</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/21</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/22</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/23</td>
<td>Off</td>
</tr>
</tbody>
</table>

Front panel contents for slot: 1

LCD screen:
  01:RE switch2
  LED: SPD ALARM 01

LEDs status:
  Alarms LED: Yellow
  System LED: Green
  Master LED: Green

<table>
<thead>
<tr>
<th>Interface</th>
<th>LED(ADM/SPD/DPX/POE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/0</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/1</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/2</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/3</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/4</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/5</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/6</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/7</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/8</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/9</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/10</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/11</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/12</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/13</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/14</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/15</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/16</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/17</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/18</td>
<td>Off</td>
</tr>
<tr>
<td>ge-1/0/19</td>
<td>Off</td>
</tr>
</tbody>
</table>
The output for the `show chassis lcd fpc-slot` command is the same as the output for the `show chassis lcd` command.

**show chassis lcd fpc-slot 1 (EX4200 Virtual Chassis)**

```
user@switch> show chassis lcd fpc-slot 1
Front panel contents for slot: 1
---------------------------------
LCD screen:
   01:RE switch2
   LED: SPD ALARM 01
LEDs status:
   Alarms LED: Yellow
   System LED: Green
   Master LED: Green
Interface   LED(ADM/SPD/DPX/POE)
-------------------------------------
ge-1/0/0     Off
ge-1/0/1     Off
ge-1/0/2     Off
ge-1/0/3     Off
ge-1/0/4     Off
ge-1/0/5     Off
ge-1/0/6     Off
ge-1/0/7     Off
ge-1/0/8     Off
ge-1/0/9     Off
ge-1/0/10    Off
ge-1/0/11    Off
ge-1/0/12    Off
ge-1/0/13    Off
ge-1/0/14    Off
ge-1/0/15    Off
ge-1/0/16    Off
ge-1/0/17    Off
ge-1/0/18    Off
ge-1/0/19    Off
ge-1/0/20    Off
ge-1/0/21    Off
ge-1/0/22    Off
ge-1/0/23    Off
```

**show chassis lcd (EX8200 Switch)**

```
user@switch> show chassis lcd
Front panel contents:
---------------------
LCD screen:
   RE st-8200-r
   LED: ADM ALARM 01
LEDs status:
   Alarms LED: Yellow
   System LED: Yellow
   Master LED: Green
Interface   LED(ADM/SPD/DPX/POE)
---------------------
ge-0/0/0        Off
ge-0/0/1        Off
ge-0/0/2        Off
ge-0/0/3        Off
ge-0/0/4        Off
ge-0/0/5        Off
ge-0/0/6        Off
ge-0/0/7        Off
ge-0/0/8        Off
ge-0/0/9        Off
ge-0/0/10       Off
ge-0/0/11       Off
ge-0/0/12       Off
ge-0/0/13       Off
ge-0/0/14       Off
ge-0/0/15       Off
ge-0/0/16       Off
ge-0/0/17       Off
ge-0/0/18       Off
ge-0/0/19       Off
ge-0/0/20       Off
ge-0/0/21       Off
ge-0/0/22       Off
ge-0/0/23       Off
ge-0/0/24       Off
ge-0/0/25       Off
ge-0/0/26       Off
ge-0/0/27       Off
ge-0/0/28       Off
ge-0/0/29       Off
ge-0/0/30       Off
ge-0/0/31       Off
ge-0/0/32       Off
ge-0/0/33       Off
ge-0/0/34       Off
ge-0/0/35       Off
ge-0/0/36       Off
ge-0/0/37       Off
ge-0/0/38       Off
ge-0/0/39       Off
ge-0/0/40       Off
ge-0/0/41       Off
ge-0/0/42       Off
ge-0/0/43       Off
ge-0/0/44       Off
ge-0/0/45       Off
ge-0/0/46       Off
ge-0/0/47       Off
xe-2/0/0        Off
xe-2/0/1        Off
xe-2/0/2        Off
xe-2/0/3        Off
xe-2/0/4        Off
xe-2/0/5        Off
xe-2/0/6        Off
xe-2/0/7        Off
xe-3/0/0        Off
xe-3/0/1        Off
xe-3/0/2        Off
xe-3/0/3        Off
show chassis lcd fpc-slot 2 (EX8200 Switch)

show chassis lcd fpc-slot 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>LED(ADM/SPD/DPX)</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-2/0/0</td>
<td>Off</td>
</tr>
<tr>
<td>xe-2/0/1</td>
<td>Off</td>
</tr>
<tr>
<td>xe-2/0/2</td>
<td>Off</td>
</tr>
<tr>
<td>xe-2/0/3</td>
<td>Off</td>
</tr>
<tr>
<td>xe-2/0/4</td>
<td>Off</td>
</tr>
<tr>
<td>xe-2/0/5</td>
<td>Off</td>
</tr>
<tr>
<td>xe-2/0/6</td>
<td>Off</td>
</tr>
<tr>
<td>xe-2/0/7</td>
<td>Off</td>
</tr>
</tbody>
</table>

show chassis lcd menu (EX4200 Switch)

user@switch> show chassis lcd menu
fpc0:

status-menu
status-menu vcp-status
status-menu power-status
status-menu environ-menu
status-menu show-version
maintenance-menu
maintenance-menu halt-menu
maintenance-menu system-reboot
maintenance-menu rescue-config
maintenance-menu vc-uplink-config
maintenance-menu factory-default

On an EX4200 switch in a Virtual Chassis, the output for the show chassis lcd menu all-members command is the same as the output for the show chassis lcd menu command.

show chassis lcd menu (EX8200 Switch)

user@switch> show chassis lcd menu
status-menu
status-menu sf-status1-menu
status-menu sf-status2-menu
status-menu psu-status1-menu
status-menu psu-status2-menu
status-menu environ-menu
status-menu show-version
maintenance-menu
maintenance-menu halt-menu
show chassis lcd (QFX3500 Switches)

user@switch> show chassis lcd
Front panel contents for slot: 0
--------------------------
LCD screen:
00:RE switch
ALARM 01
LEDs status:
Status/Beacon LED: Yellow Blinking
Interface STATUS LED ACTIVITY LED
--------------------------
fte-0/1/0 Off Off

show chassis lcd (XRE200 External Routing Engine in EX8200 Virtual Chassis)

user@external-routing-engine> show chassis lcd
member0:
--------------------------
Front panel contents:
LCD screen:
  RE ex8200-member0
  LED:ADM ALARM 04
LEDs status:
  Alarms LED: Red
  System LED: Yellow
  Master LED: Green

member1:

member8:

member9:
--------------------------
Front panel contents:
LCD screen:
  BACKUP

Interface LED(ADM/SPD/DPX/POE)
--------------------------
ge-0/0/0 On
ge-0/0/1 On
ge-0/0/2 On
ge-0/0/3 On
ge-0/0/4 Off
ge-0/0/5 Off
ge-0/0/6 Off
ge-0/0/7 Off
ge-0/0/8 Off
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/9</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/11</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/12</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/13</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/14</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/15</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/16</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/17</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/18</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/19</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/20</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/21</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/22</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/23</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/24</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/25</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/26</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/27</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/28</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/29</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/30</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/31</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/32</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/33</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/34</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/35</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/36</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/37</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/38</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/39</td>
<td>Off</td>
</tr>
<tr>
<td>ge-0/0/40</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/41</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/42</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/43</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/44</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/45</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/46</td>
<td>On</td>
</tr>
<tr>
<td>ge-0/0/47</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/0</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/1</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/2</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/3</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/4</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/5</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/6</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/7</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/8</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/9</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/10</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/11</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/12</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/13</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/14</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/15</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/16</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/17</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/18</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/19</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/20</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/21</td>
<td>Off</td>
</tr>
<tr>
<td>Interface</td>
<td>Status</td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>ge-16/0/22</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/23</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/24</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/25</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/26</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/27</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/28</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/29</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/30</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/31</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/32</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/33</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/34</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/35</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/36</td>
<td>On</td>
</tr>
<tr>
<td>ge-16/0/37</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/38</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/39</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/40</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/41</td>
<td>Off</td>
</tr>
<tr>
<td>ge-16/0/42</td>
<td>On</td>
</tr>
<tr>
<td>xe-19/0/0</td>
<td>Off</td>
</tr>
<tr>
<td>xe-19/0/1</td>
<td>On</td>
</tr>
<tr>
<td>xe-19/0/2</td>
<td>On</td>
</tr>
<tr>
<td>xe-19/0/3</td>
<td>On</td>
</tr>
<tr>
<td>xe-19/0/4</td>
<td>On</td>
</tr>
<tr>
<td>xe-19/0/5</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/0</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/1</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/2</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/3</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/4</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/5</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/6</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/7</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/8</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/9</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/10</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/11</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/12</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/13</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/14</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/15</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/16</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/17</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/18</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/19</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/20</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/21</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/22</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/23</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/24</td>
<td>On</td>
</tr>
<tr>
<td>ge-22/0/25</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/26</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/27</td>
<td>Off</td>
</tr>
<tr>
<td>ge-22/0/28</td>
<td>Off</td>
</tr>
</tbody>
</table>
show chassis lcd interconnect-device (QFabric Systems)

show chassis lcd interconnect-device IC-F1012
Front Panel Module Information
---------------------------------
LCD screen:
IC-F1012 3 Alarms active

LEDs status:
Status LED: Green
Power LED: Green
Major Alarm LED: off
Minor Alarm LED: Yellow
Fan 0 LED: Green
Fan 1 LED: Green
Fan 2 LED: Green
Fan 3 LED: Green
Fan 4 LED: Green
Fan 5 LED: Green
Fan 6 LED: Green
Fan 7 LED: Green
Fan 8 LED: Green
Fan 9 LED: Green
PEM 0 LED: Green
PEM 1 LED: Green
PEM 2 LED: Green
PEM 3 LED: off
PEM 4 LED: off
PEM 5 LED: off

LED info for: CB - 0
---------------------------------

LEDs status:
Status LED: Green
Mastership LED: Green

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-F1012:pme0</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:pme1</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:pme2</td>
<td>off</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:pme3</td>
<td>off</td>
<td>N/A</td>
</tr>
</tbody>
</table>
LED info for: CB - 1
---------------------------------
LEDs status:
  Status LED: Green
  Mastership LED: Amber

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-F1012:pme0</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:pme1</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:pme2</td>
<td>off</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:pme3</td>
<td>off</td>
<td>N/A</td>
</tr>
</tbody>
</table>

LED info for: FC 0 FPC - 0
---------------------------------
LEDs status:
  Status LED: Green

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-F1012:fte-0/0/0</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-0/0/1</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-0/0/2</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-0/0/3</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-0/0/4</td>
<td>Green</td>
<td>N/A</td>
</tr>
</tbody>
</table>

LED info for: FC 1 FPC - 1
---------------------------------
LEDs status:
  Status LED: Green

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-F1012:fte-1/0/0</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-1/0/1</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-1/0/2</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-1/0/3</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F1012:fte-1/0/4</td>
<td>Green</td>
<td>N/A</td>
</tr>
</tbody>
</table>

LED info for: RC 0 FPC - 8
---------------------------------
LEDs status:
  Status LED: Green

LED info for: RC 1 FPC - 9
---------------------------------
LEDs status:
  Status LED: Green

LED info for: RC 2 FPC - 10
---------------------------------
LEDs status:
  Status LED: Green

LED info for: RC 3 FPC - 11
---------------------------------
LEDs status:
  Status LED: Green

LED info for: RC 4 FPC - 12
---------------------------------
show chassis lcpu node-device (QFabric Systems)
show chassis lcpu node-device P3774-C
Front panel contents for: P3774-C
-----------------------------------
LCD screen:
P3774-C
LEDs status:
    Status/Beacon LED: Yellow Blinking

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3774-C:xe-0/0/6</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:xe-0/0/7</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/10</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/11</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/12</td>
<td>Green</td>
<td>Off</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/13</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/20</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/21</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/22</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/23</td>
<td>Green</td>
<td>Off</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/30</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/31</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/32</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>P3774-C:ge-0/0/33</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>P3774-C:fte-0/1/0</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>P3774-C:fte-0/1/1</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>P3774-C:fte-0/1/2</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>P3774-C:fte-0/1/3</td>
<td>Green</td>
<td>Green</td>
</tr>
</tbody>
</table>
**show configuration**

**Syntax**

show configuration
<statement-path>

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display the configuration that currently is running on the router or switch, which is the last committed configuration.

**Options**

- **none**—Display the entire configuration.

- **statement-path**—(Optional) Display one of the following hierarchies in a configuration.
  (Each **statement-path** option has additional suboptions not described here. See the appropriate configuration guide or EX Series switch documentation for more information.)
  - **access**—Network access configuration.
  - **access-profile**—Access profile configuration.
  - **accounting-options**—Accounting data configuration.
  - **applications**—Applications defined by protocol characteristics.
  - **apply-groups**—Groups from which configuration data is inherited.
  - **chassis**—Chassis configuration.
  - **chassis network-services**—Current running mode.
  - **class-of-service**—Class-of-service configuration.
  - **diameter**—Diameter base protocol layer configuration.
  - **ethernet-switching-options**—(EX Series switch only) Ethernet switching configuration.
  - **event-options**—Event processing configuration.
  - **firewall**—Firewall configuration.
  - **forwarding-options**—Options that control packet sampling.
  - **groups**—Configuration groups.
  - **interfaces**—Interface configuration.
  - **jsrc**—JSRC partition configuration.
  - **jsrc-partition**—JSRC partition configuration.
  - **logical-systems**—Logical system configuration.
  - **poe**—(EX Series switch only) Power over Ethernet configuration.
  - **policy-options**—Routing policy option configuration.
  - **protocols**—Routing protocol configuration.
• **routing-instances**—Routing instance configuration.
• **routing-options**—Protocol-independent routing option configuration.
• **security**—Security configuration.
• **services**—Service PIC applications configuration.
• **snmp**—Simple Network Management Protocol configuration.
• **system**—System parameters configuration.
• **virtual-chassis**—(EX Series switch only) Virtual Chassis configuration.
• **vlans**—(EX Series switch only) VLAN configuration.

**Additional Information**
The portions of the configuration that you can view depend on the user class that you belong to and the corresponding permissions. If you do not have permission to view a portion of the configuration, the text **ACCESS-DENIED** is substituted for that portion of the configuration. If you do not have permission to view authentication keys and passwords in the configuration, because the secret permission bit is not set for your user account, the text **SECRET-DATA** is substituted for that portion of the configuration. If an identifier in the configuration contains a space, the identifier is displayed in quotation marks.

Likewise, when you issue the `show configuration` command with the **display set** pipe option to view the configuration as **set** commands, those portions of the configuration that you do not have permissions to view are substituted with the text **ACCESS-DENIED**.

**Required Privilege Level**
```plaintext
view
```

**Related Documentation**
- Displaying the Current Junos OS Configuration
- Overview of Junos OS CLI Operational Mode Commands

**List of Sample Output**
- `show configuration` on page 265
- `show configuration policy-options` on page 266

**Output Fields**
This command displays information about the current running configuration.

**Sample Output**
```
user@host> show configuration
## Last commit: 2006-10-31 14:13:00 PST by alant version "8.2I0 [builder]"; ##
last changed: 2006-10-31 14:05:53 PST
system {
    host-name nestor;
    domain-name east.net;
    backup-router 192.1.1.254;
    time-zone America/Los_Angeles;
    default-address-selection;
    name-server {
        192.154.169.254;
        192.154.169.249;
    }
```
show configuration policy-options

user@host> show configuration policy-options
policy-options {
  policy-statement "direct routes" {
    from protocol direct;
    then accept;
  }
}
show host

Syntax  show host hostname

Release Information  Command introduced before Junos OS Release 7.4.
                    Command introduced in Junos OS Release 9.0 for EX Series switches.
                    Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  Display Domain Name System (DNS) hostname information.

Options  hostname—Hostname or address.

Additional Information  The show host command displays the raw data received from the DNS server.

Required Privilege  view

Level

List of Sample Output  show host on page 267

Sample Output

show host

user@host> show host snark
snark.boojum.net has address 192.168.1.254

user@host> show host 192.168.1.254
Name: snark.boojum.net
Address: 192.168.1.254
Aliases:
**show ntp associations**

**Syntax**
show ntp associations
<no-resolve>

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Display Network Time Protocol (NTP) peers and their state.

**Options**
none—Display NTP peers and their state.
no-resolve—(Optional) Suppress symbolic addressing.

**Required Privilege**
view

**Related Documentation**
- show ntp status on page 270

**List of Sample Output**
show ntp associations on page 269

**Output Fields**
Table 69 on page 268 describes the output fields for the show ntp associations command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote</td>
<td>Address or name of the remote NTP peer.</td>
</tr>
<tr>
<td>refid</td>
<td>Reference identifier of the remote peer. If the reference identifier is not known, this field shows a value of 0.0.0.0.</td>
</tr>
<tr>
<td>st</td>
<td>Stratum of the remote peer.</td>
</tr>
<tr>
<td>t</td>
<td>Type of peer: b (broadcast), l (local), m (multicast), or u (unicast).</td>
</tr>
<tr>
<td>when</td>
<td>When the last packet from the peer was received.</td>
</tr>
<tr>
<td>poll</td>
<td>Polling interval, in seconds.</td>
</tr>
<tr>
<td>reach</td>
<td>Reachability register, in octal.</td>
</tr>
<tr>
<td>delay</td>
<td>Current estimated delay of the peer, in milliseconds.</td>
</tr>
<tr>
<td>offset</td>
<td>Current estimated offset of the peer, in milliseconds.</td>
</tr>
<tr>
<td>disp</td>
<td>Current estimated dispersion of the peer, in milliseconds.</td>
</tr>
</tbody>
</table>
Table 69: show ntp associations Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>peer-name</strong></td>
<td>Peer name and status of the peer in the clock selection process:</td>
</tr>
<tr>
<td>space</td>
<td>Discarded because of a high stratum value or failed sanity checks.</td>
</tr>
<tr>
<td>x</td>
<td>Designated “falseticker” by the intersection algorithm.</td>
</tr>
<tr>
<td>.</td>
<td>Culled from the end of the candidate list.</td>
</tr>
<tr>
<td>–</td>
<td>Discarded by the clustering algorithm.</td>
</tr>
<tr>
<td>+</td>
<td>Included in the final selection set.</td>
</tr>
<tr>
<td>#</td>
<td>Selected for synchronization, but the distance exceeds the maximum.</td>
</tr>
<tr>
<td>*</td>
<td>Selected for synchronization.</td>
</tr>
<tr>
<td>o</td>
<td>Selected for synchronization, but the packets-per-second (pps) signal is in use.</td>
</tr>
</tbody>
</table>

Sample Output

show ntp associations

```
user@host> show ntp associations
remote   refid   st t when poll reach   delay   offset   disp
[Output truncated for brevity]
* wolfe-gw.junipe.tick.ucla.edu 2 u 43 64 377 1.86 0.319 0.08
```
**show ntp status**

**Syntax**

```
show ntp status
<no-resolve>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display the values of internal variables returned by Network Time Protocol (NTP) peers.

**Options**

- **none**—Display the values of internal variables returned by NTP peers.
- **no-resolve**—(Optional) Suppress symbolic addressing.

**Required Privilege**

Level: view

**Related Documentation**

- [show ntp associations on page 268](#)

**List of Sample Output**

[show ntp status on page 271](#)

**Output Fields**

Table 70 on page 270 describes the output fields for the `show ntp status` command. Output fields are listed in the approximate order in which they appear.

**Table 70: show ntp status Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>System status word, a code representing the status items listed.</td>
</tr>
<tr>
<td>leapnone</td>
<td>Indicates a normal synchronized state with no leap seconds imminent. Other options could be <strong>leap_add_sec</strong>, <strong>leap_del_sec</strong>, or <strong>leap_alarm</strong>, indicating a leap second will be added, deleted, or a leap second requirement is upcoming.</td>
</tr>
<tr>
<td>syncntp</td>
<td>Indicates the current synchronization source, in this case, an NTP server. Other options include <strong>sync_alarm</strong> and <strong>sync_unspec</strong>, both indicating that the router has not been synched.</td>
</tr>
<tr>
<td>xevents</td>
<td>Indicates the number of events that have occurred since that last code change. An event is often the receipt of an NTP polling message.</td>
</tr>
<tr>
<td>eventpeerstratchg</td>
<td>Describes the most recent event, in this case, the stratum of the peer server changed.</td>
</tr>
<tr>
<td>version</td>
<td>A detailed description of the version of NTP being used.</td>
</tr>
<tr>
<td>processor</td>
<td>Indicates the current hardware platform and version of the processor.</td>
</tr>
<tr>
<td>system</td>
<td>Detailed description of the name and version of the operating system in use.</td>
</tr>
<tr>
<td>leap</td>
<td>The number of leap seconds in use.</td>
</tr>
</tbody>
</table>
# Table 70: show ntp status Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stratum</td>
<td>The stratum of the peer server. Anything greater than 1 is a secondary reference source, and the number roughly represents the number of hops away from the stratum 1 server. Stratum 1 is a primary reference, such as an atomic clock.</td>
</tr>
<tr>
<td>precision</td>
<td>The precision of the peer clock, how precisely the frequency and time can be maintained with this particular timekeeping system.</td>
</tr>
<tr>
<td>rootdelay</td>
<td>The total roundtrip delay to the primary reference source, in seconds.</td>
</tr>
<tr>
<td>rootdispersion</td>
<td>The maximum error relative to the primary reference source, in seconds.</td>
</tr>
<tr>
<td>peer</td>
<td>An identification number of the peer in use.</td>
</tr>
<tr>
<td>refid</td>
<td>Reference identifier of the remote peer. If the reference identifier is not known, this field shows a value of 0.0.0.0.</td>
</tr>
<tr>
<td>reftime</td>
<td>The local time, in timestamp format, when the local clock was last updated. If the local clock has never been synchronized, the value is zero.</td>
</tr>
<tr>
<td>poll</td>
<td>The NTP broadcast message polling interval, in seconds.</td>
</tr>
<tr>
<td>clock</td>
<td>The current time on the local router clock.</td>
</tr>
<tr>
<td>state</td>
<td>The current mode of NTP operation, where 1 is symmetric active, 2 is symmetric passive, 3 is client, 4 is server, and 5 is broadcast.</td>
</tr>
<tr>
<td>offset</td>
<td>Current estimated offset of the peer, in milliseconds. Indicates the time difference between the reference clock and the local clock.</td>
</tr>
<tr>
<td>frequency</td>
<td>The frequency of the clock.</td>
</tr>
<tr>
<td>jitter</td>
<td>Indicates the magnitude of jitter, in milliseconds, between several time queries.</td>
</tr>
<tr>
<td>stability</td>
<td>A measure of how well this clock can maintain a constant frequency.</td>
</tr>
</tbody>
</table>

## Sample Output

```
show ntp status
```

```
user@host>  show ntp status
assID=0  status=0544  leap=None, sync_local_proto, 4 events, event_peer/strat_chg
version="ntpd 4.2.2p101.1570-0 Tue May 19 13:57:55 UTC 2009 (1)"
processor="x86_64", system="Linux/2.6.18-164.el5", leap=00, stratum=4,
precision=-10, rootdelay=0.000, rootdispersion=11.974, peer=59475,
refid=LOCAL(0),
reftime=d495c32c.0e71eaf2  Mon, Jan  7 2013 13:57:00.056, poll=10,
clock=d495c32c.cebd43bd  Mon, Jan  7 2013 13:57:00.807, state=4,
offset=0.000, frequency=0.000, jitter=0.977, noise=0.977,
stability=0.000, tai=0
```
show system firmware

Syntax

```
show system firmware
<compatibility>
```

Release Information

Command introduced in Junos OS Release 7.4.
Command introduced in Junos OS Release 9.4 for EX Series switches.

Description

(J Series routers and EX8200 switches only) Display firmware information.

```
NOTE: On SRX100, SRX210, SRX240, and SRX 650 devices, the show system firmware command now displays all the installed firmware versions, even if the installed firmware versions are earlier than the currently installed firmware version.
```

Options

- `compatibility`—(Optional) Display firmware compatibility information.

Required Privilege Level

- `view`

List of Sample Output

- `show system firmware on page 274`
- `show system firmware compatibility on page 274`

Output Fields

Table 71 on page 273 lists the output fields for the show system firmware command. Output fields are listed in the approximate order in which they appear.

Table 71: show system firmware Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part</td>
<td>Physical part on the router or switch affected by the firmware.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of firmware on the router or switch.</td>
</tr>
<tr>
<td>Tag</td>
<td>Location of the firmware on the interface.</td>
</tr>
<tr>
<td>Current version</td>
<td>Firmware version on the affected router or switch parts.</td>
</tr>
<tr>
<td>Available version</td>
<td>New versions of firmware for upgrading or downgrading.</td>
</tr>
<tr>
<td>Status</td>
<td>Firmware condition on the router or switch.</td>
</tr>
<tr>
<td>Action</td>
<td>Whether you can upgrade or downgrade, or if no action is available (none).</td>
</tr>
</tbody>
</table>
### Sample Output

#### show system firmware

```
user@host> show system firmware
Part       Type           Tag Current version  Available version Status
FPC 0      ROM Monitor 0  0 6.4.10              0                   OK
Routing Engine 0 RE BIOS  0 0                   0                   OK
```

#### show system firmware compatibility

```
user@host> show system firmware compatibility
Part       Type           Tag Current version  Available version Action
FPC 0      ROM Monitor 0  0 6.4.10              0                   None
Routing Engine 0 RE BIOS  0 0                   0                   None
```
show system reboot

Syntax
show system reboot
<both-routing-engines>

Syntax (EX Series Switches)
show system reboot
<all-members>
<both-routing-engines>
<local>
<member member-id>

Syntax (TX Matrix Router)
show system reboot
<all-chassis | all-lcc | lcc number | scc>
<both-routing-engines>

Syntax (TX Matrix Plus Router)
show system reboot
<all-chassis | all-lcc | lcc number | sfc number>
<both-routing-engines>

Syntax (MX Series Router)
show system reboot
<all-members>
<both-routing-engines>
<local>
<member member-id>

Syntax (QFX Series)
show system reboot
<both-routing-engines>
<infrastructure name>
<interconnect-device name>
<node-device name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display pending system reboots or halts.

Options
none—Display pending reboots or halts on the active Routing Engine.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display halt or reboot request information for all the T640 routers in the chassis that are connected to the TX Matrix router. On a TX Matrix router, display halt or reboot request information for all the T1600 or T4000 routers in the chassis that are connected to the TX Matrix Plus router.

all-members—(EX4200 switches and MX Series routers only) (Optional) Display halt or reboot request information for all members of the Virtual Chassis configuration.

all-lcc—(TX Matrix routers and TX Matrix Plus router only) (Optional) On a TX Matrix router, display system halt or reboot request information for all T640 routers...
connected to the TX Matrix router. On a TX Matrix Plus router, display halt or reboot request information for all connected T1600 or T4000 LCCs.

**both-routing-engines**—(Systems with multiple Routing Engines) (Optional) Display halt or reboot request information on both Routing Engines.

**infrastructure name**—(QFabric systems only) (Optional) Display reboot request information on the fabric manager Routing Engines and fabric control Routing Engines.

**interconnect-device name**—(QFabric systems only) (Optional) Display reboot request information on the Interconnect device.

**lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display halt or reboot request information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display halt or reboot request information for a specific router that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(EX4200 switches and MX Series routers only) (Optional) Display halt or reboot request information for the local Virtual Chassis member.

**member member-id**—(EX4200 switches and MX Series routers only) (Optional) Display halt or reboot request information for the specified member of the Virtual Chassis configuration. For EX4200 switches, replace *member-id* with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

**node-group name**—(QFabric systems only) (Optional) Display reboot request information on the Node group.

**scc**—(TX Matrix router only) (Optional) Display halt or reboot request information for the TX Matrix router (or switch-card chassis).

**sfc**—(TX Matrix Plus router only) (Optional) Display halt or reboot request information for the TX Matrix Plus router.

**Additional Information** By default, when you issue the `show system reboot` command on a TX Matrix or TX Matrix Plus master Routing Engine, the command is broadcast to all the T640 (in a routing matrix based on the TX Matrix router) or T1600 (in a routing matrix based on the TX Matrix Plus router) master Routing Engines connected to it. Likewise, if you issue the
same command on the TX Matrix or TX Matrix Plus backup Routing Engine, the command is broadcast to all the T640 (in a routing matrix based on the TX Matrix router) or T1600 (in a routing matrix based on the TX Matrix Plus router) backup Routing Engines that are connected to it.

**Required Privilege Level**

- maintenance

**Related Documentation**

- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

**List of Sample Output**

- `show system reboot` on page 277
- `show system reboot all-lcc (TX Matrix Router)` on page 277
- `show system reboot sfc (TX Matrix Plus Router)` on page 277
- `show system reboot (QFX3500 Switch)` on page 277

**Sample Output**

`show system reboot`

```
user@host> show system reboot
reboot requested by root at Wed Feb 10 17:40:46 1999
[process id 17885]
```

`show system reboot all-lcc (TX Matrix Router)`

```
user@host> show system reboot all-lcc
lcc0-re0:
-------------------------------------------------
No shutdown/reboot scheduled.

lcc2-re0:
-------------------------------------------------
No shutdown/reboot scheduled.
```

`show system reboot sfc (TX Matrix Plus Router)`

```
user@host> show system sfc 0
No shutdown/reboot scheduled.
```

`show system reboot (QFX3500 Switch)`

```
user@switch> show system reboot
No shutdown/reboot scheduled.
```
**show system software**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show system software</td>
<td>Display the Junos OS extensions loaded on your router or switch.</td>
</tr>
</tbody>
</table>

**Options**

- **none**—Display standard information about all loaded Junos OS extensions.
- **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system software information for all the T640 routers (TX Matrix Router) or all the routers (TX Matrix Plus Router) in the chassis.
- **all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system software information for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system software information for all connected TI600 or T4000 LCCs.
- **all-members**—(EX4200 switches only) (Optional) Display the system software running on all members of the Virtual Chassis configuration.
- **backup**—(J Series routers only) (Optional) Display the status of old system software packages only.

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `sfc` option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
detail—(Optional) Display detailed information about available Junos OS extensions.

infrastructure name—(QFabric systems only) (Optional) Display the system software running on the fabric control Routing Engine and the fabric manager Routing Engine.

interconnect-device name—(QFabric systems only) (Optional) Display the system software running on the Interconnect device.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system software information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system software information for a specific router that is connected to the TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SiBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SiBs in a routing matrix.

local—(EX4200 switches only) (Optional) Display the system software running on the local Virtual Chassis member.

member member-id—(EX4200 switches only) (Optional) Display the system software running on the specified member of the Virtual Chassis configuration. Replace member-id with a value from 0 through 9.

node-group name—(QFabric systems only) (Optional) Display the system software running on the Node group.

scc—(Routing matrix only) (Optional) Display the system software running on a TX Matrix router (or switch-card chassis).

sfc—(TX Matrix Plus routers only) (Optional) Display system software information for the TX Matrix Plus router.

Required Privilege Level
maintenance

Related Documentation
Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output
show system software on page 280
show system software (TX Matrix Plus Router) on page 280
show system software (QFX Series) on page 284
Output Fields  When you enter this command, you are provided a list of Junos OS packages installed on the router and their corresponding Junos OS release number.

Sample Output

show system software

user@host> show system software
Information for jbase:
Comment:
JUNOS Base OS Software Suite [7.2R1.7]

Information for jcrypto:
Comment:
JUNOS Crypto Software Suite [7.2R1.7]
Information for jdocs:
Comment:
JUNOS Online Documentation [7.2R1.7]

Information for jkernel:
Comment:
JUNOS Kernel Software Suite [7.2R1.7]

Information for jpfe:
Comment:
JUNOS Packet Forwarding Engine Support (M20/M40) [7.2R1.7]

Information for jroute:
Comment:
JUNOS Routing Software Suite [7.2R1.7]

Information for junos:
Comment:
JUNOS Base OS boot [7.2R1.7]

show system software (TX Matrix Plus Router)

user@host> show system software
sfc0-re0:  show system software
-----------------------------------------------
Information for jbase:
Comment:
JUNOS Base OS Software Suite [9.6-20090515.0]
Information for jservices-llpdf:

Comment:
JUNOS Services LL-PDF Container package [9.6-20090515.0]

Information for jservices-sfw:

Comment:
JUNOS Services Stateful Firewall [9.6-20090515.0]
Information for jservices-voice:

Comment:
JUNOS Voice Services Container package [9.6-20090515.0]

Information for junos:

Comment:
JUNOS Base OS boot [9.6-20090515.0]

Information for jbase:

Comment:
JUNOS Base OS Software Suite [9.6-20090515.0]

Information for jcrypto:

Comment:
JUNOS Crypto Software Suite [9.6-20090515.0]

Information for jdocs:

Comment:
JUNOS Online Documentation [9.6-20090515.0]

Information for jkernel:

Comment:
JUNOS Kernel Software Suite [9.6-20090515.0]

Information for jpfe:

Comment:
JUNOS Packet Forwarding Engine Support (T-Series) [9.6-20090515.0]

Information for jpfe-common:
Comment:
JUNOS Packet Forwarding Engine Support (M/T Common) [9.6-20090515.0]

Information for jroute:
Comment:
JUNOS Routing Software Suite [9.6-20090515.0]

Information for jservices-aacl:
Comment:
JUNOS Services AAACL Container package [9.6-20090515.0]

Information for jservices-appid:
Comment:
JUNOS AppId Services [9.6-20090515.0]

Information for jservices-bgf:
Comment:
JUNOS Border Gateway Function package [9.6-20090515.0]

Information for jservices-idp:
Comment:
JUNOS IDP Services [9.6-20090515.0]

Information for jservices-llpdf:
Comment:
JUNOS Services LL-PDF Container package [9.6-20090515.0]

Information for jservices-sfw:
Comment:
JUNOS Services Stateful Firewall [9.6-20090515.0]

Information for jservices-voice:
Comment:
JUNOS Voice Services Container package [9.6-20090515.0]
Information for junos:
Comment:
JUNOS Base OS boot [9.6-20090515.0]

lcc1-re0:
-------------------------------------------------------------------------
Information for jbase:
Comment:
JUNOS Base OS Software Suite [9.6-20090515.0]

Information for jcrypto:
Comment:
JUNOS Crypto Software Suite [9.6-20090515.0]

show system software (QFX Series)

user@switch> show system software
Information for jbase:
Comment:
JUNOS Base OS Software Suite [11.3-20110730.0]

Information for jcrypto:
Comment:
JUNOS Crypto Software Suite [11.3-20110730.0]

Information for jdocs:
Comment:
JUNOS Online Documentation [11.3-20110730.0]

Information for jkernel:
Comment:
JUNOS Kernel Software Suite [11.3-20110730.0]

Information for jpfe:
Comment:
JUNOS Packet Forwarding Engine Support (QFX) [11.3-20110730.0]
Information for jroute:

Comment:
JUNOS Routing Software Suite [11.3-20110730.0]

Information for jswitch:

Comment:
JUNOS Enterprise Software Suite [11.3-20110730.0]

Information for junos:

Comment:
JUNOS Base OS boot [11.3-20110730.0]

Information for jweb:

Comment:
JUNOS Web Management [11.3-20110730.0]
show system storage

Syntax

show system storage
<detail>

Syntax (EX Series Switches)

show system storage
<detail>
<all-members>
<local>
<member member-id>

Syntax (MX Series Router)

show system storage
<detail>
<all-members>
<local>
<member member-id>

Syntax (QFX Series)

show system storage
<detail>
<infrastructure name>
<interconnect-device name>
<node-group name>

Syntax (SRX Series)

show system storage
<detail>
<partitions>

For more information, see show system storage partitions (View SRX Series).

Syntax (TX Matrix Router)

show system storage
<detail>
<all-chassis | all-lcc | lcc number | scc>

Syntax (TX Matrix Plus Router and TX Matrix Plus Router with 3D SIBs)

show system storage
<detail>
<all-chassis | all-lcc | lcc number | sfc number>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

sfc option introduced for the TX Matrix Plus router in JUNOS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display statistics about the amount of free disk space in the router’s or switch’s file systems.

Options

none—Display standard information about the amount of free disk space in the router’s or switch’s file systems.

detail—(Optional) Display detailed output.
all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system storage statistics for all the routers in the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system storage statistics for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system storage statistics for all routers connected to the TX Matrix Plus router.

all-members—(EX4200 switches and MX Series routers only) (Optional) Display system storage statistics for all members of the Virtual Chassis configuration.

infrastructure name—(QFabric systems only) (Optional) Display system storage statistics for the fabric control Routing Engines or fabric manager Routing Engines.

interconnect-device name—(QFabric systems only) (Optional) Display system storage statistics for the Interconnect device.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system storage statistics for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system storage statistics for a specific router that is connected to the TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Display system storage statistics for the local Virtual Chassis member.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Display system storage statistics for the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

node-group name—(QFabric systems only) (Optional) Display system storage statistics for the Node group.

scc—(TX Matrix routers only) (Optional) Display system storage statistics for the TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus routers only) (Optional) Display system storage statistics for the TX Matrix Plus router. Replace number with 0.
Additional Information

By default, when you issue the `show system storage` command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level

view

Related Documentation

- Routing Matrix with a TX Matrix Plus Router Solutions Page
- `show system storage partitions (View SRX Series)`

List of Sample Output

show system storage on page 288
show system storage (TX Matrix Plus Router) on page 289
show system storage (QFX3500 Switch) on page 291

Output Fields

Table 72 on page 288 describes the output fields for the `show system storage` command. Output fields are listed in the approximate order in which they appear.

Table 72: show system storage Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filesystem</td>
<td>Name of the filesystem.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the filesystem.</td>
</tr>
<tr>
<td>Used</td>
<td>Amount of space used in the filesystem.</td>
</tr>
<tr>
<td>Avail</td>
<td>Amount of space available in the filesystem.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Percentage of the filesystem space that is being used.</td>
</tr>
<tr>
<td>Mounted on</td>
<td>Directory in which the filesystem is mounted.</td>
</tr>
</tbody>
</table>

Sample Output

show system storage

```
user@host> show system storage
Filesystem  Size   Used   Avail  Capacity Mounted on
/dev/ad0s1a  77M    37M    34M   52%      / 
devfs       16K    16K         0B  100%   /dev/
/dev/vn0    12M    12M         0B  100% /packages/mnt/jbase
/dev/vn1    39M    39M         0B  100% /packages/mnt/jbase
/packages/mnt/jkernel-7.2R1.7  12M    12M         0B   100% /packages/mnt/jbase
/packages/mnt/jpfe-M40-7.2R1.7  2.3M   2.3M         0B   100% /packages/mnt/jbase
/packages/mnt/jdocs-7.2R1.7  14M    14M         0B   100% /packages/mnt/jbase
/dev/vn4
```

Copyright © 2013, Juniper Networks, Inc.
show system storage (TX Matrix Plus Router)

user@host> show system storage
sfc0-re0:
-------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Capacity</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/ad0s1a</td>
<td>3.4G</td>
<td>178M</td>
<td>2.9G</td>
<td>6%</td>
<td>/</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev/</td>
</tr>
<tr>
<td>/dev/md0</td>
<td>33M</td>
<td>33M</td>
<td>0B</td>
<td>100%</td>
<td>/packages/mnt/jbase</td>
</tr>
<tr>
<td>/dev/md1</td>
<td>216M</td>
<td>216M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md2</td>
<td>66M</td>
<td>66M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md3</td>
<td>4.1M</td>
<td>4.1M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md4</td>
<td>57M</td>
<td>57M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md5</td>
<td>15M</td>
<td>15M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md6</td>
<td>34M</td>
<td>34M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md7</td>
<td>2.0G</td>
<td>10.0K</td>
<td>1.8G</td>
<td>0%</td>
<td>/tmp</td>
</tr>
<tr>
<td>/dev/md8</td>
<td>2.0G</td>
<td>1.0M</td>
<td>1.8G</td>
<td>0%</td>
<td>/mfs</td>
</tr>
<tr>
<td>/dev/ad0s1e</td>
<td>383M</td>
<td>82K</td>
<td>352M</td>
<td>0%</td>
<td>/config</td>
</tr>
<tr>
<td>procs</td>
<td>4.0K</td>
<td>4.0K</td>
<td>0B</td>
<td>100%</td>
<td>/proc</td>
</tr>
<tr>
<td>/dev/ad1s1f</td>
<td>52G</td>
<td>7.5G</td>
<td>40G</td>
<td>16%</td>
<td>/var</td>
</tr>
</tbody>
</table>
lcc0-re0:
-------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Capacity</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/ad0s1a</td>
<td>3.4G</td>
<td>178M</td>
<td>2.9G</td>
<td>6%</td>
<td>/</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev/</td>
</tr>
<tr>
<td>/dev/md0</td>
<td>33M</td>
<td>33M</td>
<td>0B</td>
<td>100%</td>
<td>/packages/mnt/jbase</td>
</tr>
<tr>
<td>/dev/md1</td>
<td>216M</td>
<td>216M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md2</td>
<td>66M</td>
<td>66M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md3</td>
<td>4.1M</td>
<td>4.1M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md4</td>
<td>57M</td>
<td>57M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md5</td>
<td>15M</td>
<td>15M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md6</td>
<td>34M</td>
<td>34M</td>
<td>0B</td>
<td>100%</td>
<td>/</td>
</tr>
<tr>
<td>/dev/md7</td>
<td>2.0G</td>
<td>10.0K</td>
<td>1.8G</td>
<td>0%</td>
<td>/tmp</td>
</tr>
<tr>
<td>/dev/md8</td>
<td>2.0G</td>
<td>1.0M</td>
<td>1.8G</td>
<td>0%</td>
<td>/mfs</td>
</tr>
<tr>
<td>/dev/ad0s1e</td>
<td>383M</td>
<td>82K</td>
<td>352M</td>
<td>0%</td>
<td>/config</td>
</tr>
<tr>
<td>procs</td>
<td>4.0K</td>
<td>4.0K</td>
<td>0B</td>
<td>100%</td>
<td>/proc</td>
</tr>
<tr>
<td>/dev/ad1s1f</td>
<td>52G</td>
<td>6.3G</td>
<td>41G</td>
<td>13%</td>
<td>/var</td>
</tr>
</tbody>
</table>
### Filesystem Utilization

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Capacity</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/ad0s1a</td>
<td>3.4G</td>
<td>178M</td>
<td>2.9G</td>
<td>6%</td>
<td>/</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev/</td>
</tr>
<tr>
<td>/dev/md0</td>
<td>33M</td>
<td>33M</td>
<td>0B</td>
<td>100%</td>
<td>/packages/mnt/jbase</td>
</tr>
<tr>
<td>/dev/md1</td>
<td>216M</td>
<td>216M</td>
<td>0B</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>/packages/mnt/jkernel-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md2</td>
<td>66M</td>
<td>66M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jpfe-T-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md3</td>
<td>4.1M</td>
<td>4.1M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jdocs-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md4</td>
<td>57M</td>
<td>57M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jroute-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md5</td>
<td>15M</td>
<td>15M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jcrypto-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md6</td>
<td>34M</td>
<td>34M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jpfe-common-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md7</td>
<td>2.0G</td>
<td>10.0K</td>
<td>1.8G</td>
<td>0%</td>
<td>/tmp</td>
</tr>
<tr>
<td>/dev/md8</td>
<td>2.0G</td>
<td>540K</td>
<td>1.8G</td>
<td>0%</td>
<td>/mfs</td>
</tr>
<tr>
<td>/dev/ad0s1e</td>
<td>383M</td>
<td>88K</td>
<td>352M</td>
<td>0%</td>
<td>/config</td>
</tr>
<tr>
<td>procfs</td>
<td>4.0K</td>
<td>4.0K</td>
<td>0B</td>
<td>100%</td>
<td>/proc</td>
</tr>
<tr>
<td>/dev/ad1s1f</td>
<td>23G</td>
<td>13G</td>
<td>7.7G</td>
<td>64%</td>
<td>/var</td>
</tr>
</tbody>
</table>

### Filesystem Utilization (Second Run)

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Capacity</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/ad0s1a</td>
<td>3.4G</td>
<td>178M</td>
<td>2.9G</td>
<td>6%</td>
<td>/</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev/</td>
</tr>
<tr>
<td>/dev/md0</td>
<td>33M</td>
<td>33M</td>
<td>0B</td>
<td>100%</td>
<td>/packages/mnt/jbase</td>
</tr>
<tr>
<td>/dev/md1</td>
<td>216M</td>
<td>216M</td>
<td>0B</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>/packages/mnt/jkernel-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md2</td>
<td>66M</td>
<td>66M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jpfe-T-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md3</td>
<td>4.1M</td>
<td>4.1M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jdocs-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md4</td>
<td>57M</td>
<td>57M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jroute-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md5</td>
<td>15M</td>
<td>15M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jcrypto-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md6</td>
<td>34M</td>
<td>34M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jpfe-common-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md7</td>
<td>2.0G</td>
<td>10.0K</td>
<td>1.8G</td>
<td>0%</td>
<td>/tmp</td>
</tr>
<tr>
<td>/dev/md8</td>
<td>2.0G</td>
<td>540K</td>
<td>1.8G</td>
<td>0%</td>
<td>/mfs</td>
</tr>
<tr>
<td>/dev/ad0s1e</td>
<td>383M</td>
<td>88K</td>
<td>352M</td>
<td>0%</td>
<td>/config</td>
</tr>
<tr>
<td>procfs</td>
<td>4.0K</td>
<td>4.0K</td>
<td>0B</td>
<td>100%</td>
<td>/proc</td>
</tr>
<tr>
<td>/dev/ad1s1f</td>
<td>23G</td>
<td>13G</td>
<td>7.7G</td>
<td>64%</td>
<td>/var</td>
</tr>
</tbody>
</table>

### Filesystem Utilization (Third Run)

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Size</th>
<th>Used</th>
<th>Avail</th>
<th>Capacity</th>
<th>Mounted on</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/ad0s1a</td>
<td>3.4G</td>
<td>178M</td>
<td>2.9G</td>
<td>6%</td>
<td>/</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>devfs</td>
<td>1.0K</td>
<td>1.0K</td>
<td>0B</td>
<td>100%</td>
<td>/dev/</td>
</tr>
<tr>
<td>/dev/md0</td>
<td>33M</td>
<td>33M</td>
<td>0B</td>
<td>100%</td>
<td>/packages/mnt/jbase</td>
</tr>
<tr>
<td>/dev/md1</td>
<td>216M</td>
<td>216M</td>
<td>0B</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>/packages/mnt/jkernel-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md2</td>
<td>66M</td>
<td>66M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jpfe-T-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md3</td>
<td>4.1M</td>
<td>4.1M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jdocs-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md4</td>
<td>57M</td>
<td>57M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jroute-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md5</td>
<td>15M</td>
<td>15M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jcrypto-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md6</td>
<td>34M</td>
<td>34M</td>
<td>0B</td>
<td>100%</td>
<td>/dev</td>
</tr>
<tr>
<td>/packages/mnt/jpfe-common-9.6-20090519.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>/dev/md7</td>
<td>2.0G</td>
<td>10.0K</td>
<td>1.8G</td>
<td>0%</td>
<td>/tmp</td>
</tr>
<tr>
<td>/dev/md8</td>
<td>2.0G</td>
<td>540K</td>
<td>1.8G</td>
<td>0%</td>
<td>/mfs</td>
</tr>
<tr>
<td>/dev/ad0s1e</td>
<td>383M</td>
<td>64K</td>
<td>352M</td>
<td>0%</td>
<td>/config</td>
</tr>
<tr>
<td>procfs</td>
<td>4.0K</td>
<td>4.0K</td>
<td>0B</td>
<td>100%</td>
<td>/proc</td>
</tr>
<tr>
<td>/dev/ad1s1f</td>
<td>23G</td>
<td>3.7G</td>
<td>17G</td>
<td>18%</td>
<td>/var</td>
</tr>
</tbody>
</table>
show system storage (QFX3500 Switch)

```
user@switch> show system storage
Filesystem  Size  Used  Avail  Capacity  Mounted on
/dev/da0s2a  343M  192M  123M   61%    /
/dev/md0   119M   119M   0B   100%  /packages/mnt/jbase
/dev/md1   513M   513M   0B   100%  /packages/mnt/jkernel-qfx-11.1R1.5
/packages/mnt/jkernel-qfx-11.1R1.5  37M   37M   0B   100%  /dev/md2
/packages/mnt/jpfe-qfx-e9xxx-11.1R1.5  6.0M   6.0M   0B   100%  /dev/md3
/packages/mnt/jdocs-qfx-11.1R1.5  216M  216M   0B   100%  /dev/md4
/packages/mnt/jroute-qfx-11.1R1.5  59M   59M   0B   100%  /dev/md5
/packages/mnt/jcrypto-qfx-11.1R1.5  85M   85M   0B   100%  /dev/md6
/packages/mnt/jswitch-qfx-11.1R1.5  63M   8.0K   58M    0%  /tmp
/dev/da0s2f  228M  14M  196M   7%    /var
/dev/da0s3d  590M   3.0M  540M    1%  /var/tmp
/dev/da0s3e  104M  162K  95M    0%  /config
procfs  4.0K   4.0K   0B   100%  /proc
```
show system switchover

Syntax

show system switchover
Syntax (TX Matrix Router)
<all-chassis | all-lcc | lcc number | scc>
Syntax (TX Matrix Plus Router)
show system switchover
<all-chassis | all-lcc | lcc number | sfc number>
Syntax (MX Series Router)
show system switchover
<all-members>
<local>
<member member-id>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.

Description
Display whether graceful Routing Engine switchover is configured, the state of the kernel replication (ready or synchronizing), any replication errors, and whether the primary and standby Routing Engines are using compatible versions of the kernel database.

NOTE: Issue the show system switchover command only on the backup Routing Engine. This command is not supported on the master Routing Engine because the kernel-replication process daemon does not run on the master Routing Engine. This process runs only on the backup Routing Engine.

Beginning Junos OS Release 9.6, the show system switchover command has been deprecated on the master Routing Engine on all routers other than a TX Matrix (switch-card chassis) or a TX Matrix Plus (switch-fabric chassis) router.

However, in a routing matrix, if you issue the show system switchover command on the master Routing Engine of the TX Matrix router (or switch-card chassis), the CLI displays graceful switchover information for the master Routing Engine of the T640 routers (or line-card chassis) in the routing matrix. Likewise, if you issue the show system switchover command on the master Routing Engine of a TX Matrix Plus router (or switch-fabric chassis), the CLI displays output for the master Routing Engine of T1600 or T4000 routers in the routing matrix.

Options

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display graceful Routing Engine switchover information for all Routing Engines on the TX Matrix router and the T640 routers configured in the routing matrix. On a TX Matrix Plus router, display graceful Routing Engine switchover information for all
Routing Engines on the TX Matrix Plus router and the T1600 or T4000 routers configured in the routing matrix.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display graceful Routing Engine switchover information for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, display graceful Routing Engine switchover information for all connected T1600 or T4000 LCCs.

Note that in this instance, packets get dropped. The LCCs perform GRES on their own chassis (GRES cannot be handled by one particular chassis for the entire router) and synchronization is not possible as the LCC plane bringup time varies for each LCC. Therefore, when there is traffic on these planes, there may be a traffic drop.

all-members—(MX Series routers only) (Optional) Display graceful Routing Engine switchover information for all Routing Engines on all members of the Virtual Chassis configuration.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display graceful Routing Engine switchover information for a specific T640 router connected to the TX Matrix router. On a TX Matrix Plus router, display graceful Routing Engine switchover information for a specific router connected to the TX Matrix Plus router.

Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers only) (Optional) Display graceful Routing Engines switchover information for all Routing Engines on the local Virtual Chassis member.

member member-id—(MX Series routers only) (Optional) Display graceful Routing Engine switchover information for all Routing Engines on the specified member of the Virtual Chassis configuration. Replace member-id with a value of 0 or 1.

scc—(TX Matrix router only) (Optional) Display graceful Routing Engine switchover information for the TX Matrix router (or switch-card chassis).

sfc—(TX Matrix Plus routers only) (Optional) Display graceful Routing Engine switchover information for the TX Matrix Plus router.

Additional Information If you issue the show system switchover command on a TX Matrix backup Routing Engine, the command is broadcast to all the T640 backup Routing Engines that are connected to it.
Likewise, if you issue the `show system switchover` command on a TX Matrix Plus backup Routing Engine, the command is broadcast to all the T1600 or T4000 backup Routing Engines that are connected to it.

If you issue the `show system switchover` command on the active Routing Engine in the master router of an MX Series Virtual Chassis, the router displays an error message that graceful Routing Engine switchover (GRES) is not enabled on this member.

### Required Privilege
- **view**

### Related Documentation
- `Routing Matrix with a TX Matrix Plus Router Solutions Page`

### List of Sample Output
- `show system switchover (Backup Routing Engine)` on page 295
- `show system switchover all-lcc (Routing Matrix)` on page 295

### Output Fields
Table 73 on page 294 describes the output fields for the `show system switchover` command. Output fields are listed in the approximate order in which they appear.

#### Table 73: show system switchover Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graceful switchover</strong></td>
<td>Display graceful Routing Engine switchover status:</td>
</tr>
<tr>
<td></td>
<td>- On—Indicates <code>graceful-switchover</code> is specified for the <code>routing-options</code> configuration command.</td>
</tr>
<tr>
<td></td>
<td>- Off—Indicates <code>graceful-switchover</code> is not specified for the <code>routing-options</code> configuration command.</td>
</tr>
<tr>
<td><strong>Configuration database</strong></td>
<td>State of the configuration database:</td>
</tr>
<tr>
<td></td>
<td>- Ready—Configuration database has synchronized.</td>
</tr>
<tr>
<td></td>
<td>- Synchronizing—Configuration database is synchronizing. Displayed when there are updates within the last 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>- Synchronize failed—Configuration database synchronize process failed.</td>
</tr>
<tr>
<td><strong>Kernel database</strong></td>
<td>State of the kernel database:</td>
</tr>
<tr>
<td></td>
<td>- Ready—Kernel database has synchronized.</td>
</tr>
<tr>
<td></td>
<td>- Synchronizing—Kernel database is synchronizing. Displayed when there are updates within the last 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>- Version incompatible—The primary and standby Routing Engines are running incompatible kernel database versions.</td>
</tr>
<tr>
<td></td>
<td>- Replication error—An error occurred when the state was replicated from the primary Routing Engine. Inspect <strong>Steady State</strong> for possible causes, or notify Juniper Networks customer support.</td>
</tr>
<tr>
<td><strong>Peer state</strong></td>
<td>Routing Engine peer state:</td>
</tr>
<tr>
<td></td>
<td>- Steady State—Peer completed switchover transition.</td>
</tr>
<tr>
<td></td>
<td>- Peer Connected—Peer in switchover transition.</td>
</tr>
</tbody>
</table>
Sample Output

show system switchover (Backup Routing Engine)

```
user@host> show system switchover
Graceful switchover: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
```

show system switchover all-lcc (Routing Matrix)

```
user@host> show system switchover all-lcc

lcc0-re0:
-------------------------------------------------------------------------
Multichassis replication: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
lcc2-re0:
-------------------------------------------------------------------------
Multichassis replication: On
Configuration database: Ready
Kernel database: Ready
Peer state: Steady State
```
show system uptime

Syntax

show system uptime

Syntax (EX Series Switches)

show system uptime
<all-members>
<local>
<member member-id>

Syntax (QFX Series)

show system uptime
<director-group name>
<infrastructure name>
<interconnect-device name>
<node-group name>

Syntax (TX Matrix Router)

show system uptime
<all-chassis | all-lcc | lcc number | scc>

Syntax (TX Matrix Plus Router)

show system uptime
<detail>
<all-chassis | all-lcc | lcc number | sfc number>

Syntax (MX Series Router)

show system uptime
<all-members>
<invoke-on>
<local>
<member member-id>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in JUNOS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display the current time and information about how long the router or switch, router or switch software, and routing protocols have been running.

Options

none—Show time since the system rebooted and processes started.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Show time since the system rebooted and processes started on all the routers in the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show time since the system rebooted and processes started for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, show time since the system rebooted and processes started for all connected T1600 or T4000 LCCs.

all-members—(EX4200 switches and MX Series routers only) (Optional) Show time since the system rebooted and processes started on all members of the Virtual Chassis configuration.
director-group name—(QFabric systems only) (Optional) Show time since the system rebooted and processes started on the Director group.

infrastructure name—(QFabric systems only) (Optional) Show time since the system rebooted and processes started on the fabric control Routing Engine and fabric manager Routing Engine.

interconnect-device name—(QFabric systems only) (Optional) Show time since the system rebooted and processes started on the Interconnect device.

invoke-on—(MX Series routers only) (Optional) Display the time since the system rebooted and processes started on the master Routing Engine, backup Routing Engine, or both, on a router with two Routing Engines.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show time since the system rebooted and processes started for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, show time since the system rebooted and processes started for a specific router that is connected to the TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Show time since the system rebooted and processes started on the local Virtual Chassis member.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Show time since the system rebooted and processes started on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

node-group name—(QFabric systems only) (Optional) Show time since the system rebooted and processes started on the Node group.

scc—(TX Matrix routers only) (Optional) Show time since the system rebooted and processes started for the TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus routers only) (Optional) Show time since the system rebooted and processes started for the TX Matrix Plus router. Replace number with 0.
**Additional Information**  
By default, when you issue the `show system uptime` command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

**Required Privilege Level**  
view

**Related Documentation**
- Monitoring System Process Information
- Monitoring System Properties
- 10-Gigabit Ethernet LAN/WAN PIC with XFP (T640 Router)
- Routing Matrix with a TX Matrix Plus Router Solutions Page

**List of Sample Output**
- show system uptime on page 298
- show system uptime all-lcc (TX Matrix Router) on page 299
- show system uptime all-lcc (TX Matrix Plus Router) on page 299
- show system uptime (QFX Series) on page 300

**Output Fields**
Table 74 on page 298 describes the output fields for the `show system uptime` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time</td>
<td>Current system time in UTC.</td>
</tr>
<tr>
<td>System booted</td>
<td>Date and time when the Routing Engine on the router or switch was last booted and how long it has been running.</td>
</tr>
<tr>
<td>Protocols started</td>
<td>Date and time when the routing protocols were last started and how long they have been running.</td>
</tr>
<tr>
<td>Last configured</td>
<td>Date and time when a configuration was last committed. Also shows the name of the user who issued the last <code>commit</code> command.</td>
</tr>
<tr>
<td>time and up</td>
<td>Current time, in the local time zone, and how long the router or switch has been operational.</td>
</tr>
<tr>
<td>users</td>
<td>Number of users logged in to the router or switch.</td>
</tr>
<tr>
<td>load averages</td>
<td>Load averages for the last 1 minute, 5 minutes, and 15 minutes.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show system uptime
user@host> show system uptime
```
show system uptime all-lcc (TX Matrix Router)

user@host> show system uptime all-lcc
lcc0-re0:
------------------------------------------------------------------------
Current time: 2004-09-13 09:55:35 PDT
Last configured: 2004-09-13 03:17:48 PDT (06:37:47 ago) by root
9:55AM PDT up 6:42, 1 user, load averages: 0.02, 0.03, 0.00
lcc2-re0:
------------------------------------------------------------------------
Current time: 2004-09-13 09:55:35 PDT
System booted: 2004-09-12 03:23:43 PDT (1d 06:31 ago)
Last configured: 2004-09-13 03:05:36 PDT (06:49:59 ago) by root
9:55AM PDT up 1 day, 6:32, 1 user, load averages: 0.02, 0.01, 0.00

show system uptime all-lcc (TX Matrix Plus Router)

user@host> show system uptime all-lcc
sfc0-re0:
------------------------------------------------------------------------
Current time: 2009-05-25 00:24:30 PDT
Protocols started: 2009-05-24 06:40:30 PDT (17:44:00 ago)
Last configured: 2009-05-24 06:33:27 PDT (17:51:03 ago) by gregdo
12:24AM up 17:45, 2 users, load averages: 0.07, 0.05, 0.01
lcc0-re0:
------------------------------------------------------------------------
Current time: 2009-05-25 00:24:30 PDT
error: the routing subsystem is not running
12:24AM up 17:45, 0 users, load averages: 0.00, 0.00, 0.00
lcc1-re0:
------------------------------------------------------------------------
Current time: 2009-05-25 00:24:30 PDT
error: the routing subsystem is not running
Last configured: 2009-05-24 06:40:18 PDT (17:44:12 ago) by root
12:24AM up 17:45, 0 users, load averages: 0.00, 0.00, 0.00
lcc2-re0:
------------------------------------------------------------------------
Current time: 2009-05-25 00:24:30 PDT
error: the routing subsystem is not running
12:24AM up 17:45, 0 users, load averages: 0.00, 0.00, 0.00
lcc3-re0:
------------------------------------------------------------------------
Current time: 2009-05-25 00:24:30 PDT
error: the routing subsystem is not running
show system uptime (QFX Series)

user@switch> show system uptime
Current time: 2010-08-27 03:12:30 PDT
System booted: 2010-08-13 17:11:54 PDT (1w6d 10:00 ago)
Protocols started: 2010-08-13 17:13:56 PDT (1w6d 09:58 ago)
Last configured: 2010-08-26 05:54:00 PDT (21:18:30 ago) by regress
3:12AM up 13 days, 10:01, 3 users, load averages: 0.00, 0.00, 0.00
show system users

Syntax

show system users
<no-resolve>

Syntax (TX Matrix Router)

show system users
<all-chassis | all-lcc | lcc number | scc>
<no-resolve>

Syntax (TX Matrix Plus Router)

show system users
<detail>
<all-chassis | all-lcc | lcc number | sfc number>
<no-resolve>

Syntax (MX Series Router)

show system users
<all-members>
<local>
<member member-id>
<no-resolve>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in JUNOS OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

List information about the users who are currently logged in to the router or switch.

NOTE: The show system users command lists the information about administrative users that are logged in to a router or switch using the CLI, J-Web, or an SSH client. The output does not list information about web users or automated users that are logged in from a remote client application using Junos XML APIs, such as NETCONF.

Options

none—List information about the users who are currently logged in to the router or switch.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Show users currently logged in to all the routers in the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to all connected T1600 or T4000 LCCs.

all-members—(MX Series routers only) (Optional) Display users currently logged in to all members of the Virtual Chassis configuration.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show users currently logged in to a specific T640 router that is
connected to the TX Matrix router. On a TX Matrix Plus router, show users currently logged in to a specific router that is connected to the TX Matrix Plus router. Replace `number` with the following values depending on the LCC configuration:

- **0 through 3**, when T640 routers are connected to a TX Matrix router in a routing matrix.
- **0 through 3**, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- **0 through 7**, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- **0, 2, 4, or 6**, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(MX Series routers only) (Optional) Display users currently logged in to the local Virtual Chassis member.

**member member-id**—(MX Series routers only) (Optional) Display users currently logged in to the specified member of the Virtual Chassis configuration. Replace `member-id` with a value of 0 or 1.

**no-resolve**—(Optional) Do not attempt to resolve IP addresses to hostnames.

**scc**—(TX Matrix routers only) (Optional) Show users currently logged in to the TX Matrix router (or switch-card chassis).

**sfc number**—(TX Matrix Plus routers only) (Optional) Show users currently logged in to the TX Matrix Plus router. Replace `number` with 0.

### Additional Information
By default, when you issue the `show system users` command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

### Required Privilege Level
`view`

### Related Documentation
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

### List of Sample Output
- `show system users` on page 303
- `show system users lcc no-resolve (TX Matrix, TX Matrix Plus Router)` on page 303
- `show system users (TX Matrix Plus Router)` on page 303
- `show system users (QFX Series)` on page 304
- `show system users no-resolve (QFX Series)` on page 304

### Output Fields
Table 75 on page 303 describes the output fields for the `show system users` command. Output fields are listed in the approximate order in which they appear.
### Table 75: show system users Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>time and up</strong></td>
<td>Current time, in the local time zone, and how long the router or switch has been operational.</td>
</tr>
<tr>
<td><strong>users</strong></td>
<td>Number of users logged in to the router or switch.</td>
</tr>
<tr>
<td><strong>load averages</strong></td>
<td>Load averages for the last 1 minute, 5 minutes, and 15 minutes.</td>
</tr>
<tr>
<td><strong>USER</strong></td>
<td>Username.</td>
</tr>
<tr>
<td><strong>TTY</strong></td>
<td>Terminal through which the user is logged in.</td>
</tr>
<tr>
<td><strong>FROM</strong></td>
<td>System from which the user has logged in. A hyphen indicates that the user is logged in through the console.</td>
</tr>
<tr>
<td><strong>LOGIN@</strong></td>
<td>Time when the user logged in.</td>
</tr>
<tr>
<td><strong>IDLE</strong></td>
<td>How long the user has been idle.</td>
</tr>
<tr>
<td><strong>WHAT</strong></td>
<td>Processes that the user is running.</td>
</tr>
</tbody>
</table>

### Sample Output

#### show system users

```bash
user@host> show system users
7:30PM up 4 days, 2:26, 2 users, load averages: 0.07, 0.02, 0.01
USER TTY FROM LOGIN@ IDLE WHAT
root d0 - Fri05PM 4days -csh (csh)
blue p0 level5.company.net 7:30PM - cli
```

#### show system users lcc no-resolve (TX Matrix, TX Matrix Plus Router)

```bash
user@host> show system users lcc 2 no-resolve
lcc2-re0:
----------------------------------------------------------------------------------------
10:34AM PDT up 1 day, 7:11, 5 users, load averages: 0.03, 0.01, 0.00
USER TTY FROM LOGIN@ IDLE WHAT
root d0 - 3:21AM 7:12 /bin/csh
regress p0 scc-re0 10:15AM - telnet hostA
regress p1 scc-re0 10:16AM - telnet hostA
regress p2 scc-re0 10:19AM - telnet hostA
regress p3 scc-re0 10:24AM - telnet hostA
```

#### show system users (TX Matrix Plus Router)

```bash
user@host> show system users
sfc0-re0:
----------------------------------------------------------------------------------------
1:41AM up 26 mins, 3 users, load averages: 0.08, 0.04, 0.03
USER TTY FROM LOGIN@ IDLE WHAT
regress p0 10.209.208.123 1:18AM 21 cli
regress p1 172.17.29.207 1:37AM 2 cli
```
regress p2       172.17.28.19                     1:40AM      - cli

lcc0-re0:
1:41AM  up 26 mins, 0 users, load averages: 0.00, 0.00, 0.03

lcc1-re0:
1:41AM  up 26 mins, 0 users, load averages: 0.00, 0.02, 0.03

lcc2-re0:
1:41AM  up 26 mins, 0 users, load averages: 0.16, 0.06, 0.02

lcc3-re0:
1:41AM  up 26 mins, 0 users, load averages: 0.12, 0.04, 0.04

regress@aj> show system users

sfc0-re0:
1:42AM  up 28 mins, 4 users, load averages: 0.02, 0.01, 0.03

USER     TTY      FROM                              LOGIN@  IDLE WHAT
regress  p0       pssraj-t61.jnpr.net              1:18AM     22 cli
regress  p1       eng-shell4.juniper.net           1:37AM      - cli
regress  p2       bigpink.juniper.net              1:40AM      - cli
regress  p3       sv-cuty-01.englab.juniper.net    1:42AM      - csh (csh)

lcc0-re0:
1:42AM  up 28 mins, 0 users, load averages: 0.02, 0.01, 0.03

lcc1-re0:
1:42AM  up 28 mins, 0 users, load averages: 0.07, 0.04, 0.03

lcc2-re0:
1:42AM  up 27 mins, 0 users, load averages: 0.07, 0.06, 0.02

lcc3-re0:
1:42AM  up 28 mins, 0 users, load averages: 0.05, 0.04, 0.04

show system users (QFX Series)

user@switch>  show system users

USER     TTY      FROM                              LOGIN@  IDLE WHAT
tlewis   p0       172.22.18.117                    2:54AM     39 -cli (cli)
tlewis   p1       172.22.18.117                    3:01AM      - cli (cli)
tcheng   p2       172.22.17.197                    3:08AM     11 -cli (cli)

show system users no-resolve (QFX Series)

user@switch>  show system users no-resolve

USER     TTY      FROM                              LOGIN@  IDLE WHAT
tlewis   p0       172.22.18.117                    2:54AM     39 -cli (cli)
tlewis   p1       172.22.18.117                    3:01AM      - cli (cli)
tcheng   p2       172.22.17.197                    3:08AM     11 -cli (cli)
show system virtual-memory

Syntax

**show system virtual-memory**

**Syntax (EX Series)**

**show system virtual-memory**

<all-members>
<local>
<member member-id>

**Syntax (TX Matrix Router)**

**show system virtual-memory**

<all-chassis | all-lcc | lcc number | scc>

**Syntax (TX Matrix Plus Router)**

**show system virtual-memory**

<all-chassis | all-lcc | lcc number | sfc number>

**Syntax (MX Series Router)**

**show system virtual-memory**

<all-members>
<local>
<member member-id>

**Syntax (QFX Series)**

**show system virtual-memory**

<infrastructure name>
<interconnect-device name>
<node-group name>

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display the usage of Junos OS kernel memory listed first by size of allocation and then by type of usage. Use the **show system virtual-memory** command for troubleshooting with Juniper Networks Customer Support.

**Options**

**none**—Display kernel dynamic memory usage information.

**all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display kernel dynamic memory usage information for all chassis.

**all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display kernel dynamic memory usage information for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display kernel dynamic memory usage information for all connected T1600 or T4000 LCCs.

**all-members**—(EX4200 switches and MX Series routers only) (Optional) Display kernel dynamic memory usage information for all members of the Virtual Chassis configuration.

**interconnect-device name**—(QFabric systems only) (Optional) Display kernel dynamic memory usage information for the Interconnect device.

**lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display kernel dynamic memory usage information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display kernel dynamic memory usage information for a specific router that is connected to the TX Matrix Plus router. Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(EX4200 switches and MX Series routers only) (Optional) Display kernel dynamic memory usage information for the local Virtual Chassis member.

**member member-id**—(EX4200 switches and MX Series routers only) (Optional) Display kernel dynamic memory usage information for the specified member of the Virtual Chassis configuration. For EX4200 switches, replace *member-id* with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

**node-group name**—(QFabric systems only) (Optional) Display kernel dynamic memory usage information for the Node group.

**scc**—(TX Matrix routers only) (Optional) Display kernel dynamic memory usage information for the TX Matrix router (or switch-card chassis).

**sfc number**—(TX Matrix Plus routers only) (Optional) Display kernel dynamic memory usage information for the TX Matrix Plus router. Replace *number* with 0.

**Additional Information** By default, when you issue the `show system virtual-memory` command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.
NOTE: The `show system virtual-memory` command with the `| display XML` pipe option now displays XML output for the command in the parent tags: `<vmstat-memstat-malloc>`, `<vmstat-memstat-zone>`, `<vmstat-sumstat>`, `<vmstat-intr>`, and `<vmstat-kernel-state>` with each child element as a separate XML tag. In Junos OS Releases 10.1 and earlier, the `| display XML` option for this command does not have an XML API element and the entire output is displayed in a single `<output>` tag element.

**Required Privilege Level**

- view

**Related Documentation**

- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

**List of Sample Output**

- `show system virtual-memory` on page 309
- `show system virtual-memory scc (TX Matrix Router)` on page 313
- `show system virtual-memory sfc (TX Matrix Plus Router)` on page 314
- `show system virtual-memory | display xml` on page 317
- `show system virtual-memory (QFX Series)` on page 340

**Output Fields**

Table 76 on page 308 lists the output fields for the `show system virtual-memory` command. Output fields are listed in the approximate order in which they appear.
Table 76: show system virtual-memory Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory statistics by bucket size</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>Memory block size (bytes). The kernel memory allocator appropriates blocks of memory whose size is exactly a power of 2.</td>
</tr>
<tr>
<td>In Use</td>
<td>Number of memory blocks of this size that are in use (bytes).</td>
</tr>
<tr>
<td>Free</td>
<td>Number of memory blocks of this size that are free (bytes).</td>
</tr>
<tr>
<td>Requests</td>
<td>Number of memory allocation requests made.</td>
</tr>
<tr>
<td>HighWater</td>
<td>Maximum value the free list can have. Once the system starts reclaiming physical memory, it continues until the free list is increased to this value.</td>
</tr>
<tr>
<td>Couldfree</td>
<td>Total number of times that the free elements for a bucket size exceed the high-water mark for that bucket size.</td>
</tr>
<tr>
<td>Memory usage type by bucket size</td>
<td></td>
</tr>
<tr>
<td>Size</td>
<td>Memory block size (bytes).</td>
</tr>
<tr>
<td>Type(s)</td>
<td>Kernel modules that are using these memory blocks. For a definition of each type, refer to a FreeBSD book.</td>
</tr>
<tr>
<td>Memory statistics by type</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Kernel module that is using dynamic memory.</td>
</tr>
<tr>
<td>InUse</td>
<td>Number of memory blocks used by this type. The number is rounded up.</td>
</tr>
<tr>
<td>MemUse</td>
<td>Amount of memory in use, in kilobytes (KB).</td>
</tr>
<tr>
<td>HighUse</td>
<td>Maximum memory ever used by this type.</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum memory that can be allocated to this type.</td>
</tr>
<tr>
<td>Requests</td>
<td>Total number of dynamic memory allocation requests this type has made.</td>
</tr>
<tr>
<td>Type Limit</td>
<td>Number of times requests were blocked for reaching the maximum limit.</td>
</tr>
<tr>
<td>Kern Limit</td>
<td>Number of times requests were blocked for the kernel map.</td>
</tr>
<tr>
<td>Size(s)</td>
<td>Memory block sizes this type is using.</td>
</tr>
<tr>
<td>Memory Totals</td>
<td></td>
</tr>
<tr>
<td>In Use</td>
<td>Total kernel dynamic memory in use (bytes, rounded up).</td>
</tr>
<tr>
<td>Free</td>
<td>Total kernel dynamic memory free (bytes, rounded up).</td>
</tr>
</tbody>
</table>
### Table 76: show system virtual-memory Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests</td>
<td>Total number of memory allocation requests.</td>
</tr>
<tr>
<td>ITEM</td>
<td>Kernel module that is using memory.</td>
</tr>
<tr>
<td>Size</td>
<td>Memory block size (bytes).</td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum memory that can be allocated to this type.</td>
</tr>
<tr>
<td>Used</td>
<td>Number of memory blocks used by this type. The number is rounded up.</td>
</tr>
<tr>
<td>Free</td>
<td>Number of memory blocks available to this type.</td>
</tr>
<tr>
<td>Requests</td>
<td>Total number of memory allocation requests this type has made.</td>
</tr>
<tr>
<td>interrupt</td>
<td>Timer events and scheduling interruptions.</td>
</tr>
<tr>
<td>total</td>
<td>Total number of interruptions for each type.</td>
</tr>
<tr>
<td>rate</td>
<td>Interruption rate.</td>
</tr>
<tr>
<td>Total</td>
<td>Total for all interruptions.</td>
</tr>
</tbody>
</table>

### Sample Output

```bash
user@host> show system virtual-memory
Memory statistics by bucket size
<table>
<thead>
<tr>
<th>Size</th>
<th>In Use</th>
<th>Free</th>
<th>Requests</th>
<th>HighWater</th>
<th>Couldfree</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>906</td>
<td>118</td>
<td>154876</td>
<td>1280</td>
<td>0</td>
</tr>
<tr>
<td>32</td>
<td>455</td>
<td>313</td>
<td>209956</td>
<td>640</td>
<td>0</td>
</tr>
<tr>
<td>64</td>
<td>4412</td>
<td>260</td>
<td>75380</td>
<td>320</td>
<td>20</td>
</tr>
<tr>
<td>128</td>
<td>3200</td>
<td>32</td>
<td>19361</td>
<td>160</td>
<td>81</td>
</tr>
<tr>
<td>256</td>
<td>1510</td>
<td>10</td>
<td>8844</td>
<td>80</td>
<td>4</td>
</tr>
<tr>
<td>512</td>
<td>446</td>
<td>2</td>
<td>5085</td>
<td>40</td>
<td>0</td>
</tr>
<tr>
<td>1K</td>
<td>18</td>
<td>2</td>
<td>5901</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>2K</td>
<td>1128</td>
<td>2</td>
<td>4445</td>
<td>10</td>
<td>1368</td>
</tr>
<tr>
<td>4K</td>
<td>185</td>
<td>1</td>
<td>456</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>8K</td>
<td>5</td>
<td>1</td>
<td>2653</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>16K</td>
<td>181</td>
<td>0</td>
<td>233</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>32K</td>
<td>2</td>
<td>0</td>
<td>1848</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>64K</td>
<td>20</td>
<td>0</td>
<td>22</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>128K</td>
<td>5</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>256K</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>512K</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Memory usage type by bucket size
<table>
<thead>
<tr>
<th>Size</th>
<th>Type(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>uc_devlist, nexusdev, iftable, temp, devbuf, atexit, COS, BPF, DEVFS mount, DEVFS node, vnodes, mount, pcb, soname, proc-args, kld, MD disk, rman, ATA generic, bus, sysctl, ippool, pfestat, ifstate,</td>
</tr>
</tbody>
</table>
```
### Memory statistics by type

<table>
<thead>
<tr>
<th>Type</th>
<th>InUse</th>
<th>MemUse</th>
<th>HighUse</th>
<th>Limit Requests</th>
<th>Limit Limit</th>
<th>Limit Limit</th>
<th>Size(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>isadev</td>
<td>13</td>
<td>1K</td>
<td>1K127753K</td>
<td>13 0 0</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>atkbdev</td>
<td>2</td>
<td>1K</td>
<td>1K127753K</td>
<td>2 0 0</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>uc_devlist</td>
<td>24</td>
<td>3K</td>
<td>3K127753K</td>
<td>24 0 0</td>
<td>16,2K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nexusdev</td>
<td>3</td>
<td>1K</td>
<td>1K127753K</td>
<td>3 0 0</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>memdesc</td>
<td>1</td>
<td>4K</td>
<td>4K127753K</td>
<td>1 0 0</td>
<td>4K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mbuf</td>
<td>1</td>
<td>152K</td>
<td>152K127753K</td>
<td>1 0 0</td>
<td>256K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iflogical</td>
<td>6</td>
<td>2K</td>
<td>2K127753K</td>
<td>6 0 0</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iftable</td>
<td>17</td>
<td>9K</td>
<td>9K127753K</td>
<td>18 0 0</td>
<td>16,64,256,1K,4K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZONE</td>
<td>15</td>
<td>2K</td>
<td>2K127753K</td>
<td>15 0 0</td>
<td>128</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM pgdata</td>
<td>1</td>
<td>64K</td>
<td>64K127753K</td>
<td>1 0 0</td>
<td>64K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UFS mount</td>
<td>12</td>
<td>26K</td>
<td>26K127753K</td>
<td>12 0 0</td>
<td>512,2K,4K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UFS ihash</td>
<td>1</td>
<td>128K</td>
<td>128K127753K</td>
<td>1 0 0</td>
<td>128K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFS node</td>
<td>6</td>
<td>2K</td>
<td>2K127753K</td>
<td>35 0 0</td>
<td>64,256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FFS node</td>
<td>906</td>
<td>227K</td>
<td>227K127753K</td>
<td>1352 0 0</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dirrem</td>
<td>0</td>
<td>0K</td>
<td>0K127753K</td>
<td>500 0 0</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mkdir</td>
<td>0</td>
<td>0K</td>
<td>0K127753K</td>
<td>38 0 0</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>diradd</td>
<td>0</td>
<td>0K</td>
<td>0K127753K</td>
<td>521 0 0</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>freefile</td>
<td>0</td>
<td>0K</td>
<td>0K127753K</td>
<td>374 0 0</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>freeblks</td>
<td>0</td>
<td>0K</td>
<td>0K8K127753K</td>
<td>219 0 0</td>
<td>128</td>
<td></td>
<td></td>
</tr>
<tr>
<td>freefrag</td>
<td>0</td>
<td>0K</td>
<td>0K127753K</td>
<td>193 0 0</td>
<td>32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>allocindir</td>
<td>0</td>
<td>0K</td>
<td>0K127753K</td>
<td>1518 0 0</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>indirdep</td>
<td>0</td>
<td>0K</td>
<td>0K17K127753K</td>
<td>76 0 0</td>
<td>32,32K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>allocdirect</td>
<td>0</td>
<td>0K</td>
<td>0K10K127753K</td>
<td>760 0 0</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bmsafemap</td>
<td>0</td>
<td>0K</td>
<td>0K1K127753K</td>
<td>72 0 0</td>
<td>32</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Memory Totals: In Use Free Requests
9311K 54K 489068

ITEM SIZE LIMIT USED FREE REQUESTS
PIPE: 192, 0, 4, 81, 4422
SWAPMETA: 160, 95814, 0, 0, 0
unpcb: 160, 0, 114, 36, 279
ripcb: 192, 25330, 5, 37, 5
syncache: 128, 15359, 0, 64, 5
tcpcb: 576, 25330, 23, 12, 32
udpcb: 192, 25330, 14, 28, 255
socket: 256, 25330, 246, 26, 819
KNOTE: 96, 0, 27, 57, 71
NFSNODE: 352, 0, 0, 0, 0
NFSMOUNT: 544, 0, 0, 0, 0
VNODE: 224, 0, 2778, 43, 2778
NAMEI: 1024, 0, 0, 8, 40725
VMSPACE: 192, 0, 57, 71, 3906
PROC: 448, 0, 73, 17, 3923
DP fakepg: 64, 0, 0, 0, 0
PV ENTRY: 28, 499566, 44530, 152053, 1525141
MAP ENTRY: 48, 0, 1439, 134, 351075
KMAP ENTRY: 48, 35645, 179, 119, 10904
MAP: 108, 0, 7, 3, 7
VM OBJECT: 92, 0, 2575, 109, 66912

792644 cpu context switches
9863474 device interrupts
286510 software interrupts
390851 traps
3596829 system calls
16 kernel threads created
3880 fork() calls
27 vfork() calls
0 rfork() calls
0 swap pager pageins
0 swap pager pages paged in
0 swap pager pageouts
0 swap pager pages paged out
380 vnode pager pageins
395 vnode pager pages paged in
122 vnode pager pageouts
1476 vnode pager pages paged out
  0 page daemon wakeups
  0 pages examined by the page daemon
  101 pages reactivated
161722 copy-on-write faults
  0 copy-on-write optimized faults
84623 zero fill pages zeroed
83063 zero fill pages prezeroed
  7 intransit blocking page faults
535606 total VM faults taken
  0 pages affected by kernel thread creation
238254 pages affected by fork()
  2535 pages affected by vfork()
  0 pages affected by rfork()
283379 pages freed
  0 pages freed by daemon
190091 pages freed by exiting processes
17458 pages active
29166 pages inactive
  0 pages in VM cache
10395 pages wired down
134610 pages free
  4096 bytes per page
183419 total name lookups
  cache hits (90% pos + 7% neg) system 0% per-directory
deletions 0%, falsehits 0%, toolong 0%

interrupt    total      rate
ata0 irq14    113338    3
mux irq7      727643   21
fxp1 irq10    1178671  34
sio0 irq4     833       0
clk irq0     3439769  99
rtc irq8     4403221 127
Total         9863475 286

Kernel direct memory map:
  4423  pages used
  4057340  pages maximum

Note: Kernel direct memory map only displays for 64 bit platform.

show system virtual-memory scc (TX Matrix Router)
user@host> show system virtual-memory scc

Memory statistics by bucket size

<table>
<thead>
<tr>
<th>Size</th>
<th>In Use</th>
<th>Free</th>
<th>Requests</th>
<th>HighWater</th>
<th>Couldfree</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>898</td>
<td>126</td>
<td>749493</td>
<td>1280</td>
<td>0</td>
</tr>
<tr>
<td>32</td>
<td>2018</td>
<td>1310</td>
<td>980643</td>
<td>640</td>
<td>632</td>
</tr>
<tr>
<td>64</td>
<td>3490</td>
<td>13342</td>
<td>935420</td>
<td>320</td>
<td>5365</td>
</tr>
</tbody>
</table>

Memory usage type by bucket size

<table>
<thead>
<tr>
<th>Size</th>
<th>Type(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>uc_devlist, COS, BPF, DEVFS mount, DEVFS node, vnodes, mount, pcb, soname, rman, bus, sysctl, ifstate, pfe_ipc, mkey, socket, rtable, ifmaddr, ipfw, rnode, iftable, temp, devbuf, atexit, proc-args, kld, MD disk</td>
</tr>
<tr>
<td>32</td>
<td>atkbddev, Gzip trees, dirrem, mkdir, diradd, freefile, freefrag, indirdep, bmsafemap, newblk, tseg_qent, COS, vnodes,</td>
</tr>
</tbody>
</table>
### Memory statistics by type

<table>
<thead>
<tr>
<th>Type</th>
<th>InUse</th>
<th>MemUse</th>
<th>HighUse</th>
<th>Limit</th>
<th>Requests</th>
<th>Limit</th>
<th>Limit</th>
<th>Size(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>isadev</td>
<td>12</td>
<td>1K</td>
<td>1K</td>
<td>166400K</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>64</td>
</tr>
<tr>
<td>atkbddev</td>
<td>2</td>
<td>1K</td>
<td>1K</td>
<td>166400K</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>uc_devlist</td>
<td>24</td>
<td>3K</td>
<td>3K</td>
<td>166400K</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>16,2K</td>
</tr>
</tbody>
</table>

### Memory Totals:  In Use    Free    Requests

- In Use: 6091K
- Free: 1554K
- Requests: 2897122

---

**show system virtual-memory sfc (TX Matrix Plus Router)**

```
user@host> show system virtual-memory sfc
sfc0-re0:

<table>
<thead>
<tr>
<th>Type</th>
<th>InUse</th>
<th>MemUse</th>
<th>HighUse</th>
<th>Requests</th>
<th>Size(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAM dev queue</td>
<td>1</td>
<td>1K</td>
<td>-</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>entropy</td>
<td>1024</td>
<td>64K</td>
<td>-</td>
<td>1024</td>
<td>64</td>
</tr>
<tr>
<td>linker</td>
<td>487</td>
<td>6272K</td>
<td>-</td>
<td>1163</td>
<td>16,32,64,4096,32768,131072</td>
</tr>
<tr>
<td>USB</td>
<td>127</td>
<td>6272K</td>
<td>-</td>
<td>127</td>
<td>16,32,64,128,256,1024,2048</td>
</tr>
<tr>
<td>lockf</td>
<td>46</td>
<td>98416</td>
<td>-</td>
<td>98416</td>
<td>64</td>
</tr>
<tr>
<td>USBdev</td>
<td>10</td>
<td>34</td>
<td>16,128,2048,16384</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ifstateSLLNode</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>1096</td>
<td>16</td>
</tr>
<tr>
<td>devbuf</td>
<td>21243</td>
<td>15683K</td>
<td>-</td>
<td>21810</td>
<td>16,32,64,256,1024,2048,4096,8192,16384,32768,65536,131072</td>
</tr>
<tr>
<td>ip6ndp</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>in6ifmulti</td>
<td>1</td>
<td>1K</td>
<td>-</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>in6grentry</td>
<td>1</td>
<td>1K</td>
<td>-</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>iflogical</td>
<td>20</td>
<td>5K</td>
<td>-</td>
<td>29</td>
<td>2048</td>
</tr>
<tr>
<td>iffamily</td>
<td>45</td>
<td>6K</td>
<td>-</td>
<td>69</td>
<td>32,1024,2048</td>
</tr>
<tr>
<td>rtnextthop</td>
<td>266</td>
<td>46K</td>
<td>-</td>
<td>608013</td>
<td>32,256,512,1024,2048,4096</td>
</tr>
<tr>
<td>metrics</td>
<td>31</td>
<td>4K</td>
<td>-</td>
<td>54</td>
<td>256</td>
</tr>
<tr>
<td>rnode</td>
<td>212</td>
<td>4K</td>
<td>-</td>
<td>607848</td>
<td>16,32</td>
</tr>
<tr>
<td>rcache</td>
<td>4</td>
<td>8K</td>
<td>-</td>
<td>4</td>
<td>65536</td>
</tr>
<tr>
<td>iflist</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>6</td>
<td>16,64</td>
</tr>
<tr>
<td>ifdevice</td>
<td>11</td>
<td>8K</td>
<td>-</td>
<td>17</td>
<td>16,32,768</td>
</tr>
<tr>
<td>ifstat</td>
<td>424</td>
<td>472K</td>
<td>-</td>
<td>427</td>
<td>512,16384,65536</td>
</tr>
<tr>
<td>ipfw</td>
<td>42</td>
<td>123K</td>
<td>-</td>
<td>145</td>
<td>23K</td>
</tr>
<tr>
<td>ip6ndp</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>in6ifmulti</td>
<td>1</td>
<td>1K</td>
<td>-</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>in6grentry</td>
<td>1</td>
<td>1K</td>
<td>-</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>iflogical</td>
<td>20</td>
<td>5K</td>
<td>-</td>
<td>29</td>
<td>2048</td>
</tr>
<tr>
<td>iffamily</td>
<td>45</td>
<td>6K</td>
<td>-</td>
<td>69</td>
<td>32,1024,2048</td>
</tr>
<tr>
<td>rtnextthop</td>
<td>266</td>
<td>46K</td>
<td>-</td>
<td>608013</td>
<td>32,256,512,1024,2048,4096</td>
</tr>
<tr>
<td>metrics</td>
<td>31</td>
<td>4K</td>
<td>-</td>
<td>54</td>
<td>256</td>
</tr>
<tr>
<td>rnode</td>
<td>212</td>
<td>4K</td>
<td>-</td>
<td>607848</td>
<td>16,32</td>
</tr>
<tr>
<td>rcache</td>
<td>4</td>
<td>8K</td>
<td>-</td>
<td>4</td>
<td>65536</td>
</tr>
<tr>
<td>iflist</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>6</td>
<td>16,64</td>
</tr>
<tr>
<td>ifdevice</td>
<td>11</td>
<td>8K</td>
<td>-</td>
<td>17</td>
<td>16,32,768</td>
</tr>
<tr>
<td>ifstat</td>
<td>424</td>
<td>472K</td>
<td>-</td>
<td>427</td>
<td>512,16384,65536</td>
</tr>
<tr>
<td>ipfw</td>
<td>42</td>
<td>123K</td>
<td>-</td>
<td>145</td>
<td>23K</td>
</tr>
<tr>
<td>ip6ndp</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>in6ifmulti</td>
<td>1</td>
<td>1K</td>
<td>-</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>in6grentry</td>
<td>1</td>
<td>1K</td>
<td>-</td>
<td>1</td>
<td>64</td>
</tr>
<tr>
<td>iflogical</td>
<td>20</td>
<td>5K</td>
<td>-</td>
<td>29</td>
<td>2048</td>
</tr>
<tr>
<td>iffamily</td>
<td>45</td>
<td>6K</td>
<td>-</td>
<td>69</td>
<td>32,1024,2048</td>
</tr>
<tr>
<td>rtnextthop</td>
<td>266</td>
<td>46K</td>
<td>-</td>
<td>608013</td>
<td>32,256,512,1024,2048,4096</td>
</tr>
<tr>
<td>metrics</td>
<td>31</td>
<td>4K</td>
<td>-</td>
<td>54</td>
<td>256</td>
</tr>
<tr>
<td>rnode</td>
<td>212</td>
<td>4K</td>
<td>-</td>
<td>607848</td>
<td>16,32</td>
</tr>
<tr>
<td>rcache</td>
<td>4</td>
<td>8K</td>
<td>-</td>
<td>4</td>
<td>65536</td>
</tr>
<tr>
<td>iflist</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>6</td>
<td>16,64</td>
</tr>
<tr>
<td>ifdevice</td>
<td>11</td>
<td>8K</td>
<td>-</td>
<td>17</td>
<td>16,32,768</td>
</tr>
<tr>
<td>ifstat</td>
<td>424</td>
<td>472K</td>
<td>-</td>
<td>427</td>
<td>512,16384,65536</td>
</tr>
<tr>
<td>ipfw</td>
<td>42</td>
<td>123K</td>
<td>-</td>
<td>145</td>
<td>23K</td>
</tr>
</tbody>
</table>

### show system virtual-memory sfc0

```bash
user@host> show system virtual-memory sfc 0
sfc0-re0:
```

---

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th></th>
<th>InUse</th>
<th>MemUse</th>
<th>HighUse</th>
<th>Requests</th>
<th>Size(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>jsr</td>
<td>2</td>
<td>1K</td>
<td>-</td>
<td>22</td>
<td>16</td>
</tr>
<tr>
<td>idl</td>
<td>1</td>
<td>4K</td>
<td>-</td>
<td>165</td>
<td></td>
</tr>
<tr>
<td>rtsmsg</td>
<td>0</td>
<td>OK</td>
<td>-</td>
<td>16</td>
<td>131072</td>
</tr>
<tr>
<td>module</td>
<td>250</td>
<td>16K</td>
<td>-</td>
<td>250</td>
<td>64,128</td>
</tr>
<tr>
<td>mtx_pool</td>
<td>1</td>
<td>8K</td>
<td>-</td>
<td>1</td>
<td>64,128</td>
</tr>
<tr>
<td>DEVFS3</td>
<td>113</td>
<td>13K</td>
<td>-</td>
<td>114</td>
<td>256</td>
</tr>
<tr>
<td>DEVFS1</td>
<td>106</td>
<td>24K</td>
<td>-</td>
<td>106</td>
<td>2048</td>
</tr>
<tr>
<td>pgrp</td>
<td>15</td>
<td>1K</td>
<td>-</td>
<td>8600</td>
<td>64</td>
</tr>
<tr>
<td>session</td>
<td>11</td>
<td>2K</td>
<td>-</td>
<td>2829</td>
<td>512</td>
</tr>
<tr>
<td>proc</td>
<td>2</td>
<td>1K</td>
<td>-</td>
<td>2</td>
<td>16384</td>
</tr>
<tr>
<td>subproc</td>
<td>296</td>
<td>572K</td>
<td>-</td>
<td>24689</td>
<td>2048,131072</td>
</tr>
<tr>
<td>cored</td>
<td>38</td>
<td>5K</td>
<td>-</td>
<td>619244</td>
<td>256</td>
</tr>
<tr>
<td>plimit</td>
<td>18</td>
<td>4K</td>
<td>-</td>
<td>21311</td>
<td>2048</td>
</tr>
<tr>
<td>uidinfo</td>
<td>3</td>
<td>1K</td>
<td>-</td>
<td>10</td>
<td>32,512</td>
</tr>
<tr>
<td>sysctloid</td>
<td>2701</td>
<td>64K</td>
<td>-</td>
<td>1024</td>
<td>64</td>
</tr>
<tr>
<td>linkr</td>
<td>487</td>
<td>6272K</td>
<td>-</td>
<td>1163</td>
<td>16,32,4096,32768,131072</td>
</tr>
<tr>
<td>USB</td>
<td>127</td>
<td>10K</td>
<td>-</td>
<td>127</td>
<td>16,32,64,128,256,1024,2048</td>
</tr>
<tr>
<td>lockf</td>
<td>23</td>
<td>2K</td>
<td>-</td>
<td>169585</td>
<td>64</td>
</tr>
<tr>
<td>USBdev</td>
<td>10</td>
<td>2K</td>
<td>-</td>
<td>34</td>
<td>16,128,2048,16384</td>
</tr>
<tr>
<td>I/O</td>
<td>5128</td>
<td>10760K</td>
<td>-</td>
<td>5310</td>
<td></td>
</tr>
<tr>
<td>devstat</td>
<td>8</td>
<td>17K</td>
<td>-</td>
<td>8</td>
<td>16,131072</td>
</tr>
<tr>
<td>eventhandler</td>
<td>46</td>
<td>2K</td>
<td>-</td>
<td>47</td>
<td>32,128</td>
</tr>
<tr>
<td>kobj</td>
<td>93</td>
<td>186K</td>
<td>-</td>
<td>111</td>
<td>65536</td>
</tr>
<tr>
<td>DEVFS</td>
<td>8</td>
<td>1K</td>
<td>-</td>
<td>9</td>
<td>16,64</td>
</tr>
<tr>
<td>rman</td>
<td>106</td>
<td>7K</td>
<td>-</td>
<td>490</td>
<td>16,32,64</td>
</tr>
<tr>
<td>sbuf</td>
<td>0</td>
<td>0K</td>
<td>-</td>
<td>28234</td>
<td>16,32,64,128,32768</td>
</tr>
</tbody>
</table>

...
### System Resource Usage

<table>
<thead>
<tr>
<th>Resource</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifstate</td>
<td>710270 42176K</td>
<td>- 9583703</td>
</tr>
<tr>
<td>16,32,64,128,256,512,1024,2048,8192,16384,32768</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>idxbucket</td>
<td>1 1K</td>
<td>- 1 16</td>
</tr>
<tr>
<td>itable16</td>
<td>5045 1245K</td>
<td>- 1825178 1024,4096</td>
</tr>
<tr>
<td>itable32</td>
<td>157 10K</td>
<td>- 157 64</td>
</tr>
<tr>
<td>itable64</td>
<td>2 1K</td>
<td>- 2 128</td>
</tr>
<tr>
<td>lr</td>
<td>1 1K</td>
<td>- 4 16384</td>
</tr>
<tr>
<td>pic</td>
<td>37 6K</td>
<td>- 37 64,16384</td>
</tr>
<tr>
<td>pfestat</td>
<td>0 0K</td>
<td>- 1682 32,64,128,256,131072</td>
</tr>
<tr>
<td>gencfg</td>
<td>1486 424K</td>
<td>- 2812 16,32,64,256,16384,32768,65536</td>
</tr>
<tr>
<td>jsr</td>
<td>0 0K</td>
<td>- 22 16</td>
</tr>
<tr>
<td>rtsmsg</td>
<td>0 0K</td>
<td>- 3 131072</td>
</tr>
<tr>
<td>module</td>
<td>250 16K</td>
<td>- 250 64,128</td>
</tr>
<tr>
<td>mtx_pool</td>
<td>1 8K</td>
<td>- 1 64,128</td>
</tr>
<tr>
<td>DEVFS3</td>
<td>108 12K</td>
<td>- 109 256</td>
</tr>
<tr>
<td>DEVFS1</td>
<td>101 23K</td>
<td>- 101 2048</td>
</tr>
<tr>
<td>pgrp</td>
<td>5 1K</td>
<td>- 917 64</td>
</tr>
<tr>
<td>session</td>
<td>5 1K</td>
<td>- 917 512</td>
</tr>
<tr>
<td>proc</td>
<td>2 1K</td>
<td>- 2 16384</td>
</tr>
<tr>
<td>subproc</td>
<td>217 441K</td>
<td>- 4867 2048,131072</td>
</tr>
<tr>
<td>cred</td>
<td>21 3K</td>
<td>- 48719 256</td>
</tr>
<tr>
<td>plimit</td>
<td>9 2K</td>
<td>- 5255 2048</td>
</tr>
<tr>
<td>uidinfo</td>
<td>2 1K</td>
<td>- 2 32,512</td>
</tr>
<tr>
<td>sysctloid</td>
<td>2786 85K</td>
<td>- 2786 16,32,64</td>
</tr>
<tr>
<td>sysctltmp</td>
<td>0 0K</td>
<td>- 1833 16,32,64,1024</td>
</tr>
<tr>
<td>umtx</td>
<td>126 8K</td>
<td>- 126 64</td>
</tr>
<tr>
<td>SWAP</td>
<td>2 277K</td>
<td>- 2 64</td>
</tr>
<tr>
<td>bus</td>
<td>780 125K</td>
<td>- 131072 16,32,64,128,32768</td>
</tr>
<tr>
<td>bus-sc</td>
<td>69 69K</td>
<td>- 1194</td>
</tr>
<tr>
<td>devstat</td>
<td>8 17K</td>
<td>- 8 16,131072</td>
</tr>
<tr>
<td>eventhandler</td>
<td>45 2K</td>
<td>- 46 32,128</td>
</tr>
<tr>
<td>kobj</td>
<td>93 186K</td>
<td>- 111 65536</td>
</tr>
<tr>
<td>DEVFS</td>
<td>8 1K</td>
<td>- 9 16,64</td>
</tr>
<tr>
<td>rman</td>
<td>94 6K</td>
<td>- 477 16,32,64</td>
</tr>
<tr>
<td>sbuf</td>
<td>0 0K</td>
<td>- 532 16,32,32768,131072</td>
</tr>
<tr>
<td>NULLFS hash</td>
<td>1 1K</td>
<td>- 1 64</td>
</tr>
<tr>
<td>taskqueue</td>
<td>5 1K</td>
<td>- 5 64</td>
</tr>
<tr>
<td>turnstiles</td>
<td>127 8K</td>
<td>- 127 64</td>
</tr>
<tr>
<td>Unitno</td>
<td>6 1K</td>
<td>- 44 16,64</td>
</tr>
<tr>
<td>iocltlops</td>
<td>0 0K</td>
<td>- 1771718 16,32,64,128,8192,16384,65536,131072</td>
</tr>
<tr>
<td>iov</td>
<td>0 0K</td>
<td>- 79425 16,32,64,256,512,1024,2048,131072</td>
</tr>
<tr>
<td>msg</td>
<td>4 25K</td>
<td>- 4 32768,131072</td>
</tr>
<tr>
<td>sem</td>
<td>4 7K</td>
<td>- 4 16384,32768,131072</td>
</tr>
<tr>
<td>shm</td>
<td>2 13K</td>
<td>- 4 32768</td>
</tr>
<tr>
<td>ttys</td>
<td>93 16K</td>
<td>- 195 512,32768</td>
</tr>
<tr>
<td>soname</td>
<td>31 3K</td>
<td>- 389284 16,32,64,256</td>
</tr>
<tr>
<td>pcb</td>
<td>101 16K</td>
<td>- 4374</td>
</tr>
<tr>
<td>16,32,64,128,1024,2048,8192,16384,65536,131072</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>BIO buffer</td>
<td>40 80K</td>
<td>- 750 65536</td>
</tr>
<tr>
<td>vfs cache</td>
<td>1 512K</td>
<td>- 1 65536</td>
</tr>
<tr>
<td>cluster_save buffer</td>
<td>0 0K</td>
<td>- 55 32,64</td>
</tr>
<tr>
<td>VFS hash</td>
<td>1 256K</td>
<td>- 1 32,64</td>
</tr>
<tr>
<td>vnodes</td>
<td>1 1K</td>
<td>- 1 512</td>
</tr>
<tr>
<td>mount</td>
<td>266 21K</td>
<td>- 481 16,32,64,128,256,4096,32768</td>
</tr>
<tr>
<td>vnodemarker</td>
<td>0 0K</td>
<td>- 2497 16384</td>
</tr>
<tr>
<td>pfs_nodes</td>
<td>25 3K</td>
<td>- 25 128</td>
</tr>
<tr>
<td>pfs_vncache</td>
<td>144 5K</td>
<td>- 386 32</td>
</tr>
<tr>
<td>STP</td>
<td>1 1K</td>
<td>- 1 64</td>
</tr>
</tbody>
</table>
### show system virtual-memory | display xml

```
user@host> show system virtual-memory | display xml
<rpc-reply xmlns:junos="http://xml.juniper.net/junos/10.2R1/junos">
  <system-virtual-memory-information>
    <memstat-name>CAM dev queue</memstat-name>
    <inuse>1</inuse>
    <num>317</num>
  </system-virtual-memory-information>
</rpc-reply>
```

---

### Chapter 5: Administration

<table>
<thead>
<tr>
<th>ITEM</th>
<th>SIZE</th>
<th>LIMIT</th>
<th>USED</th>
<th>FREE</th>
<th>REQUESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMA Kegs:</td>
<td>136</td>
<td>0</td>
<td>71</td>
<td>1</td>
<td>71</td>
</tr>
</tbody>
</table>

...
<memstat-size>64,2048</memstat-size>
<memstat-name>iffamily</memstat-name>
<inuse>28</inuse>
<memuse>4</memuse>
<high-use>--</high-use>
<memstat-req>28</memstat-req>
<memstat-size>32,1024,2048</memstat-size>
<memstat-name>rtnexthop</memstat-name>
<inuse>127</inuse>
<memuse>18</memuse>
<high-use>--</high-use>
<memstat-req>129</memstat-req>
<memstat-size>32,256,512,1024,2048,4096</memstat-size>
<memstat-name>metrics</memstat-name>
<inuse>3</inuse>
<memuse>1</memuse>
<high-use>--</high-use>
<memstat-req>5</memstat-req>
<memstat-size>256</memstat-size>
<memstat-name>inifmulti</memstat-name>
<inuse>3</inuse>
<memuse>1</memuse>
<high-use>--</high-use>
<memstat-req>3</memstat-req>
<memstat-size>64</memstat-size>
<memstat-name>ingrentry</memstat-name>
<inuse>6</inuse>
<memuse>1</memuse>
<high-use>--</high-use>
<memstat-req>6</memstat-req>
<memstat-size>64</memstat-size>
<memstat-name>rnode</memstat-name>
<inuse>68</inuse>
<memuse>2</memuse>
<high-use>--</high-use>
<memstat-req>76</memstat-req>
<memstat-size>16,32</memstat-size>
<memstat-name>rcache</memstat-name>
<inuse>4</inuse>
<memuse>8</memuse>
<high-use>--</high-use>
<memstat-req>4</memstat-req>
<memstat-size>65536</memstat-size>
<memstat-name>ifdevice</memstat-name>
<inuse>4</inuse>
<memuse>4</memuse>
<high-use>--</high-use>
<memstat-req>4</memstat-req>
<memstat-size>16</memstat-size>
<memstat-name>ifstat</memstat-name>
<inuse>40</inuse>
<memuse>22</memuse>
<high-use>--</high-use>
<memstat-req>40</memstat-req>
<memstat-size>512,16384,32768</memstat-size>
<memstat-name>ipfw</memstat-name>
<inuse>42</inuse>
<memuse>23</memuse>
<high-use>--</high-use>
<memstat-req>91</memstat-req>
<memstat-size>16,32,64,128,256,512,1024,16384,32768,65536,131072</memstat-size>
<memstat-name>ifmaddr</memstat-name>
<br>inuse>103</br><br>memuse>3</br><br>high-use>-</br><br>memstat-req>103</br><br>memstat-size>16,32</br><br>memstat-name>rtable</memstat-name>
<br>inuse>129</br><br>memuse>14</br><br>high-use>-</br><br>memstat-req>139</br><br>memstat-size>16,32,64,128,1024,16384</br><br>memstat-name>sysctl</memstat-name>
<br>inuse>0</br><br>memuse>0</br><br>high-use>-</br><br>memstat-req>14847</br><br>memstat-size>16,32,64,4096,16384,32768</br><br>memstat-name>ifaddr</memstat-name>
<br>inuse>29</br><br>memuse>3</br><br>high-use>-</br><br>memstat-req>29</br><br>memstat-size>64,128</br><br>memstat-name>mkey</memstat-name>
<br>inuse>345</br><br>memuse>6</br><br>high-use>-</br><br>memstat-req>2527</br><br>memstat-size>16,128</br><br>memstat-name>pfe_ipc</memstat-name>
<br>inuse>0</br><br>memuse>0</br><br>high-use>-</br><br>memstat-req>1422</br><br><memstat-size>16,32,64,128,512,1024,2048,8192,16384,32768,65536,131072</memstat-size>
<memstat-name>ifstate</memstat-name>
<br>inuse>594</br><br>memuse>31</br><br>high-use>-</br><br>memstat-req>655</br><br><memstat-size>16,32,64,128,256,1024,2048,4096,16384,32768</memstat-size>
<memstat-name>itable16</memstat-name>
<br>inuse>276</br><br>memuse>52</br><br>high-use>-</br><br>memstat-req>294</br><br>memstat-size>1024,4096</br><br>memstat-name>itable32</memstat-name>
<br>inuse>160</br><br>memuse>10</br><br>high-use>-</br><br>memstat-req>160</br><br>memstat-size>64</br><br>memstat-name>itable64</memstat-name>
<br>inuse>2</br><br>memuse>1
<table>
<thead>
<tr>
<th>Memstat Name</th>
<th>Memstat-req</th>
<th>Memstat-size</th>
<th>Memstat-name</th>
<th>Inuse</th>
<th>Memuse</th>
<th>High-use</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVFS1</td>
<td>117</td>
<td>256</td>
<td>DEVFS1</td>
<td>102</td>
<td>23</td>
<td>-</td>
</tr>
<tr>
<td>pgrp</td>
<td>109</td>
<td>2048</td>
<td>pgrp</td>
<td>12</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>session</td>
<td>212</td>
<td>64</td>
<td>session</td>
<td>8</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>proc</td>
<td>212</td>
<td>64</td>
<td>proc</td>
<td>2</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>subproc</td>
<td>212</td>
<td>16384</td>
<td>subproc</td>
<td>496</td>
<td>496</td>
<td>-</td>
</tr>
<tr>
<td>cred</td>
<td>1522</td>
<td>2048, 131072</td>
<td>cred</td>
<td>30</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>plimit</td>
<td>133</td>
<td>2048</td>
<td>plimit</td>
<td>17</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>uidinfo</td>
<td>6</td>
<td>32, 512</td>
<td>uidinfo</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>sysctloid</td>
<td>1117</td>
<td>32, 512</td>
<td>sysctloid</td>
<td>1117</td>
<td>34</td>
<td>-</td>
</tr>
<tr>
<td>sysctltmp</td>
<td>1117</td>
<td>16, 32, 64</td>
<td>sysctltmp</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>
<memstat-req>743</memstat-req>
<memstat-size>16,32,64,1024</memstat-size>
<memstat-name>umtx</memstat-name>
<inuse>144</inuse>
<memuse>9</memuse>
<high-use></high-use>
<memstat-req>144</memstat-req>
<memstat-size>64</memstat-size>
<memstat-name>SWAP</memstat-name>
<inuse>2</inuse>
<memuse>209</memuse>
<high-use></high-use>
<memstat-req>2</memstat-req>
<memstat-size>64</memstat-size>
<memstat-name>bus</memstat-name>
<inuse>496</inuse>
<memuse>55</memuse>
<high-use></high-use>
<memstat-req>1196</memstat-req>
<memstat-size>16,32,64,128,32768</memstat-size>
<memstat-name>bus-sc</memstat-name>
<inuse>23</inuse>
<memuse>33</memuse>
<high-use></high-use>
<memstat-req>335</memstat-req>
<memstat-size>16,32,128,512,1024,2048,8192,16384,65536,131072</memstat-size>
<memstat-name>devstat</memstat-name>
<inuse>10</inuse>
<memuse>21</memuse>
<high-use></high-use>
<memstat-req>10</memstat-req>
<memstat-size>16,131072</memstat-size>
<memstat-name>eventhandler</memstat-name>
<inuse>35</inuse>
<memuse>2</memuse>
<high-use></high-use>
<memstat-req>36</memstat-req>
<memstat-size>32,128</memstat-size>
<memstat-name>kobj</memstat-name>
<inuse>93</inuse>
<memuse>186</memuse>
<high-use></high-use>
<memstat-req>111</memstat-req>
<memstat-size>65536</memstat-size>
<memstat-name>DEVFS</memstat-name>
<inuse>8</inuse>
<memuse>1</memuse>
<high-use></high-use>
<memstat-req>9</memstat-req>
<memstat-size>16,64</memstat-size>
<memstat-name>rman</memstat-name>
<inuse>71</inuse>
<memuse>5</memuse>
<high-use></high-use>
<memstat-req>433</memstat-req>
<memstat-size>16,32,64</memstat-size>
<memstat-name>sbuf</memstat-name>
<inuse>0</inuse>
<memuse>0</memuse>
<high-use></high-use>
<memstat-size>16,32,64,128,256,4096,32768</memstat-size>
<memstat-name>vnodemarker</memstat-name>
<inuse>0</inuse>
<memuse>0</memuse>
<high-use>--</high-use>
<memstat-req>498</memstat-req>
<memstat-size>16384</memstat-size>
<memstat-name>pfs_nodes</memstat-name>
<inuse>25</inuse>
<memuse>3</memuse>
<high-use>--</high-use>
<memstat-req>25</memstat-req>
<memstat-size>128</memstat-size>
<memstat-name>pfs_vncache</memstat-name>
<inuse>27</inuse>
<memuse>1</memuse>
<high-use>--</high-use>
<memstat-req>1</memstat-req>
<memstat-size>64</memstat-size>
<memstat-name>STP</memstat-name>
<inuse>1</inuse>
<memuse>1</memuse>
<high-use>--</high-use>
<memstat-req>1</memstat-req>
<memstat-size>16,32,64,128,256,512,2048,16384,32768,131072</memstat-size>
<memstat-name>syncache</memstat-name>
<inuse>1</inuse>
<memuse>8</memuse>
<high-use>--</high-use>
<memstat-req>1</memstat-req>
<memstat-size>16,32,64,128,256,512,2048,16384,32768,131072</memstat-size>
<memstat-name>tlv_stat</memstat-name>
<inuse>0</inuse>
<memuse>0</memuse>
<high-use>--</high-use>
<memstat-req>8</memstat-req>
<memstat-size>16,32,64,128,256,512,2048,16384,32768,131072</memstat-size>
<memstat-name>NFS daemon</memstat-name>
<inuse>1</inuse>
<memuse>8</memuse>
<high-use>--</high-use>
<memstat-req>1</memstat-req>
<memstat-size>16,32,64,128,256,512,2048,16384,32768,131072</memstat-size>
<memstat-name>p1003.1b</memstat-name>
<inuse>1</inuse>
<memuse>1</memuse>
<high-use>--</high-use>
<memstat-req>1</memstat-req>
<memstat-size>16</memstat-size>
<memstat-name>MD disk</memstat-name>
<inuse>10</inuse>
<memstat-req name="bmsafemap">336</memstat-req>
<memstat-size name="bmsafemap">64,4096</memstat-size>
<memuse name="bmsafemap">0</memuse>

<memstat-req name="allocdirect">63</memstat-req>
<memstat-size name="allocdirect">64</memstat-size>
<memuse name="allocdirect">0</memuse>

<memstat-req name="indirdir">320</memstat-req>
<memstat-size name="indirdir">128</memstat-size>
<memuse name="indirdir">0</memuse>

<memstat-req name="allocindir">17</memstat-req>
<memstat-size name="allocindir">32</memstat-size>
<memuse name="allocindir">0</memuse>

<memstat-req name="freefrag">15</memstat-req>
<memstat-size name="freefrag">64</memstat-size>
<memuse name="freefrag">0</memuse>

<memstat-req name="freeblks">12</memstat-req>
<memstat-size name="freeblks">32</memstat-size>
<memuse name="freeblks">0</memuse>

<memstat-req name="freefile">40</memstat-req>
<memstat-size name="freefile">2048</memstat-size>
<memuse name="freefile">0</memuse>

<memstat-req name="diradd">101</memstat-req>
<memstat-size name="diradd">32</memstat-size>
<memuse name="diradd">0</memuse>

<memstat-req name="dirrem">465</memstat-req>
<memstat-size name="dirrem">64</memstat-size>
<memuse name="dirrem">0</memuse>
<table>
<thead>
<tr>
<th>Memstat-req</th>
<th>Memstat-size</th>
<th>Memstat-name</th>
<th>Inuse</th>
<th>Memuse</th>
<th>High-use</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>168</td>
<td>32</td>
<td>newdirblk</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>32</td>
<td>savedino</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>157</td>
<td>512</td>
<td>UFS mount</td>
<td>15</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4096, 16384, 32768, 65536</td>
<td>512</td>
<td>UMAHash</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1583</td>
<td>64</td>
<td>VM pgdata</td>
<td>2</td>
<td>65</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>32</td>
<td>kenv</td>
<td>24</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
<memstat-name>$PIR</memstat-name>
<inuse>4</inuse>
<memuse>1</memuse>
<high-use>-</high-use>
<memstat-req>4</memstat-req>
<memstat-size>32</memstat-size>
<memstat-name>KTRACE</memstat-name>
<inuse>100</inuse>
<memuse>10</memuse>
<high-use>-</high-use>
<memstat-req>100</memstat-req>
<memstat-size>128</memstat-size>
<memstat-name>kbdmux</memstat-name>
<inuse>5</inuse>
<memuse>9</memuse>
<high-use>-</high-use>
<memstat-req>5</memstat-req>
<memstat-size>128</memstat-size>
<memstat-name>UMA Kegs:</memstat-name>
<zone-size>136</zone-size>
<count-limit>0</count-limit>
<used>71</used>
<free>1</free>
<zone-req>71</zone-req>
<zone-name>UMA Zones:</zone-name>
<zone-size>120</zone-size>
<count-limit>0</count-limit>
<used>71</used>
<free>19</free>
<zone-req>71</zone-req>
<zone-name>UMA Slabs:</zone-name>
<zone-size>64</zone-size>
<count-limit>0</count-limit>
<used>490</used>
<free>41</free>
<zone-req>579</zone-req>
<zone-name>UMA RCntSlabs:</zone-name>
<zone-size>104</zone-size>
<count-limit>0</count-limit>
<used>276</used>
<free>20</free>
<zone-req>276</zone-req>
<zone-name>UMA Hash:</zone-name>
<zone-size>128</zone-size>
<count-limit>0</count-limit>
<used>4</used>
<free>26</free>
<zone-req>5</zone-req>
<zone-name>16 Bucket:</zone-name>
<zone-size>76</zone-size>
<count-limit>0</count-limit>
<used>30</used>
<free>20</free>
<zone-req>30</zone-req>
<zone-name>32 Bucket:</zone-name>
<zone-size>140</zone-size>
<count-limit>0</count-limit>
<used>33</used>
<free>23</free>
<zone-req>33</zone-req>
<zone-name>64 Bucket:</zone-name>
<zone-size>268</zone-size>
<count-limit>0</count-limit>
<used>33</used>
<free>9</free>
<zone-req>33</zone-req>
<zone-name>128 Bucket:</zone-name>
<zone-size>524</zone-size>
<count-limit>0</count-limit>
<used>49</used>
<free>0</free>
<zone-req>49</zone-req>
<zone-name>VM OBJECT:</zone-name>
<zone-size>128</zone-size>
<count-limit>0</count-limit>
<used>2111</used>
<free>79</free>
<zone-req>25214</zone-req>
<zone-name>MAP:</zone-name>
<zone-size>160</zone-size>
<count-limit>0</count-limit>
<used>7</used>
<free>41</free>
<zone-req>7</zone-req>
<zone-name>VM OBJECT:</zone-name>
<zone-size>68</zone-size>
<count-limit>33336</count-limit>
<used>19</used>
<free>149</free>
<zone-req>2397</zone-req>
<zone-name>MAP ENTRY:</zone-name>
<zone-size>68</zone-size>
<count-limit>0</count-limit>
<used>2031</used>
<free>153</free>
<zone-req>62417</zone-req>
<zone-name>PV ENTRY:</zone-name>
<zone-size>24</zone-size>
<count-limit>509095</count-limit>
<used>57177</used>
<free>6333</free>
<zone-req>1033683</zone-req>
<zone-name>DP fakepg:</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>mt_zone:</zone-name>
<zone-size>64</zone-size>
<count-limit>0</count-limit>
<used>238</used>
<free>57</free>
<zone-req>238</zone-req>
<zone-name>16:</zone-name>
<zone-size>16</zone-size>
<count-limit>0</count-limit>
<used>2114</used>
<free>119</free>
<zone-req>80515</zone-req>
<zone-name>32:</zone-name>
<zone-size>32</zone-size>
<count-limit>0</count-limit>
<used>1335</used>
<free>134</free>
<zone-req>10259</zone-req>
<zone-name>64:</zone-name>
<zone-size>64</zone-size>
<count-limit>0</count-limit>
<used>3529</used>
<free>129</free>
<zone-req>29110</zone-req>
<zone-name>96:</zone-name>
<zone-size>96</zone-size>
<count-limit>0</count-limit>
<used>2062</used>
<free>58</free>
<zone-req>4365</zone-req>
<zone-name>112:</zone-name>
<zone-size>112</zone-size>
<count-limit>0</count-limit>
<used>361</used>
<free>164</free>
<zone-req>24613</zone-req>
<zone-name>128:</zone-name>
<zone-size>128</zone-size>
<count-limit>0</count-limit>
<used>359</used>
<free>61</free>
<zone-req>942</zone-req>
<zone-name>160:</zone-name>
<zone-size>160</zone-size>
<count-limit>0</count-limit>
<used>364</used>
<free>44</free>
<zone-req>577</zone-req>
<zone-name>224:</zone-name>
<zone-size>224</zone-size>
<count-limit>0</count-limit>
<used>422</used>
<free>20</free>
<zone-req>1950</zone-req>
<zone-name>256:</zone-name>
<zone-size>256</zone-size>
<count-limit>0</count-limit>
<used>204</used>
<free>36</free>
<zone-req>1225</zone-req>
<zone-name>288:</zone-name>
<zone-size>288</zone-size>
<count-limit>0</count-limit>
<used>2</used>
<free>24</free>
<zone-req>10</zone-req>
<zone-name>512:</zone-name>
<zone-size>512</zone-size>
<count-limit>0</count-limit>
<used>49</used>
<free>7</free>
<zone-req>911</zone-req>
<zone-name>1024:</zone-name>
<zone-size>1024</zone-size>
<count-limit>0</count-limit>
<used>213</used>
<free>11</free>
<zone-req>1076</zone-req>
<zone-name>2048:</zone-name>
<zone-size>2048</zone-size>
<count-limit>0</count-limit>
<used>199</used>
<free>113</free>
<zone-req>640</zone-req>
<zone-name>4096:</zone-name>
<zone-size>4096</zone-size>
<count-limit>0</count-limit>
<used>144</used>
<free>7</free>
<zone-req>2249</zone-req>
<zone-name>Files:</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>665</used>
<free>77</free>
<zone-req>16457</zone-req>
<zone-name>MAC labels:</zone-name>
<zone-size>20</zone-size>
<count-limit>0</count-limit>
<used>3998</used>
<free>227</free>
<zone-req>22947</zone-req>
<zone-name>PROC:</zone-name>
<zone-size>544</zone-size>
<count-limit>0</count-limit>
<used>116</used>
<free>10</free>
<zone-req>1394</zone-req>
<zone-name>THREAD:</zone-name>
<zone-size>416</zone-size>
<count-limit>0</count-limit>
<used>127</used>
<free>17</free>
<zone-req>131</zone-req>
<zone-name>KSEGRP:</zone-name>
<zone-size>88</zone-size>
<count-limit>0</count-limit>
<used>127</used>
<free>73</free>
<zone-req>131</zone-req>
<zone-name>UPCALL:</zone-name>
<zone-size>44</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>SLEEPQUEUE:</zone-name>
<zone-size>32</zone-size>
<count-limit>0</count-limit>
<used>145</used>
<free>194</free>
<zone-req>145</zone-req>
<zone-name>VMSPACE:</zone-name>
<zone-size>268</zone-size>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>GENCFG::</zone-name>
<zone-size>72</zone-size>
<count-limit>1000004</count-limit>
<used>57</used>
<free>102</free>
<zone-req>57</zone-req>
<zone-name>VNODE::</zone-name>
<zone-size>292</zone-size>
<count-limit>0</count-limit>
<used>2718</used>
<free>25</free>
<zone-req>2922</zone-req>
<zone-name>VNODEPOLL::</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>S VFS Cache::</zone-name>
<zone-size>68</zone-size>
<count-limit>0</count-limit>
<used>2500</used>
<free>76</free>
<zone-req>3824</zone-req>
<zone-name>L VFS Cache::</zone-name>
<zone-size>291</zone-size>
<count-limit>0</count-limit>
<used>51</used>
<free>14</free>
<zone-req>63</zone-req>
<zone-name>NAMEI::</zone-name>
<zone-size>1024</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>8</free>
<zone-req>5330</zone-req>
<zone-name>NFSMOUNT::</zone-name>
<zone-size>480</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>NFSNODE::</zone-name>
<zone-size>460</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>PIPE::</zone-name>
<zone-size>404</zone-size>
<count-limit>0</count-limit>
<used>27</used>
<free>9</free>
<zone-req>717</zone-req>
<zone-name>KNOTE::</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>42</used>
<table>
<thead>
<tr>
<th>Zone</th>
<th>Requested</th>
<th>Size</th>
<th>Limit</th>
<th>Used</th>
<th>Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>socket</td>
<td>3311</td>
<td>412</td>
<td>25191</td>
<td>343</td>
<td>8</td>
</tr>
<tr>
<td>unpcb</td>
<td>2524</td>
<td>140</td>
<td>25200</td>
<td>170</td>
<td>26</td>
</tr>
<tr>
<td>ipq</td>
<td>2157</td>
<td>52</td>
<td>216</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ipq</td>
<td>2157</td>
<td>52</td>
<td>216</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>udpcb</td>
<td>32</td>
<td>232</td>
<td>25194</td>
<td>19</td>
<td>32</td>
</tr>
<tr>
<td>tcpcb</td>
<td>105</td>
<td>520</td>
<td>25193</td>
<td>40</td>
<td>16</td>
</tr>
<tr>
<td>tcpw</td>
<td>105</td>
<td>520</td>
<td>25193</td>
<td>40</td>
<td>16</td>
</tr>
<tr>
<td>tcpw</td>
<td>0</td>
<td>52</td>
<td>5092</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpw</td>
<td>0</td>
<td>52</td>
<td>5092</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpw</td>
<td>0</td>
<td>52</td>
<td>5092</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpw</td>
<td>0</td>
<td>52</td>
<td>5092</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpw</td>
<td>0</td>
<td>52</td>
<td>5092</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>syncache</td>
<td>55</td>
<td>128</td>
<td>15360</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>syncache</td>
<td>55</td>
<td>128</td>
<td>15360</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>syncache</td>
<td>55</td>
<td>128</td>
<td>15360</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>syncache</td>
<td>55</td>
<td>128</td>
<td>15360</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>syncache</td>
<td>55</td>
<td>128</td>
<td>15360</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>tcpress</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpress</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpress</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpress</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tcpress</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbpf</td>
<td>55</td>
<td>20</td>
<td>1690</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
<pages-affected-by-fork>95343</pages-affected-by-fork>
<pages-affected-by-vfork>3526</pages-affected-by-vfork>
<pages-affected-by-rfork>0</pages-affected-by-rfork>
<pages-freed>221502</pages-freed>
<pages-freed-by-deamon>0</pages-freed-by-deamon>
<pages-freed-by-exiting-proc>75630</pages-freed-by-exiting-proc>
<pages-active>45826</pages-active>
<pages-inactive>13227</pages-inactive>
<pages-in-vm-cache>49278</pages-in-vm-cache>
<pages-wired-down>10640</pages-wired-down>
<pages-free>70706</pages-free>
<bytes-per-page>4096</bytes-per-page>
<swap-pages-used>0</swap-pages-used>
<peak-swap-pages-used>0</peak-swap-pages-used>
<total-name-lookups>214496</total-name-lookups>
<positive-cache-hits>92</positive-cache-hits>
<negative-cache-hits>5</negative-cache-hits>
<pass2>0</pass2>
<cache-deletions>0</cache-deletions>
<cache-falsehits>0</cache-falsehits>
<toolong>0</toolong>
</vmstat-sumstat>
</vmstat-intr>
</vm-kernel-state>
</vm-directmm-size-information>
</system-virtual-memory-information>
</cli>
</rpc-reply>

Note: <kernel-direct-mm-size-information> only displays for 64 bit platform.
show system virtual-memory (QFX Series)

user@switch>  show system virtual-memory | display xml
<rpc-reply xmlns:junos="http://xml.juniper.net/junos/11.1R1/junos">
  <system-virtual-memory-information>
    <vmstat-memstat-malloc>
      <memstat-name>CAM dev queue</memstat-name>
      <inuse>1</inuse>
      <memuse>1</memuse>
      <high-use></high-use>
      <memstat-req>1</memstat-req>
      <memstat-size>64</memstat-size>
    </vmstat-memstat-malloc>
    <memstat-name>entropy</memstat-name>
    <inuse>1024</inuse>
    <memuse>64</memuse>
    <high-use></high-use>
    <memstat-req>1024</memstat-req>
    <memstat-size>64</memstat-size>
  </system-virtual-memory-information>
</rpc-reply>
<high-use>-</high-use>
<memstat-req>1</memstat-req>
<memstat-size>64</memstat-size>
<memstat-name>iflogical</memstat-name>
<inuse>13</inuse>
<memuse>3</memuse>
<high-use>-</high-use>
<memstat-req>13</memstat-req>
<memstat-size>64,2048</memstat-size>
<memstat-name>iffamily</memstat-name>
<inuse>28</inuse>
<memuse>4</memuse>
<high-use>-</high-use>
<memstat-req>28</memstat-req>
<memstat-size>32,1024,2048</memstat-size>
<memstat-name>rtnexthop</memstat-name>
<inuse>127</inuse>
<memuse>18</memuse>
<high-use>-</high-use>
<memstat-req>129</memstat-req>
<memstat-size>32,256,512,1024,2048,4096</memstat-size>
<memstat-name>metrics</memstat-name>
<inuse>3</inuse>
<memuse>1</memuse>
<high-use>-</high-use>
<memstat-req>3</memstat-req>
<memstat-size>256</memstat-size>
<memstat-name>infmulti</memstat-name>
<inuse>3</inuse>
<memuse>1</memuse>
<high-use>-</high-use>
<memstat-req>28</memstat-req>
<memstat-size>16,32</memstat-size>
<memstat-name>rnode</memstat-name>
<inuse>68</inuse>
<memuse>2</memuse>
<high-use>-</high-use>
<memstat-req>76</memstat-req>
<memstat-size>16,32</memstat-size>
<memstat-name>rcache</memstat-name>
<inuse>4</inuse>
<memuse>8</memuse>
<high-use>-</high-use>
<memstat-req>4</memstat-req>
<memstat-size>65536</memstat-size>
<memstat-name>ifdevice</memstat-name>
<inuse>4</inuse>
<memuse>1</memuse>
<high-use>-</high-use>
<memstat-req>4</memstat-req>
<memstat-size>16</memstat-size>
<memstat-name>ifstat</memstat-name>
<inuse>40</inuse>
<memuse>22</memuse>
<high-use>-</high-use>
<table>
<thead>
<tr>
<th>Name</th>
<th>Inuse</th>
<th>Memuse</th>
<th>Size</th>
<th>Memstat-req</th>
</tr>
</thead>
<tbody>
<tr>
<td>dirrem</td>
<td>0</td>
<td>0</td>
<td>32</td>
<td>136</td>
</tr>
<tr>
<td>newdirblk</td>
<td>0</td>
<td>0</td>
<td>32</td>
<td>168</td>
</tr>
<tr>
<td>savedino</td>
<td>0</td>
<td>0</td>
<td>32</td>
<td>1</td>
</tr>
<tr>
<td>UFS mount</td>
<td>15</td>
<td>36</td>
<td>512</td>
<td>157</td>
</tr>
<tr>
<td>ata_dma</td>
<td>2</td>
<td>1</td>
<td>2048,65536,131072</td>
<td>2048,65536,131072</td>
</tr>
<tr>
<td>file desc</td>
<td>141</td>
<td>32</td>
<td>256</td>
<td>4096,16384,32768,65536</td>
</tr>
<tr>
<td>sigio</td>
<td>1</td>
<td>1</td>
<td>64</td>
<td>4096,16384,32768,65536</td>
</tr>
<tr>
<td>VM pgdata</td>
<td>2</td>
<td>65</td>
<td>256</td>
<td>1583</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>High Use</th>
<th>Mem Stat Request</th>
<th>Mem Stat Size</th>
<th>Mem Stat Name</th>
<th>In Use</th>
<th>Mem Use</th>
<th>High Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>20</td>
<td>32</td>
<td>kenv</td>
<td>24</td>
<td>5</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>27</td>
<td>16,32,64,131072</td>
<td>atkbddev</td>
<td>2</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>2</td>
<td>32</td>
<td>kqueue</td>
<td>15</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>19</td>
<td>1024,4096,32768</td>
<td>proc-args</td>
<td>57</td>
<td>3</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>1001</td>
<td>16,32,64,128,256,512,1024</td>
<td>isadep</td>
<td>21</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>21</td>
<td>64</td>
<td>zombie</td>
<td>0</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>1278</td>
<td>128</td>
<td>ithread</td>
<td>69</td>
<td>3</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>69</td>
<td>16,64,256</td>
<td>legacydrv</td>
<td>4</td>
<td>4</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>4</td>
<td>16</td>
<td>memdesc</td>
<td>1</td>
<td>4</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>1278</td>
<td>131072</td>
<td>nexusdev</td>
<td>2</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>128</td>
<td>128</td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

---

352 Copyright © 2013, Juniper Networks, Inc.


<used>30</used>
<free>20</free>
<zone-req>30</zone-req>
<zone-name>32 Bucket:</zone-name>
<zone-size>140</zone-size>
<count-limit>0</count-limit>
<used>33</used>
<free>23</free>
<zone-req>33</zone-req>
<zone-name>64 Bucket:</zone-name>
<zone-size>268</zone-size>
<count-limit>0</count-limit>
<used>33</used>
<free>9</free>
<zone-req>33</zone-req>
<zone-name>128 Bucket:</zone-name>
<zone-size>524</zone-size>
<count-limit>0</count-limit>
<used>49</used>
<free>0</free>
<zone-req>49</zone-req>
<zone-name>VM OBJECT:</zone-name>
<zone-size>128</zone-size>
<count-limit>0</count-limit>
<used>2111</used>
<free>79</free>
<zone-req>25214</zone-req>
<zone-name>MAP:</zone-name>
<zone-size>160</zone-size>
<count-limit>0</count-limit>
<used>7</used>
<free>41</free>
<zone-req>7</zone-req>
<zone-name>KMAP_ENTRY:</zone-name>
<zone-size>68</zone-size>
<count-limit>35336</count-limit>
<used>19</used>
<free>149</free>
<zone-req>2397</zone-req>
<zone-name>MAP ENTRY:</zone-name>
<zone-size>68</zone-size>
<count-limit>0</count-limit>
<used>2031</used>
<free>153</free>
<zone-req>62417</zone-req>
<zone-name>PV ENTRY:</zone-name>
<zone-size>24</zone-size>
<count-limit>509095</count-limit>
<used>57177</used>
<free>6333</free>
<zone-req>1033683</zone-req>
<zone-name>OP fakepg:</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>mt_zone:</zone-name>
<zone-size>64</zone-size>
<count-limit>0</count-limit>
<used>238</used>
<free>57</free>  
<zone-req>238</zone-req>  
<zone-name>16:</zone-name>  
<zone-size>16</zone-size>  
<count-limit>0</count-limit>  
<used>2114</used>  
<free>119</free>  
<zone-req>80515</zone-req>  
<zone-name>32:</zone-name>  
<zone-size>32</zone-size>  
<count-limit>0</count-limit>  
<used>1335</used>  
<free>134</free>  
<zone-req>10259</zone-req>  
<zone-name>64:</zone-name>  
<zone-size>64</zone-size>  
<count-limit>0</count-limit>  
<used>3529</used>  
<free>129</free>  
<zone-req>29110</zone-req>  
<zone-name>96:</zone-name>  
<zone-size>96</zone-size>  
<count-limit>0</count-limit>  
<used>2062</used>  
<free>58</free>  
<zone-req>4365</zone-req>  
<zone-name>112:</zone-name>  
<zone-size>112</zone-size>  
<count-limit>0</count-limit>  
<used>361</used>  
<free>164</free>  
<zone-req>24613</zone-req>  
<zone-name>128:</zone-name>  
<zone-size>128</zone-size>  
<count-limit>0</count-limit>  
<used>359</used>  
<free>61</free>  
<zone-req>942</zone-req>  
<zone-name>160:</zone-name>  
<zone-size>160</zone-size>  
<count-limit>0</count-limit>  
<used>364</used>  
<free>44</free>  
<zone-req>577</zone-req>  
<zone-name>224:</zone-name>  
<zone-size>224</zone-size>  
<count-limit>0</count-limit>  
<used>422</used>  
<free>20</free>  
<zone-req>1950</zone-req>  
<zone-name>256:</zone-name>  
<zone-size>256</zone-size>  
<count-limit>0</count-limit>  
<used>204</used>  
<free>36</free>  
<zone-req>1225</zone-req>  
<zone-name>288:</zone-name>  
<zone-size>288</zone-size>  
<count-limit>0</count-limit>  
<used>2</used>  
<free>24</free>
<table>
<thead>
<tr>
<th>Zone Name</th>
<th>Size</th>
<th>Count Limit</th>
<th>Used</th>
<th>Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files</td>
<td>72</td>
<td>0</td>
<td>665</td>
<td>77</td>
</tr>
<tr>
<td>MAC labels</td>
<td>20</td>
<td>0</td>
<td>3998</td>
<td>77</td>
</tr>
<tr>
<td>PROC</td>
<td>544</td>
<td>0</td>
<td>116</td>
<td>116</td>
</tr>
<tr>
<td>THREAD</td>
<td>416</td>
<td>0</td>
<td>127</td>
<td>17</td>
</tr>
<tr>
<td>KSEGRP</td>
<td>88</td>
<td>0</td>
<td>127</td>
<td>73</td>
</tr>
<tr>
<td>UPCALL</td>
<td>44</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zone Name</td>
<td>Size</td>
<td>Count Limit</td>
<td>Used</td>
<td>Free</td>
</tr>
<tr>
<td>Zone Req 10</td>
<td>512</td>
<td>0</td>
<td>49</td>
<td>7</td>
</tr>
<tr>
<td>Zone Req 911</td>
<td>1024</td>
<td>0</td>
<td>213</td>
<td>11</td>
</tr>
<tr>
<td>Zone Req 1076</td>
<td>2048</td>
<td>0</td>
<td>199</td>
<td>11</td>
</tr>
<tr>
<td>Zone Req 640</td>
<td>4096</td>
<td>0</td>
<td>144</td>
<td>7</td>
</tr>
<tr>
<td>Zone Req 2249</td>
<td>Files</td>
<td>72</td>
<td>3998</td>
<td>77</td>
</tr>
<tr>
<td>Zone Req 1394</td>
<td>THREAD</td>
<td>416</td>
<td>127</td>
<td>17</td>
</tr>
<tr>
<td>Zone Req 131</td>
<td>KSEGRP</td>
<td>88</td>
<td>127</td>
<td>73</td>
</tr>
<tr>
<td>Zone Req 131</td>
<td>UPCALL</td>
<td>44</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Zone Req 0</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
<zone-name>SLEEPQUEUE:</zone-name>  
<zone-size>32</zone-size>  
<count-limit>0</count-limit>  
<used>145</used>  
<free>194</free>  
<zone-req>145</zone-req>  
<zone-name>VMSPACE:</zone-name>  
<zone-size>268</zone-size>  
<count-limit>0</count-limit>  
<used>57</used>  
<free>13</free>  
<zone-req>1335</zone-req>  
<zone-name>mbuf_packet:</zone-name>  
<zone-size>256</zone-size>  
<count-limit>180000</count-limit>  
<used>256</used>  
<free>128</free>  
<zone-req>49791</zone-req>  
<zone-name>mbuf:</zone-name>  
<zone-size>256</zone-size>  
<count-limit>180000</count-limit>  
<used>50</used>  
<free>466</free>  
<zone-req>105183</zone-req>  
<zone-name>mbuf_cluster:</zone-name>  
<zone-size>2048</zone-size>  
<count-limit>25190</count-limit>  
<used>387</used>  
<free>165</free>  
<zone-req>5976</zone-req>  
<zone-name>mbuf_jumbo_pagesize:</zone-name>  
<zone-size>4096</zone-size>  
<count-limit>0</count-limit>  
<used>0</used>  
<free>0</free>  
<zone-req>0</zone-req>  
<zone-name>mbuf_jumbo_9k:</zone-name>  
<zone-size>9216</zone-size>  
<count-limit>0</count-limit>  
<used>0</used>  
<free>0</free>  
<zone-req>0</zone-req>  
<zone-name>mbuf_jumbo_16k:</zone-name>  
<zone-size>16384</zone-size>  
<count-limit>0</count-limit>  
<used>0</used>  
<free>0</free>  
<zone-req>0</zone-req>  
<zone-name>ACL UMA zone:</zone-name>  
<zone-size>388</zone-size>  
<count-limit>0</count-limit>  
<used>0</used>  
<free>0</free>  
<zone-req>0</zone-req>  
<zone-name>g_bio:</zone-name>  
<zone-size>132</zone-size>  
<count-limit>0</count-limit>  
<used>0</used>  
<free>174</free>  
<zone-req>69750</zone-req>  
<zone-name>ata_request:</zone-name>
<zone-name>ata_composite:</zone-name>
<zone-size>192</zone-size>
<count-limit>1000004</count-limit>
<used>57</used>
<free>102</free>
<zone-name>GENCFG:</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-name>VNODE:</zone-name>
<zone-size>292</zone-size>
<count-limit>0</count-limit>
<used>2718</used>
<free>25</free>
<zone-name>VNODEPOLL:</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-name>S VFS Cache:</zone-name>
<zone-size>68</zone-size>
<count-limit>0</count-limit>
<used>2500</used>
<free>76</free>
<zone-name>L VFS Cache:</zone-name>
<zone-size>291</zone-size>
<count-limit>0</count-limit>
<used>51</used>
<free>14</free>
<zone-name>NAMEI:</zone-name>
<zone-size>1024</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>8</free>
<zone-name>NFSMOUNT:</zone-name>
<zone-size>480</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-name>NFSNODE:</zone-name>
<zone-size>460</zone-size>
<count-limit>0</count-limit>
<used>0</used>
<free>0</free>
<zone-name>PIPE:</zone-name>
<zone-size>404</zone-size>
<count-limit>0</count-limit>
<used>27</used>
<free>9</free>
<zone-req>717</zone-req>
<zone-name>knote:</zone-name>
<zone-size>72</zone-size>
<count-limit>0</count-limit>
<used>42</used>
<free>64</free>
<zone-req>3311</zone-req>
<zone-name>socket:</zone-name>
<zone-size>412</zone-size>
<count-limit>25191</count-limit>
<used>343</used>
<free>8</free>
<zone-req>2524</zone-req>
<zone-name>unpcb:</zone-name>
<zone-size>140</zone-size>
<count-limit>25200</count-limit>
<used>170</used>
<free>26</free>
<zone-req>2157</zone-req>
<zone-name>ipq:</zone-name>
<zone-size>52</zone-size>
<count-limit>216</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>udp:<zone-name>
<zone-size>232</zone-size>
<count-limit>25194</count-limit>
<used>19</used>
<free>32</free>
<zone-req>31</zone-req>
<zone-name>inpcb:</zone-name>
<zone-size>232</zone-size>
<count-limit>25194</count-limit>
<used>40</used>
<free>28</free>
<zone-req>105</zone-req>
<zone-name>tcpcb:</zone-name>
<zone-size>520</zone-size>
<count-limit>25193</count-limit>
<used>40</used>
<free>26</free>
<zone-req>105</zone-req>
<zone-name>tcptw:</zone-name>
<zone-size>56</zone-size>
<count-limit>5092</count-limit>
<used>0</used>
<free>0</free>
<zone-req>0</zone-req>
<zone-name>syncache:</zone-name>
<zone-size>128</zone-size>
<count-limit>15360</count-limit>
<used>0</used>
<free>60</free>
<zone-req>55</zone-req>
<zone-name>tcp:<zone-name>
<zone-size>20</zone-size>
<count-limit>1690</count-limit>
<used>0</used> <free>0</free> <zone-req>0</zone-req> <zone-name>sackhole:</zone-name> <zone-size>20</zone-size> <count-limit>0</count-limit> <used>0</used> <free>0</free> <zone-req>0</zone-req> <zone-name>ripcb:</zone-name> <zone-size>232</zone-size> <count-limit>25194</count-limit> <used>5</used> <free>29</free> <zone-req>5</zone-req> <zone-name>SWAPMETA:</zone-name> <zone-size>276</zone-size> <count-limit>94948</count-limit> <used>0</used> <free>0</free> <zone-req>0</zone-req> <zone-name>FFS inode:</zone-name> <zone-size>132</zone-size> <count-limit>0</count-limit> <used>1146</used> <free>72</free> <zone-req>1306</zone-req> <zone-name>FFS1 dinode:</zone-name> <zone-size>128</zone-size> <count-limit>0</count-limit> <used>1146</used> <free>24</free> <zone-req>1306</zone-req> <zone-name>FFS2 dinode:</zone-name> <zone-size>256</zone-size> <count-limit>0</count-limit> <used>0</used> <free>0</free> <zone-req>0</zone-req> <vmstat-memstat-zone> <vmstat-sumstat> <cpu-context-switch>934906</cpu-context-switch> <dev-intr>1707986</dev-intr> <soft-intr>33819</soft-intr> <traps>203604</traps> <sys-calls>1200636</sys-calls> <kernel-thrds>60</kernel-thrds> <fork-calls>1113</fork-calls> <vfork-calls>21</vfork-calls> <rfork-calls>0</rfork-calls> <swap-pageins>0</swap-pageins> <swap-pagedin>0</swap-pagedin> <swap-pageouts>0</swap-pageouts> <swap-pagedout>0</swap-pagedout> <vnode-pageins>23094</vnode-pageins> <vnode-pagedin>23119</vnode-pagedin> <vnode-pageouts>226</vnode-pageouts> <vnode-pagedout>3143</vnode-pagedout> <page-daemon-wakeup>0</page-daemon-wakeup> <page-daemon-examined-pages>0</page-daemon-examined-pages> <pages-reactivated>8821</pages-reactivated>
<copy-on-write-faults>48364</copy-on-write-faults>
<copy-on-write-optimized-faults>31</copy-on-write-optimized-faults>
<zero-fill-pages-prezeroed>70061</zero-fill-pages-prezeroed>
<transit-blocking-page-faults>85</transit-blocking-page-faults>
<total-vm-faults>191824</total-vm-faults>
<pages-affected-by-kernel-thrd-creat>0</pages-affected-by-kernel-thrd-creat>
<pages-affected-by-fork>95343</pages-affected-by-fork>
<pages-affected-by-vfork>3526</pages-affected-by-vfork>
<pages-affected-by-rfork>0</pages-affected-by-rfork>
<pages-freed>221502</pages-freed>
<pages-freed-by-deamon>0</pages-freed-by-deamon>
<pages-freed-by-exiting-proc>75630</pages-freed-by-exiting-proc>
<pages-active>45826</pages-active>
<pages-inactive>13227</pages-inactive>
<pages-in-vm-cache>49278</pages-in-vm-cache>
<pages-wired-down>10640</pages-wired-down>
<pages-free>70706</pages-free>
<bytes-per-page>4096</bytes-per-page>
<swap-pages-used>0</swap-pages-used>
<total-name-lookups>214496</total-name-lookups>
<positive-cache-hits>92</positive-cache-hits>
<negative-cache-hits>5</negative-cache-hits>
<pass2>0</pass2>
<cache-deletions>0</cache-deletions>
<cache-falsehits>0</cache-falsehits>
<toolong>0</toolong>

</vmstat-sumstat>
</vmstat-intr>

<intr-name>irq0: clk</intr-name>
<intr-cnt>1243455</intr-cnt>
<intr-rate>999</intr-rate>
<intr-name>irq4: sio0</intr-name>
<intr-cnt>1140</intr-cnt>
<intr-rate>0</intr-rate>
<intr-name>irq8: rtc</intr-name>
<intr-cnt>159164</intr-cnt>
<intr-rate>127</intr-rate>
<intr-name>irq9: cbb1 fxp0</intr-name>
<intr-cnt>28490</intr-cnt>
<intr-rate>22</intr-rate>
<intr-name>irq10: fxp1</intr-name>
<intr-cnt>20593</intr-cnt>
<intr-rate>16</intr-rate>
<intr-name>irq14: ata0</intr-name>
<intr-cnt>503</intr-cnt>
<intr-rate>4</intr-rate>
<intr-name>Total</intr-name>
<intr-cnt>1457873</intr-cnt>
<intr-rate>1171</intr-rate>

</vmstat-intr>

<vm-kmem-map-free>248524800</vm-kmem-map-free>
</vm-kernel-state>
</system-virtual-memory-information>
</cli>
**show task replication**

**Syntax**
show task replication

**Release Information**
Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Displays nonstop active routing (NSR) status. When you issue this command on the master Routing Engine, the status of nonstop active routing synchronization is also displayed.

**Options**
This command has no options.

**Required Privilege Level**
view

**List of Sample Output**
show task replication (Issued on the Master Routing Engine) on page 363
show task replication (Issued on the Backup Routing Engine) on page 364

**Output Fields**
Table 77 on page 363 lists the output fields for the show task replication command. Output fields are listed in the approximate order in which they appear.

**Table 77: show task replication Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful replication</td>
<td>Displays whether or not graceful Routing Engine switchover is configured. The status can be <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>RE mode</td>
<td>Displays the Routing Engine on which the command is issued: <strong>Master</strong>, <strong>Backup</strong>, or <strong>Not applicable</strong> (when the router has only one Routing Engine).</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocols that are supported by nonstop active routing.</td>
</tr>
<tr>
<td>Synchronization Status</td>
<td>Nonstop active routing synchronization status for the supported protocols. States are <strong>NotStarted</strong>, <strong>InProgress</strong>, and <strong>Complete</strong>.</td>
</tr>
</tbody>
</table>

**Sample Output**

show task replication (Issued on the Master Routing Engine)

```
user@host> show task replication
Stateful Replication: Enabled
RE mode: Master

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Synchronization Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>NotStarted</td>
</tr>
<tr>
<td>BGP</td>
<td>Complete</td>
</tr>
<tr>
<td>IS-IS</td>
<td>NotStarted</td>
</tr>
<tr>
<td>LDP</td>
<td>Complete</td>
</tr>
<tr>
<td>PIM</td>
<td>Complete</td>
</tr>
</tbody>
</table>
```
show task replication (Issued on the Backup Routing Engine)

user@host> show task replication
Stateful Replication: Enabled
RE mode: Backup
show version

Syntax

show version
<brief | detail>

Syntax (EX Series Switches)

show version
<all-members>
<brief | detail>
<local>
<member member-id>

Syntax (TX Matrix Router)

show version
<brief | detail>
<all-chassis | all-lcc | lcc number | scc>

Syntax (TX Matrix Plus Router)

show version
<all-chassis | all-lcc | lcc number | sfc number>
<brief | detail>

Syntax (MX Series Router)

show version
<brief | detail>
<all-members>
<local>
<member member-id>

Syntax (QFX Series)

show version
<brief | detail>
<component component-name | all>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display the hostname and version information about the software running on the router or switch.

Options

none—Display standard information about the hostname and version of the software running on the router or switch.

brief | detail—(Optional) Display the specified level of output.

all-members—(EX4200 switches and MX Series routers only) (Optional) Display standard information about the hostname and version of the software running on all members of the Virtual Chassis configuration.

component all—(QFabric systems only) (Optional) Display the host name and version information about the software running on all the components on the QFabric system.

component component-name—(QFabric systems only) (Optional) Display the host name and version information about the software running on a specific QFabric system component. Replace component-name with the name of the QFabric system.
component. The component-name can be the name of a diagnostics Routing Engine, Director group, fabric control Routing Engine, fabric manager Routing Engine, Interconnect device, or Node group.

**local**—(EX4200 switches and MX Series routers only) (Optional) Display standard information about the hostname and version of the software running on the local Virtual Chassis member.

**member member-id**—(EX4200 switches and MX Series routers only) (Optional) Display standard information about the hostname and version of the software running on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

**scc**—(TX Matrix routers only) (Optional) Display the hostname and version information about the software running on the TX Matrix router (or switch-card chassis).

**lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display the host name and version information about the software running on a specified T640 router (line-card chassis or LCC) that is connected to the TX Matrix router. On a TX Matrix Plus router, display the host name and version information about the software running for a specified T1600 or T4000 router (LCC) that is connected to the TX Matrix Plus router.

Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**sfc number**—(TX Matrix Plus routers only) (Optional) Display the hostname and version information about the software running on the TX Matrix Plus router (or switch-fabric chassis). Replace number with 0.

**Additional Information**

By default, when you issue the `show version` command on a TX Matrix or TX Matrix Plus master Routing Engine, the command is broadcast to all the T640 (in a routing matrix based on a TX Matrix router) or T1600 or T4000 (in a routing matrix based on a TX Matrix Plus router) master Routing Engines connected to it. Likewise, if you issue the same command on the TX Matrix or TX Matrix Plus backup Routing Engine, the command is broadcast to all the T640 (in a routing matrix based on a TX Matrix router) or T1600 or T4000 (in a routing matrix based on a TX Matrix Plus router) backup Routing Engines that are connected to it.
Required Privilege Level

List of Sample Output

show version on page 368
show version (TX Matrix Plus Router) on page 368
show version (TX Matrix Plus Router with 3D SIBs) on page 371
show version (MX Series Router) on page 374
show version (QFX3500 Switch) on page 374
show version (QFabric System) on page 375
show version component all (QFabric System) on page 375
Sample Output

show version

user@host> show version
Hostname: router1
Model: m20
JUNOS Base OS boot [7.2-20050312.0]
JUNOS Base OS Software Suite [7.2-20050312.0]
JUNOS Kernel Software Suite [7.2R1.7]
JUNOS Packet Forwarding Engine Support (M20/M40) [7.2R1.7]
JUNOS Routing Software Suite [7.2R1.7]
JUNOS Online Documentation [7.2R1.7]
JUNOS Crypto Software Suite [7.2R1.7]

{master}
user@host> show version psd 1
psd1-re0:
---------------------------------------------------------------------
Hostname: china
Model: t640
JUNOS Base OS boot [9.1I20080311_1959_builder]
JUNOS Base OS Software Suite [9.1-20080321.0]
JUNOS Kernel Software Suite [9.1-20080321.0]
JUNOS Crypto Software Suite [9.1-20080321.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [9.1-20080321.0]
JUNOS Packet Forwarding Engine Support (T-series) [9.1-20080321.0]
JUNOS Online Documentation [9.1-20080321.0]
JUNOS Routing Software Suite [9.1-20080321.0]
labpkg [7.0]

show version (TX Matrix Plus Router)

user@host> show version
sfc0-re0:
---------------------------------------------------------------------
Hostname: host
Model: txp
JUNOS Base OS boot [12.3-20121019.0]
JUNOS Base OS Software Suite [12.3-20121019.0]
JUNOS Kernel Software Suite [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (T-Series) [12.3-20121019.0]
JUNOS Online Documentation [12.3-20121019.0]
JUNOS Services AAACL Container package [12.3-20121019.0]
JUNOS Services Application Level Gateways [12.3-20121019.0]
JUNOS AppId Services [12.3-20121019.0]
JUNOS Border Gateway Function package [12.3-20121019.0]
JUNOS Services Captive Portal and Content Delivery Container package [12.3-20121019.0]
JUNOS Services HTTP Content Management package [12.3-20121019.0]
JUNOS IDP Services [12.3-20121019.0]
JUNOS Services LL-PDF Container package [12.3-20121019.0]
JUNOS Services NAT [12.3-20121019.0]
JUNOS Services PTSP Container package [12.3-20121019.0]
JUNOS Services RPM [12.3-20121019.0]
JUNOS Services Stateful Firewall [12.3-20121019.0]
JUNOS Voice Services Container package [12.3-20121019.0]
JUNOS Services Example Container package [12.3-20121019.0]
Chapter 5: Administration

JUNOS Services Crypto [12.3-20121019.0]
JUNOS Services SSL [12.3-20121019.0]
JUNOS Services IPSec [12.3-20121019.0]
JUNOS Runtime Software Suite [12.3-20121019.0]
JUNOS Routing Software Suite [12.3-20121019.0]

lcc0-re0:
-------------------------------------------------------------------------
Hostname: host1
Model: t1600
JUNOS Base OS boot [12.3-20121019.0]
JUNOS Base OS Software Suite [12.3-20121019.0]
JUNOS Kernel Software Suite [12.3-20121019.0]
JUNOS Crypto Software Suite [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (T-Series) [12.3-20121019.0]
JUNOS Online Documentation [12.3-20121019.0]
JUNOS Services AACL Container package [12.3-20121019.0]
JUNOS Services Application Level Gateways [12.3-20121019.0]
JUNOS AppId Services [12.3-20121019.0]
JUNOS Border Gateway Function package [12.3-20121019.0]
JUNOS Services Captive Portal and Content Delivery Container package [12.3-20121019.0]
JUNOS Services HTTP Content Management package [12.3-20121019.0]
JUNOS IDP Services [12.3-20121019.0]
JUNOS Services LL-PDF Container package [12.3-20121019.0]
JUNOS Services NAT [12.3-20121019.0]
JUNOS Services PTSP Container package [12.3-20121019.0]
JUNOS Services RPM [12.3-20121019.0]
JUNOS Services Stateful Firewall [12.3-20121019.0]
JUNOS Voice Services Container package [12.3-20121019.0]
JUNOS Services Example Container package [12.3-20121019.0]
JUNOS Services Crypto [12.3-20121019.0]
JUNOS Services SSL [12.3-20121019.0]
JUNOS Services IPSec [12.3-20121019.0]
JUNOS Runtime Software Suite [12.3-20121019.0]
JUNOS Routing Software Suite [12.3-20121019.0]

lcc1-re0:
-------------------------------------------------------------------------
Hostname: host2
Model: t1600
JUNOS Base OS boot [12.3-20121019.0]
JUNOS Base OS Software Suite [12.3-20121019.0]
JUNOS Kernel Software Suite [12.3-20121019.0]
JUNOS Crypto Software Suite [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (T-Series) [12.3-20121019.0]
JUNOS Online Documentation [12.3-20121019.0]
JUNOS Services AACL Container package [12.3-20121019.0]
JUNOS Services Application Level Gateways [12.3-20121019.0]
JUNOS AppId Services [12.3-20121019.0]
JUNOS Border Gateway Function package [12.3-20121019.0]
JUNOS Services Captive Portal and Content Delivery Container package [12.3-20121019.0]
JUNOS Services HTTP Content Management package [12.3-20121019.0]
JUNOS IDP Services [12.3-20121019.0]
JUNOS Services LL-PDF Container package [12.3-20121019.0]
JUNOS Services NAT [12.3-20121019.0]
JUNOS Services PTSP Container package [12.3-20121019.0]
JUNOS Services RPM [12.3-20121019.0]
JUNOS Services Stateful Firewall [12.3-20121019.0]
JUNOS Voice Services Container package [12.3-20121019.0]
JUNOS Services Example Container package [12.3-20121019.0]
JUNOS Services Crypto [12.3-20121019.0]
JUNOS Services SSL [12.3-20121019.0]
JUNOS Services IPSec [12.3-20121019.0]
JUNOS Runtime Software Suite [12.3-20121019.0]
JUNOS Routing Software Suite [12.3-20121019.0]
JUNOS Services Stateful Firewall [12.3-20121019.0]
JUNOS Voice Services Container package [12.3-20121019.0]
JUNOS Services Example Container package [12.3-20121019.0]
JUNOS Services Crypto [12.3-20121019.0]
JUNOS Services SSL [12.3-20121019.0]
JUNOS Services IPSec [12.3-20121019.0]
JUNOS Runtime Software Suite [12.3-20121019.0]
JUNOS Routing Software Suite [12.3-20121019.0]

lcc2-re0:

Hostname: host3
Model: t1600
JUNOS Base OS boot [12.3-20121019.0]
JUNOS Base OS Software Suite [12.3-20121019.0]
JUNOS Kernel Software Suite [12.3-20121019.0]
JUNOS Crypto Software Suite [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (T-Series) [12.3-20121019.0]
JUNOS Online Documentation [12.3-20121019.0]
JUNOS Services AACL Container package [12.3-20121019.0]
JUNOS Services Application Level Gateways [12.3-20121019.0]
JUNOS AppId Services [12.3-20121019.0]
JUNOS Border Gateway Function package [12.3-20121019.0]
JUNOS Services Captive Portal and Content Delivery Container package [12.3-20121019.0]
JUNOS Services HTTP Content Management package [12.3-20121019.0]
JUNOS IDP Services [12.3-20121019.0]
JUNOS Services LL-PDF Container package [12.3-20121019.0]
JUNOS Services NAT [12.3-20121019.0]
JUNOS Services PTSP Container package [12.3-20121019.0]
JUNOS Services RPM [12.3-20121019.0]
JUNOS Services Stateful Firewall [12.3-20121019.0]
JUNOS Voice Services Container package [12.3-20121019.0]
JUNOS Services Example Container package [12.3-20121019.0]
JUNOS Services Crypto [12.3-20121019.0]
JUNOS Services SSL [12.3-20121019.0]
JUNOS Services IPSec [12.3-20121019.0]
JUNOS Runtime Software Suite [12.3-20121019.0]
JUNOS Routing Software Suite [12.3-20121019.0]

lcc3-re0:

Hostname: host4
Model: t1600
JUNOS Base OS boot [12.3-20121019.0]
JUNOS Base OS Software Suite [12.3-20121019.0]
JUNOS Kernel Software Suite [12.3-20121019.0]
JUNOS Crypto Software Suite [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [12.3-20121019.0]
JUNOS Packet Forwarding Engine Support (T-Series) [12.3-20121019.0]
JUNOS Online Documentation [12.3-20121019.0]
JUNOS Services AACL Container package [12.3-20121019.0]
JUNOS Services Application Level Gateways [12.3-20121019.0]
JUNOS AppId Services [12.3-20121019.0]
JUNOS Border Gateway Function package [12.3-20121019.0]
JUNOS Services Captive Portal and Content Delivery Container package [12.3-20121019.0]
JUNOS Services HTTP Content Management package [12.3-20121019.0]
JUNOS IDP Services [12.3-20121019.0]
JUNOS Services LL-PDF Container package [12.3-20121019.0]
show version (TX Matrix Plus Router with 3D SIBs)

user@host> show version
sfc0-re0:

Hostname: sfc0
Model: txp
JUNOS Base OS boot [13.1-20130306.0]
JUNOS Base OS Software Suite [13.1-20130306.0]
JUNOS Kernel Software Suite [13.1-20130306.0]
JUNOS Crypto Software Suite [13.1-20130306.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [13.1-20130306.0]
JUNOS Packet Forwarding Engine Support (T-Series) [13.1-20130306.0]
JUNOS Online Documentation [13.1-20130306.0]
JUNOS Services AAA Container package [13.1-20130306.0]
JUNOS Services Application Level Gateways [13.1-20130306.0]
JUNOS AppId Services [13.1-20130306.0]
JUNOS Border Gateway Function package [13.1-20130306.0]
JUNOS Services Captive Portal and Content Delivery Container package [13.1-20130306.0]
JUNOS Services HTTP Content Management package [13.1-20130306.0]
JUNOS IDP Services [13.1-20130306.0]
JUNOS Services Jflow Container package [13.1-20130306.0]
JUNOS Services LL-PDF Container package [13.1-20130306.0]
JUNOS Services MobileNext Software package [13.1-20130306.0]
JUNOS Services Mobile Subscriber Service Container package [13.1-20130306.0]
JUNOS Services NAT [13.1-20130306.0]
JUNOS Services PTSP Container package [13.1-20130306.0]
JUNOS Services RPM [13.1-20130306.0]
JUNOS Services Stateful Firewall [13.1-20130306.0]
JUNOS Voice Services Container package [13.1-20130306.0]
JUNOS Services Example Container package [13.1-20130306.0]
JUNOS Services Crypto [13.1-20130306.0]
JUNOS Services SSL [13.1-20130306.0]
JUNOS Services IPSec [13.1-20130306.0]
JUNOS Runtime Software Suite [13.1-20130306.0]
JUNOS Routing Software Suite [13.1-20130306.0]

lcc0-re0:

Hostname: lcc0
Model: t4000
JUNOS Base OS boot [13.1-20130306.0]
JUNOS Base OS Software Suite [13.1-20130306.0]
JUNOS Kernel Software Suite [13.1-20130306.0]
JUNOS Crypto Software Suite [13.1-20130306.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [13.1-20130306.0]
JUNOS Packet Forwarding Engine Support (T-Series) [13.1-20130306.0]
JUNOS Online Documentation [13.1-20130306.0]
JUNOS Services AACL Container package [13.1-20130306.0]
JUNOS Services Application Level Gateways [13.1-20130306.0]
JUNOS AppId Services [13.1-20130306.0]
JUNOS Border Gateway Function package [13.1-20130306.0]
JUNOS Services Captive Portal and Content Delivery Container package [13.1-20130306.0]
JUNOS Services HTTP Content Management package [13.1-20130306.0]
JUNOS IDP Services [13.1-20130306.0]
JUNOS Services Jflow Container package [13.1-20130306.0]
JUNOS Services LL-PDF Container package [13.1-20130306.0]
JUNOS Services MobileNext Software package [13.1-20130306.0]
JUNOS Services Mobile Subscriber Service Container package [13.1-20130306.0]
JUNOS Services NAT [13.1-20130306.0]
JUNOS Services PTSP Container package [13.1-20130306.0]
JUNOS Services RPM [13.1-20130306.0]
JUNOS Services Stateful Firewall [13.1-20130306.0]
JUNOS Voice Services Container package [13.1-20130306.0]
JUNOS Services Example Container package [13.1-20130306.0]
JUNOS Services Crypto [13.1-20130306.0]
JUNOS Services SSL [13.1-20130306.0]
JUNOS Services IPSec [13.1-20130306.0]
JUNOS Runtime Software Suite [13.1-20130306.0]
JUNOS Routing Software Suite [13.1-20130306.0]

lcc2-re0:
---------------------------------------------------------------------------
Hostname: lcc2
Model: t4000
JUNOS Base OS boot [13.1-20130306.0]
JUNOS Base OS Software Suite [13.1-20130306.0]
JUNOS Kernel Software Suite [13.1-20130306.0]
JUNOS Crypto Software Suite [13.1-20130306.0]
JUNOS Packet Forwarding Engine Support (M/T Common) [13.1-20130306.0]
JUNOS Packet Forwarding Engine Support (T-Series) [13.1-20130306.0]
JUNOS Online Documentation [13.1-20130306.0]
JUNOS Services AACL Container package [13.1-20130306.0]
JUNOS Services Application Level Gateways [13.1-20130306.0]
JUNOS AppId Services [13.1-20130306.0]
JUNOS Border Gateway Function package [13.1-20130306.0]
JUNOS Services Captive Portal and Content Delivery Container package [13.1-20130306.0]
JUNOS Services HTTP Content Management package [13.1-20130306.0]
JUNOS IDP Services [13.1-20130306.0]
JUNOS Services Jflow Container package [13.1-20130306.0]
JUNOS Services LL-PDF Container package [13.1-20130306.0]
JUNOS Services MobileNext Software package [13.1-20130306.0]
JUNOS Services Mobile Subscriber Service Container package [13.1-20130306.0]
JUNOS Services NAT [13.1-20130306.0]
JUNOS Services PTSP Container package [13.1-20130306.0]
JUNOS Services RPM [13.1-20130306.0]
JUNOS Services Stateful Firewall [13.1-20130306.0]
JUNOS Voice Services Container package [13.1-20130306.0]
JUNOS Services Example Container package [13.1-20130306.0]
JUNOS Services Crypto [13.1-20130306.0]
JUNOS Services SSL [13.1-20130306.0]
JUNOS Services IPSec [13.1-20130306.0]
JUNOS Runtime Software Suite [13.1-20130306.0]
JUNOS Routing Software Suite [13.1-20130306.0]
show version (MX Series Router)

user@host5> show version
Hostname: host5
Model: mx80
JUNOS Base OS boot [11.3-20110717.0]
JUNOS Base OS Software Suite [11.3-20110717.0]
JUNOS Kernel Software Suite [11.3-20110717.0]
JUNOS Crypto Software Suite [11.3-20110717.0]
JUNOS Packet Forwarding Engine Support (MX80) [11.3-20110717.0]
JUNOS Online Documentation [11.3-20110717.0]
JUNOS Routing Software Suite [11.3-20110717.0]

show version (QFX3500 Switch)

user@switch> show version
Hostname: switch
Model: qfx_s3500
JUNOS Base OS boot [11.1R1]
JUNOS Base OS Software Suite [11.1R1]
JUNOS Kernel Software Suite [11.1R1]
JUNOS Crypto Software Suite [11.1R1]
JUNOS Online Documentation [11.1R1]
JUNOS Enterprise Software Suite [11.1R1]
JUNOS Packet Forwarding Engine Support (QFX) [11.1R1]
JUNOS Routing Software Suite [11.1R1]

show version (QFabric System)

user@qfabric> show version
Hostname: qfabric
Model: qfx3000-g
Serial Number: qfsn-0123456789
QFabric System ID: f158527a-f99e-11e0-9fbd-00e081c57cda
JUNOS Base Version [12.2I20111018_0215_dc-builder]

show version component all (QFabric System)

user@switch> show version component all
dg1:
   -
   Hostname: qfabric
   Model: qfx3100
   JUNOS Base Version [11.3R1.6]

dg0:
   -
   Hostname: qfabric
   Model: qfx3100
   JUNOS Base Version [11.3R1.6]

NW-NG-0:
   -
   Hostname: qfabric
   Model: qfx-jvre
   JUNOS Base OS boot [11.3R1.6]
   JUNOS Base OS Software Suite [11.3R1.6]
   JUNOS Kernel Software Suite [11.3R1.6]
   JUNOS Crypto Software Suite [11.3R1.6]
   JUNOS Online Documentation [11.3R1.6]
   JUNOS Enterprise Software Suite [11.3R1.6]
   JUNOS Packet Forwarding Engine Support (QFX RE) [11.3R1.6]
   JUNOS Routing Software Suite [11.3R1.6]

FC-0:
   -
   Hostname: qfabric
   Model: qfx-jvre
   JUNOS Base OS boot [11.3R1.6]
   JUNOS Base OS Software Suite [11.3R1.6]
   JUNOS Kernel Software Suite [11.3R1.6]
   JUNOS Crypto Software Suite [11.3R1.6]
   JUNOS Online Documentation [11.3R1.6]
   JUNOS Enterprise Software Suite [11.3R1.6]
   JUNOS Packet Forwarding Engine Support (QFX RE) [11.3R1.6]
   JUNOS Routing Software Suite [11.3R1.6]
FC-1:
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3R1.6]
JUNOS Base OS Software Suite [11.3R1.6]
JUNOS Kernel Software Suite [11.3R1.6]
JUNOS Crypto Software Suite [11.3R1.6]
JUNOS Online Documentation [11.3R1.6]
JUNOS Enterprise Software Suite [11.3R1.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3R1.6]
JUNOS Routing Software Suite [11.3R1.6]

DRE-0:
Hostname: dre-0
Model: qfx-jvre
JUNOS Base OS boot [11.3R1.6]
JUNOS Base OS Software Suite [11.3R1.6]
JUNOS Kernel Software Suite [11.3R1.6]
JUNOS Crypto Software Suite [11.3R1.6]
JUNOS Online Documentation [11.3R1.6]
JUNOS Enterprise Software Suite [11.3R1.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3R1.6]
JUNOS Routing Software Suite [11.3R1.6]

FM-0:
Hostname: qfabric
Model: qfx-jvre
JUNOS Base OS boot [11.3R1.6]
JUNOS Base OS Software Suite [11.3R1.6]
JUNOS Kernel Software Suite [11.3R1.6]
JUNOS Crypto Software Suite [11.3R1.6]
JUNOS Online Documentation [11.3R1.6]
JUNOS Enterprise Software Suite [11.3R1.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3R1.6]
JUNOS Routing Software Suite [11.3R1.6]

nodedevice1:
Hostname: qfabric
Model: QFX3500
JUNOS Base OS boot [11.3R1.6]
JUNOS Base OS Software Suite [11.3R1.6]
JUNOS Kernel Software Suite [11.3R1.6]
JUNOS Crypto Software Suite [11.3R1.6]
JUNOS Online Documentation [11.3R1.6]
JUNOS Enterprise Software Suite [11.3R1.6]
JUNOS Packet Forwarding Engine Support (QFX RE) [11.3R1.6]
JUNOS Routing Software Suite [11.3R1.6]

interconnectdevice1:
Hostname: qfabric
Model: QFX3108
JUNOS Base OS boot [11.3R1.6]
JUNOS Base OS Software Suite [11.3R1.6]
JUNOS Kernel Software Suite [11.3R1.6]
JUNOS Crypto Software Suite [11.3R1.6]
JUNOS Online Documentation [11.3R1.6]
JUNOS Enterprise Software Suite [11.3R1.6]
warning: from interconnectdevice0: Disconnected
show version fpc

Syntax

```
show version fpc
<slot-number>
```

Release Information
Command introduced in Junos OS Release 11.4 for EX Series switches.

Description
Display the version of Junos OS for EX Series switches loaded on the line cards in an EX8200 switch.

Options

- `none`—List the version of Junos OS for EX Series switches loaded on the line cards in the EX8200 switch.

- `<slot-number>`—(Optional) Display the version of Junos OS for EX Series switches loaded on the line card slot specified by the slot-number value.

Required Privilege

Level `view`

Related Documentation

- `show version` on page 365
- List of Sample Output
  - `show version fpc` on page 378
  - `show version fpc 5` on page 378

Sample Output

```
show version fpc

user@switch> show version fpc
fpc 0 :
JUNOS 11.4I JUNOS 11.4I #0: 2011-12-07 11:33:18 UTC dmadhuri@bng-junos-pool
40.juniper.net:/b/dmadhuri/nyse_0612/obj-powerpc/bsd/kernels/EX8200-LC/kernel
powerpc
fpc 4 :
JUNOS 11.4I JUNOS 11.4I #0: 2011-12-07 11:33:18 UTC dmadhuri@bng-junos-pool
40.juniper.net:/b/dmadhuri/nyse_0612/obj-powerpc/bsd/kernels/EX8200-LC/kernel
powerpc
fpc 5 :
JUNOS 11.4I JUNOS 11.4I #0: 2011-12-07 11:33:18 UTC dmadhuri@bng-junos-pool
40.juniper.net:/b/dmadhuri/nyse_0612/obj-powerpc/bsd/kernels/EX8200-LC/kernel
powerpc
fpc 7 :
JUNOS 11.4I JUNOS 11.4I #0: 2011-12-07 11:33:18 UTC dmadhuri@bng-junos-pool
40.juniper.net:/b/dmadhuri/nyse_0612/obj-powerpc/bsd/kernels/EX8200-LC/kernel
powerpc

show version fpc 5

user@switch> show version fpc 5
fpc 5 :
JUNOS 11.4I JUNOS 11.4I #0: 2011-12-07 11:33:18 UTC dmadhuri@bng-junos-pool
40.juniper.net:/b/dmadhuri/nyse_0612/obj-powerpc/bsd/kernels/EX8200-LC/kernel
powerpc
```
Troubleshooting Procedures

Troubleshooting Loss of the Root Password

Problem
If you forget the root password for the switch, you can use the password recovery procedure to reset the root password.

NOTE: You need physical access to the switch to recover the root password.

Solution
To recover the root password:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.
2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port on the back of the switch. See Figure 1 on page 379.

Figure 1: Connecting to the Console Port on the EX Series Switch

3. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
4. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.

6. When the following prompt appears, press the Spacebar to access the switch’s bootstrap loader command prompt:
   
   Hit [Enter] to boot immediately, or space bar for command prompt.
   Booting [kernel] in 1 second...

7. At the following prompt, type `boot -s` to start up the system in single-user mode:
   
   `loader> boot -s`

8. At the following prompt, type `recovery` to start the root password recovery procedure:
   
   `Enter full path name of shell or 'recovery' for root password recovery or RETURN for /bin/sh: recovery`
   
   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

9. Enter configuration mode in the CLI:
   
   `user@switch> configure`

10. Set the root password. For example:
    
    `user@switch# set system root-authentication plain-text-password`

11. At the following prompt, enter the new root password. For example:
    
    `New password: juniper!`
    
    Retype new password:

12. At the second prompt, reenter the new root password.

13. If you are finished configuring the network, commit the configuration.
    
    `root@switch# commit`
    
    commit complete

14. Exit configuration mode in the CLI.
    
    `root@switch# exit`

15. Exit operational mode in the CLI.
    
    `root@switch> exit`

16. At the prompt, enter y to reboot the switch.
    
    `Reboot the system? [y/n] y`

---

**Related Documentation**

- Connecting and Configuring an EX Series Switch (CLI Procedure)
• **Connecting and Configuring an EX Series Switch (J-Web Procedure)**

• For information about configuring an encrypted root password, configuring SSH keys to authenticate root logins, and configuring special requirements for plain-text passwords, see the *Junos OS System Basics Configuration Guide*. 
PART 4

User Interfaces

- Overview on page 385
- Configuration on page 395
- Administration on page 399
CHAPTER 7

Overview

- Software Overview on page 385
- User Interfaces on page 387

Software Overview

- Understanding Software Infrastructure and Processes on page 385

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 385
- Junos OS Processes on page 386

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.

- Routing Engine—Provides three main functions:
  - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network.
- Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

**Junos OS Processes**

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 61 on page 112 describes the primary Junos OS processes.

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis process</td>
<td>chassisd</td>
<td>Detects hardware on the system that is used to configure network interfaces. Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered. Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</td>
</tr>
<tr>
<td>Ethernet switching process</td>
<td>eswd</td>
<td>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces. Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>Forwarding process</td>
<td>pfem</td>
<td>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</td>
</tr>
<tr>
<td>Interface process</td>
<td>dcd</td>
<td>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</td>
</tr>
<tr>
<td>Management process</td>
<td>mgd</td>
<td>Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the switch. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</td>
</tr>
<tr>
<td>Routing protocol process</td>
<td>rpd</td>
<td>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</td>
</tr>
</tbody>
</table>
User Interfaces

You can use two interfaces to monitor, configure, troubleshoot, and manage a Juniper Networks EX Series Ethernet Switch: the J-Web graphical user interface and the Junos operating system (Junos OS) command-line interface (CLI). Both of these user interfaces are shipped with the switch. This topic describes the CLI. For information about the J-Web user interface, see “J-Web User Interface for EX Series Switches Overview” on page 389.

CLI Overview

Junos operating system (Junos OS) CLI is a Juniper Networks specific command shell that runs on top of a UNIX-based operating system kernel. The CLI provides command help and command completion.

The CLI also provides a variety of UNIX utilities, such as Emacs-style keyboard sequences that allow you to move around on a command line and scroll through recently executed commands, regular expression matching to locate and replace values and identifiers in a configuration, filter command output, or log file entries, store and archive router files on a UNIX-based file system, and exit from the CLI environment and create a UNIX C shell or Bourne shell to navigate the file system, manage switch processes, and so on.

CLI Help and Command Completion

To access CLI Help, type a question mark (?) at any level of the hierarchy. The system displays a list of the available commands or statements and a short description of each.

To complete a command, statement, or option that you have partially typed, press the Tab key or the Spacebar. If the partially typed letters uniquely identify a command, the complete command name appears. Otherwise, a beep indicates that you have entered an ambiguous command and the possible completions are displayed. This completion feature also applies to other strings, such as filenames, interface names, usernames, and configuration statements.
The CLI has two modes, operational mode and configuration mode.

In operational mode, you enter commands to monitor and troubleshoot switch hardware and software and network connectivity. Operational mode is indicated by the > prompt—for example, user@switch>.

In configuration mode, you can define all properties of the Juniper Networks Junos operating system (Junos OS), including interfaces, VLANs, Virtual Chassis information, routing protocols, user access, and several system hardware properties.

To enter configuration mode, enter the configure command: .

user@switch> configure

Configuration mode is indicated by the # prompt, and includes the current location in the configuration hierarchy—for example:

[edit interfaces ge-0/0/12]
user@switch#

In configuration mode, you are actually viewing and changing the candidate configuration file. The candidate configuration allows you to make configuration changes without causing operational changes to the current operating configuration, called the active configuration. When you commit the changes you added to the candidate configuration, the system updates the active configuration. Candidate configurations enable you to alter your configuration without causing potential damage to your current network operations.

To activate your configuration changes, enter the commit command.

To return to operational mode, go to the top of the configuration hierarchy and then quit—for example:

[edit interfaces ge-0/0/12]
user@switch# top
[edit]
user@switch# exit

You can also activate your configuration changes and exit configuration mode with a single command, commit and-quit. This command succeeds only if there are no mistakes or syntax errors in the configuration.

TIP: When you commit the candidate configuration, you can require an explicit confirmation for the commit to become permanent by using the commit confirmed command. This is useful for verifying that a configuration change works correctly and does not prevent management access to the switch. After you issue the commit confirmed command, you must issue another commit command within the defined period of time (10 minutes by default) or the system reverts to the previous configuration.
Related Documentation

- EX Series Switch Software Features Overview on page 27
- Junos OS CLI User Guide

EX Series Switches Hardware and CLI Terminology Mapping

The terms used to describe hardware components in EX Series switches documentation are sometimes different from the terms used in the Junos OS command line interface (CLI).

See the following topics to map the hardware terms used in EX Series switches documentation to the corresponding terms used in the CLI:

- EX2200 Switch Hardware and CLI Terminology Mapping
- EX3200 Switch Hardware and CLI Terminology Mapping
- EX4200 Switch Hardware and CLI Terminology Mapping
- EX4500 Switch Hardware and CLI Terminology Mapping
- EX6210 Switch Hardware and CLI Terminology Mapping
- EX8208 Switch Hardware and CLI Terminology Mapping
- EX8216 Switch Hardware and CLI Terminology Mapping

Related Documentation

- EX2200 Switches Hardware Overview
- EX3200 Switches Hardware Overview
- EX4200 Switches Hardware Overview
- EX4500 Switches Hardware Overview
- EX6210 Switch Hardware Overview
- EX8208 Switch Hardware Overview
- EX8216 Switch Hardware Overview

J-Web User Interface for EX Series Switches Overview

You can use two interfaces to monitor, configure, troubleshoot, and manage a Juniper Networks EX Series Ethernet Switch: the J-Web graphical user interface and the Juniper Networks Junos operating system (Junos OS) command-line interface (CLI). Both of these user interfaces are shipped with the switch. This topic describes the J-Web interface. You can navigate the J-Web interface, scroll pages, and expand and collapse elements as you do in a typical Web browser interface. For information about the CLI user interface, see “CLI User Interface Overview” on page 387.

To access the J-Web interface for the switch, your management device requires the following software:

- Supported browsers—Microsoft Internet Explorer version 7.0 and Mozilla Firefox version 3.0 and later
NOTE: Other browser versions might not work on the switch. The browser and the network must support receiving and processing HTTP 1.1 GZIP compressed data.

- Language support—English-version browsers
- Supported OS—Microsoft Windows XP Service Pack 3

Each page of the J-Web interface is divided into panes.

- Top pane—Displays system identity information and links.
- Main pane—Location where you monitor, configure, diagnose (troubleshoot), and manage (maintain) the switch by entering information in text boxes, making selections, and clicking buttons.
- Side pane—Displays suboptions of the Monitor, Configure, Troubleshoot, or Maintain task currently displayed in the main pane. Click a suboption to access it in the main pane.

The layout of the panes allows you to quickly navigate through the interface. Table 79 on page 390 summarizes the elements of the J-Web interface.

The J-Web interface provides CLI tools that enable you to perform all of the tasks that you can perform from the Junos OS CLI, including a CLI Viewer to view the current configuration, a CLI Editor for viewing and modifying the configuration, and a Point & Click CLI editor that allows you to click through all of the available CLI statements.

<table>
<thead>
<tr>
<th>J-Web Interface Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Pane</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Top Pane</strong></td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>The hostname of the switch.</td>
</tr>
<tr>
<td>Logged in as: username</td>
<td>The username you used to log in to the switch.</td>
</tr>
</tbody>
</table>
### Table 79: J-Web Interface (continued)

<table>
<thead>
<tr>
<th>J-Web Interface Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Pane</strong></td>
<td></td>
</tr>
<tr>
<td>Commit Options</td>
<td>A set of options using which you can configure committing multiple changes with a single commit.</td>
</tr>
<tr>
<td></td>
<td>• Commit—Commits the candidate configuration of the current user session, along with changes from other user sessions.</td>
</tr>
<tr>
<td></td>
<td>• Compare—Displays the XML log of pending configurations on the device.</td>
</tr>
<tr>
<td></td>
<td>• Discard—Discards the candidate configuration of the current user session, along with changes from other user sessions.</td>
</tr>
<tr>
<td></td>
<td>• Preference—Indicates your choice of committing all configurations changes together or committing each configuration change immediately. The two commit options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Commit changes immediately</strong>—Sets the system to force an immediate commit on every page after every configuration change.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Validate changes until explicit commit</strong>—Loads all configuration changes for an accumulated single commit. If there are errors in loading the configuration, the errors are logged. This is the default mode.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> There are some pages on which configuration changes must be committed immediately. For such pages, if you configure the commit options for a single commit, the system displays warning notifications that remind you to commit your changes immediately. An example of such a page is <strong>Switching</strong>.</td>
</tr>
<tr>
<td><strong>Help</strong></td>
<td>Displays links to information on help and the J-Web interface.</td>
</tr>
<tr>
<td></td>
<td>• Help Contents—View context-sensitive help topics.</td>
</tr>
<tr>
<td></td>
<td>• About—Displays information about the J-Web interface, such as the version number.</td>
</tr>
<tr>
<td><strong>Logout</strong></td>
<td>Ends your current login session with the switch and returns you to the login page.</td>
</tr>
<tr>
<td><strong>Taskbar</strong></td>
<td>Menu of J-Web main options. Click the tab to access an option.</td>
</tr>
<tr>
<td></td>
<td>• Dashboard—Displays a high-level, graphical view of the chassis and the status of the switch. It displays system health information, alarms, and system status.</td>
</tr>
<tr>
<td></td>
<td>• Configure—Configure the switch, and view configuration history.</td>
</tr>
<tr>
<td></td>
<td>• Monitor—View information about configuration and hardware on the switch.</td>
</tr>
<tr>
<td></td>
<td>• Maintain—Manage files and licenses, upgrade software, and reboot the switch.</td>
</tr>
<tr>
<td></td>
<td>• Troubleshoot—Run diagnostic tools to troubleshoot network issues.</td>
</tr>
<tr>
<td><strong>Help (?) icon</strong></td>
<td>Displays useful information—such as the definition, format, and valid range of an option—when you mouse over the question mark.</td>
</tr>
<tr>
<td><strong>Red asterisk (*)</strong></td>
<td>Indicates a required field.</td>
</tr>
</tbody>
</table>
### Understanding J-Web Configuration Tools

The J-Web graphical user interface (GUI) allows you to monitor, configure, troubleshoot, and manage the switching platform by means of a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled. The J-Web interface provides access to all the configuration statements supported by the switch.

The J-Web interface provides three methods of configuring the switch:

- Configure menu
- Point & Click CLI Editor
- CLI Editor

Table 80 on page 393 gives a comparison of the three methods of configuration.

---

### Table 79: J-Web Interface (continued)

<table>
<thead>
<tr>
<th>J-Web Interface Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Pane</strong></td>
<td></td>
</tr>
<tr>
<td>Icon legend</td>
<td>(Applies to the Point &amp; Click CLI editor only) Explains icons that appear in the user interface to provide information about configuration statements:</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>C—Comment. Mouse over the icon to view a comment about the configuration statement.</td>
</tr>
<tr>
<td><strong>I</strong></td>
<td>I—Inactive. The configuration statement does not apply for the switch.</td>
</tr>
<tr>
<td><strong>M</strong></td>
<td>M—Modified. The configuration statement has been added or modified.</td>
</tr>
<tr>
<td>*<strong>—Mandatory</strong></td>
<td>*—Mandatory. The configuration statement must have a value.</td>
</tr>
</tbody>
</table>

| **Task Pane**           |             |
| Configuration hierarchy | (Applies to the Junos OS CLI configuration editor only) Displays the hierarchy of committed statements in the switch configuration. |
| **Click**               | Click Expand all to display the entire hierarchy. |
| **Hide all**            | Click Hide all to display only the statements at the top level. |
| **+**                   | Click plus signs (+) to expand individual items. |
| **-**                   | Click minus signs (-) to hide individual Items. |
Table 80: Switching Platform Configuration Interfaces

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Function</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure menu</td>
<td>Web browser pages for setting up the switch quickly and easily without configuring each statement individually. For example, use the Virtual Chassis Configuration page to configure the Virtual Chassis parameters on the switch.</td>
<td>Configure basic switch platform services:</td>
<td>Use for basic configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Switching</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Virtual Chassis</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• System Properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Routing</td>
<td></td>
</tr>
<tr>
<td>Point &amp; Click CLI editor</td>
<td>Web browser pages divided into panes in which you can do any of the following:</td>
<td>Configure all switching platform services:</td>
<td>Use for complete configuration if you are not familiar with the Junos OS CLI or prefer a graphical interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Expand the entire configuration hierarchy and click a configuration statement to view or edit. The main pane displays all the options for the statement, with a text box for each option.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Paste a complete configuration hierarchy into a scrollable text box, or edit individual lines.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Upload or download a complete configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Roll back to a previous configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create or delete a rescue configuration.</td>
<td></td>
</tr>
<tr>
<td>CLI editor</td>
<td>Interface in which you do any of the following:</td>
<td>Configure all switching platform services:</td>
<td>Use for complete configuration if you know the Junos OS CLI or prefer a command interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type commands on a line and press Enter to create a hierarchy of configuration statements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create an ASCII text file that contains the statement hierarchy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Upload a complete configuration, or roll back to a previous configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create or delete a rescue configuration.</td>
<td></td>
</tr>
</tbody>
</table>

Related Documentation
- Understanding J-Web User Interface Sessions on page 393
- J-Web User Interface for EX Series Switches Overview on page 389
- Connecting and Configuring an EX Series Switch (J-Web Procedure)
- Configuration Files Terms on page 499

Understanding J-Web User Interface Sessions
You establish a J-Web session with the switch through an HTTP-enabled or HTTPS-enabled Web browser. The HTTPS protocol, which uses 128-bit encryption, is available only in domestic versions of the Juniper Networks Junos operating system (Junos
OS). To use HTTPS, you must have installed a certificate on the switch and enabled HTTPS. See “Generating SSL Certificates to Be Used for Secure Web Access” on page 418.

When you attempt to log in through the J-Web interface, the switch authenticates your username with the same methods used for Telnet and SSH.

If the switch does not detect any activity through the J-Web interface for 15 minutes, the session times out and is terminated. You must log in again to begin a new session.

To explicitly terminate a J-Web session at any time, click Logout in the top pane.

Related Documentation

- J-Web User Interface for EX Series Switches Overview on page 389
- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 415
CHAPTER 8

Configuration

• Configuration Tasks on page 395

Configuration Tasks

• Using the J-Web CLI Terminal on page 395
• Starting the J-Web Interface on page 397

Using the J-Web CLI Terminal

The J-Web CLI terminal provides access to the Junos OS command-line interface (CLI) through the J-Web interface. The functionality and behavior of the CLI available through the CLI Terminal page is the same as that of the Junos OS CLI available through the switch console. The CLI terminal supports all CLI commands and other features such as CLI help and autocompletion. Using the CLI terminal page, you can fully configure, monitor, and manage the switch.

This topic covers:

• Configuring the Web Browser on page 395
• Setting Domain Name, Hostname, and Name Server on page 396
• Enabling SSH on your system on page 396
• Sample Configuration on an EX Series Switch on page 396

Configuring the Web Browser

Configure your Web browser as follows:

• Install Java Runtime Environment (JRE) version 1.4 or later on your system. JRE is a software package that must be installed on the client system to run Java applications. You can download the latest version of JRE from the Java software website http://www.java.com/. Installing JRE installs Java plug-ins, which once installed, load automatically and transparently to render Java applets.

NOTE: By default Mozilla Firefox has blocked JRE versions earlier than 1.6.0_31 and 1.7.0 through 1.7.0_2. However, Mozilla Firefox users can still click Add-ons > Plugin to enable Java.
• Set your browser to support and enable Java applets. To know more about checking the status of Java applets in your browser see http://java.com/en/download/help/enable_browser.xml.

Setting Domain Name, Hostname, and Name Server

Configure the domain name and hostname of the switch on your system. Ensure that the DNS server setting is correct. DNS name resolution must happen properly. Ensure that there is connectivity between the client and the management device.

You can set the domain name, hostname, and the DNS name server either through the J-Web interface or the CLI:

• To set through the J-Web interface:
  See “Configuring System Identity for an EX Series Switch (J-Web Procedure)” on page 118 for more information.

• To set through the CLI:
  
  set system domain-name domain-name
  set system host-name host-name
  set system name-server dns-ip-address

Enabling SSH on your system

SSH provides a secure method of logging in to the switch, and encrypting traffic so that it is not intercepted. If SSH is not enabled on the system, the CLI terminal page displays the error message:

To enable SSH on your system, do the following:

set system services ssh

Sample Configuration on an EX Series Switch

1. Type the configure command to enter the configuration mode:

   user@switch> configure

2. Log in as host:

   user@switch# set system host-name host

3. Configure the encrypted password; for example:

   user@switch# set system root-authentication encrypted-password "$1Smr3D4eVfSmc7y54e6hk4JlpuWPao6."

4. Map the hostname to the IP address:

   user@switch# set system static-host-mapping host inet 10.9.221.31

5. Configure the IP address for the DNS server:

   user@switch# set system name-server 10.0.220.1
6. Enable the system services by using:

   set system services:admin
   set system services ssh

7. Select Troubleshoot > CLI Terminal. The password window is displayed.

8. Enter the password, and click OK. The CLI Terminal window appears on the J-Web page.

   NOTE: If you exit from the CLI terminal, the connection is lost. Click CLI Terminal if you want to connect again.

   Related Documentation
   • CLI User Interface Overview on page 387
   • Understanding J-Web Configuration Tools on page 392

Starting the J-Web Interface

You can use the J-Web graphical interface to configure and manage the EX Series switch.

To start the J-Web interface:

1. Launch your HTTP-enabled or HTTPS-enabled Web browser.

   To use HTTPS, you must have installed a certificate on the switch and enabled HTTPS.

2. After http:// or https:// in your Web browser, type the hostname or IP address of the switch and press Enter.

   The J-Web login page appears.

3. On the login page, type your username and password, and click Log In.

   To correct or change the username or password you typed, click Reset, type the new entry or entries, and click Log In.

   NOTE: The default username is root with no password. You must change this during initial configuration or the system does not accept the configuration.

   The Chassis Dashboard information page appears.

To explicitly terminate a J-Web session at any time, click Logout in the top pane.

   Related Documentation
   • J-Web User Interface for EX Series Switches Overview on page 389
   • Dashboard for EX Series Switches on page 670
CHAPTER 9

Administration

- Operational Commands on page 399

Operational Commands
set cli directory

Syntax

set cli directory directory

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Set the current working directory.

Options
directory—Pathname of the working directory.

Required Privilege

Level view

Related Documentation

• CLI User Interface Overview
• show cli directory

List of Sample Output

set cli directory on page 400

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

set cli directory

user@host> set cli directory /var/home/regress
Current directory: /var/home/regress
set cli idle-timeout

**Syntax**

```
set cli idle-timeout <minutes>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Set the maximum time that an individual session can be idle before the user is logged off the router or switch.

**Options**

- `minutes`—(Optional) Maximum idle time. The range of values, in minutes, is 0 through 100,000. If you do not issue this command, and the user’s login class does not specify this value, the user is never forced off the system after extended idle times. Setting the value to 0 disables the timeout.

**Required Privilege**

- `view`

**Related Documentation**

- [CLI User Interface Overview](#)
- [show cli](#)

**List of Sample Output**

- set cli idle-timeout on page 401

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
set cli idle-timeout

user@host> set cli idle-timeout 60
Idle timeout set to 60 minutes
```
**set cli prompt**

**Syntax**  
set cli prompt string

**Release Information**  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Set the prompt so that it is displayed within the CLI.

**Options**  
*string*—CLI prompt string. To include spaces in the prompt, enclose the string in quotation marks. By default, the string is \textit{username@hostname}.

**Required Privilege Level**  
view

**Related Documentation**  
- CLI User Interface Overview
- show cli

**List of Sample Output**  
set cli prompt on page 402

**Output Fields**  
When you enter this command, the new CLI prompt is displayed.

**Sample Output**

set cli prompt

user@host> set cli prompt lab1-router>
lab1-router>
set cli restart-on-upgrade

Syntax
set cli restart-on-upgrade string (off | on)

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
For an individual session, set the CLI to prompt you to restart the router or switch after upgrading the software.

Options
off—Disables the prompt.
on—Enables the prompt.

Required Privilege
view

Related Documentation
• CLI User Interface Overview
• show cli

List of Sample Output
set cli restart-on-upgrade on page 403

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
set cli restart-on-upgrade

user@host> set cli restart-on-upgrade on
Enabling restart-on-upgrade
**set cli screen-length**

**Syntax**

```
set cli screen-length length
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Set terminal screen length.

**Options**

`length`—Number of lines of text that the terminal screen displays (0 through 10,000). The default is 24.

**Additional Information**

The point at which the ---(more)--- prompt appears on the screen is a function of this setting and the settings for the `set cli screen-width` and `set cli terminal` commands.

**Required Privilege Level**

view

**Related Documentation**

- CLI User Interface Overview
- `set cli screen-width` on page 405
- `set cli terminal`
- `show cli`

**List of Sample Output**

set cli screen-length on page 404

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
set cli screen-length
user@host> set cli screen-length 75
Screen length set to 75
```
**set cli screen-width**

**Syntax**

```
set cli screen-width width
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Set the terminal screen width.

**Options**

`width`—Number of characters (0 through 1024) in a line. The default is 80.

**Additional Information**

The point at which the ---(more)--- prompt appears on the screen is a function of this setting and the settings for the `set cli screen-length` and `set cli terminal` commands.

**Required Privilege**

View

**Related Documentation**

- CLI User Interface Overview
- `set cli screen-length` on page 404
- `set cli terminal`
- `show cli`

**List of Sample Output**

`set cli screen-width` on page 405

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
set cli screen-width

user@host> set cli screen-width
Screen width set to 132
```
set cli timestamp

Syntax  set cli timestamp (format timestamp-format | disable)

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description  Set a timestamp for CLI output.

Options  format timestamp-format—Set the date and time format for the timestamp. The
timestamp format you specify can include the following placeholders in any order:
  • %m—Two-digit month
  • %d—Two-digit date
  • %T—Six-digit hour, minute, and seconds

disable—Remove the timestamp from the CLI.

Required Privilege  view

Related Documentation  • CLI User Interface Overview
  • show cli

List of Sample Output  set cli timestamp on page 406

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

set cli timestamp

user@host> set cli timestamp format '%m-%d-%T'
'04-21-17:39:13'
CLI timestamp set to: '%m-%d-%T'
**start shell**

**Syntax**  
start shell (csh | sh)  
<user username>

**Release Information**  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**  
Exit from the CLI environment and create a UNIX-level shell. To return to the CLI, type `exit` from the shell.

---

**NOTE:**
- To issue this command, the user must have the required login access privileges configured by including the permissions statement at the `[edit system login class class-name]` hierarchy level.
- UNIX wheel group membership or permissions are no longer required to issue this command.

**Options**
- **csh**—Create a UNIX C shell.
- **sh**—Create a UNIX Bourne shell.
- **user username**—(Optional) Start the shell as another user.

**Additional Information**  
When you are in the shell, the shell prompt has the following format:  
`username@hostname%`

An example of the prompt is:
```
root@host%
```

**Required Privilege Level**  
shell and maintenance

**List of Sample Output**  
start shell csh on page 407

**Output Fields**  
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
start shell csh

user@host> start shell csh
%
exit
```
username@hostname% startshell sh
% exit
user@host>
PART 5

Access and User Management

- Overview on page 411
- Configuration on page 415
- Administration on page 463
- Troubleshooting Procedures on page 485
CHAPTER 10

Overview

- Software Overview on page 411

Software Overview

- Understanding Software Infrastructure and Processes on page 411

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 411
- Junos OS Processes on page 412

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.

- Routing Engine—Provides three main functions:
  - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network.
- Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

**Junos OS Processes**

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 61 on page 112 describes the primary Junos OS processes.

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis process</td>
<td>chassisd</td>
<td>Detects hardware on the system that is used to configure network interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>eswd</td>
<td>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>switching</td>
<td></td>
<td>Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarding</td>
<td>pfem</td>
<td>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface process</td>
<td>dcd</td>
<td>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</td>
</tr>
<tr>
<td>Management</td>
<td>mgd</td>
<td>Provides communication between the other processes and an interface to the configuration database.</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td>Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interacts with the other processes when commands are issued through one of the user interfaces on the switch.</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>rpd</td>
<td>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Related Documentation

- For more information about processes, see *Junos OS Network Operations Guide*
- For more information about basic system parameters, supported protocols, and software processes, see *Junos OS System Basics Configuration Guide*
CHAPTER 11

Configuration

- Configuration Tasks on page 415
- Configuration Statements on page 420

Configuration Tasks

- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 415
- Generating SSL Certificates to Be Used for Secure Web Access on page 418
- Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure) on page 419

Configuring Management Access for the EX Series Switch (J-Web Procedure)

You can manage an EX Series switch remotely through the J-Web interface. To communicate with the switch, the J-Web interface uses Hypertext Transfer Protocol (HTTP). HTTP allows easy Web access but no encryption. The data that is transmitted between the Web browser and the switch by means of HTTP is vulnerable to interception and attack. To enable secure Web access the switch supports HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

Navigate to the Secure Access Configuration page by selecting Configure > System Properties > Management Access. On this page, you can enable HTTP and HTTPS access on interfaces for managing the EX Series switch through the J-Web interface. You can also install SSL certificates and enable Junos XML management protocol over SSL with the Secure Access page.

1. Click Edit to modify the configuration. Enter information into the Management Access Configuration page as described in Table 82 on page 416.

2. To verify that Web access is enabled correctly, connect to the switch using the appropriate method:
   - For HTTP access—In your Web browser, type http://URL or http://IP address.
   - For HTTPS access—In your Web browser, type https://URL or https://IP address.
For SSL Junos XML management protocol access—To use this option, you must have a Junos XML management protocol client such as Junos Scope. For information about how to log into Junos Scope, see the Junos Scope Software User Guide.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 82: Secure Management Access Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Access tab</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Management Port IP/Management Port IPv6 | Specifies the management port IP address. The software supports both IPv4 (displayed as IP) and IPv6 address. | To specify an IPv4 address:  
1. Select the check box **IPv4 address**.  
2. Type an IP address—for example: 10.10.10.10.  
3. Enter the subnet mask or address prefix. For example, 24 bits represents 255.255.255.0.  
4. Click OK.  
To specify an IPv6 address:  
1. Select the check box **IPv6 address**.  
2. Type an IP address—for example: 2001:ab8:85a3::8a2e:370:7334.  
3. Enter the subnet mask or address prefix.  
4. Click OK. |
| Default Gateway | Defines a default gateway through which to direct packets addressed to networks that are not explicitly listed in the bridge table constructed by the switch. | For IPv4 address type a 32-bit IP address, in dotted decimal notation. Type a 128-bit IP address for IPv6 address type. |
| Loopback address | Specifies the IP address of the loopback interface. | Type an IP address. |
| Subnet Mask | Specifies the subnet mask for the loopback interface. | Enter the subnet mask or address prefix. |
| **Services tab** | | |
| Services | Specifies services to be enabled: telnet and SSH. | Select to enable the required services. |
| Enable Junos XML management protocol over Clear Text | Enables clear text access to the Junos XML management protocol XML scripting API. | To enable clear text access, select the **Enable Junos XML management protocol over Clear Text** check box. |
YourActionFunctionField

To enable SSL access, select the **Enable Junos XML management protocol over SSL** check box.

**Enables secure SSL access to the Junos XML management protocol XML scripting API.**

To enable an SSL certificate, select a certificate from the Junos XML management protocol SSL Certificate list—for example, new.

**Specifies SSL certificates to be used for encryption.**

This field is available only after you create at least one SSL certificate.

To enable HTTP access, select the **Enable HTTP access** check box.

**Enables HTTP access on interfaces.**

Select and clear interfaces by clicking the direction arrows:

- To enable HTTP access on an interface, add the interface to the HTTP Interfaces list. You can either select all interfaces or specific interfaces.

To enable HTTPS access, select the **Enable HTTPS access** check box.

**Enables HTTPS access on interfaces.**

Select and deselect interfaces by clicking the direction arrows:

- To enable HTTPS access on an interface, add the interface to the HTTPS Interfaces list. You can either select all interfaces or specific interfaces.

**NOTE:** Specify the certificate to be used for HTTPS access.

To add a certificate:

1. Have a general SSL certificate available. See Generating SSL Certificates for more information.
2. Click Add. The Add a Local Certificate page opens.
3. Type a name in the Certificate Name box—for example, new.
4. Open the certificate file and copy its contents.
5. Paste the generated certificate and RSA private key in the Certificate box.

To edit a certificate, select it and click Edit.

To delete a certificate, select it and click Delete.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Junos XML protocol over SSL</td>
<td>Enables secure SSL access to the Junos XML management protocol XML scripting API.</td>
<td>To enable SSL access, select the <strong>Enable Junos XML management protocol over SSL</strong> check box.</td>
</tr>
<tr>
<td>Junos XML management protocol Certificate</td>
<td>Specifies SSL certificates to be used for encryption. This field is available only after you create at least one SSL certificate.</td>
<td>To enable an SSL certificate, select a certificate from the Junos XML management protocol SSL Certificate list—for example, new.</td>
</tr>
<tr>
<td>Enable HTTP</td>
<td>Enables HTTP access on interfaces.</td>
<td>To enable HTTP access, select the <strong>Enable HTTP access</strong> check box. Select and clear interfaces by clicking the direction arrows: To enable HTTP access on an interface, add the interface to the HTTP Interfaces list. You can either select all interfaces or specific interfaces.</td>
</tr>
<tr>
<td>Enable HTTPS</td>
<td>Enables HTTPS access on interfaces.</td>
<td>To enable HTTPS access, select the <strong>Enable HTTPS access</strong> check box. Select and deselect interfaces by clicking the direction arrows: To enable HTTPS access on an interface, add the interface to the HTTPS Interfaces list. You can either select all interfaces or specific interfaces. <strong>NOTE:</strong> Specify the certificate to be used for HTTPS access.</td>
</tr>
</tbody>
</table>

**Certificates tab**

**Certificates**

Displays digital certificates required for SSL access to the switch. Allows you to add and delete SSL certificates.

To add a certificate:

1. Have a general SSL certificate available. See Generating SSL Certificates for more information.
2. Click Add. The Add a Local Certificate page opens.
3. Type a name in the Certificate Name box—for example, new.
4. Open the certificate file and copy its contents.
5. Paste the generated certificate and RSA private key in the Certificate box.

To edit a certificate, select it and click Edit.

To delete a certificate, select it and click Delete.
Generating SSL Certificates to Be Used for Secure Web Access

You can set up secure Web access for an EX Series switch. To enable secure Web access, you must generate a digital Secure Sockets Layer (SSL) certificate and then enable HTTPS access on the switch.

To generate an SSL certificate:

1. Enter the following `openssl` command in your SSH command-line interface on a BSD or Linux system on which `openssl` is installed. The `openssl` command generates a self-signed SSL certificate in the privacy-enhanced mail (PEM) format. It writes the certificate and an unencrypted 1024-bit RSA private key to the specified file.

   ```
   % openssl req -x509 -nodes -newkey rsa:1024 -keyout filename.pem -out filename.pem
   
   where `filename` is the name of a file in which you want the SSL certificate to be written—for example, `my-certificate.pem`.
   ```

2. When prompted, type the appropriate information in the identification form. For example, type `US` for the country name.

3. Display the contents of the file that you created.

   ```
   cat my-certificate.pem
   ```

You can use the J-Web Configuration page to install the SSL certificate on the switch. To do this, copy the file containing the certificate from the BSD or Linux system to the switch. Then open the file, copy its contents, and paste them into the Certificate box on the J-Web Secure Access Configuration page.

You can also use the following CLI statement to install the SSL certificate on the switch:

```
[edit]
user@switch# set security certificates local my-signed-cert load-key-file my-certificate.pem
```
Configuring MS-CHAPv2 to Provide Password-Change Support (CLI Procedure)

Junos OS for EX Series switches enables you to configure the Microsoft Corporation implementation of the Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) on the switch to provide password-change support. Configuring MS-CHAPv2 on the switch provides users accessing a switch the option of changing the password when the password expires, is reset, or is configured to be changed at next login.

See RFC 2433, Microsoft PPP CHAP Extensions, for information about MS-CHAP.

Before you configure MS-CHAPv2 to provide password-change support, ensure that you have:

- Configured RADIUS server authentication. Configure users on the authentication server and set the first-tried option in the authentication order to radius. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.

To configure MS-CHAPv2, specify the following:

```
[edit system radius-options]
user@switch# set password-protocol mschap-v2
```

You must have the required access permission on the switch in order to change your password.

Related Documentation

- Managing Users (J-Web Procedure) on page 463
- For more about configuring user access, see the Junos OS Access Privilege Configuration Guide.
### Configuration Statements

#### allow-commands

<table>
<thead>
<tr>
<th>Syntax</th>
<th>allow-commands &quot;regular-expression&quot;;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit system login class class-name]</td>
</tr>
</tbody>
</table>
| Release Information | Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description     | Specify the operational mode commands that members of a login class can use. |
| Default         | If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement. |
| Options         | regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2.  
If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. |
| Required Privilege Level | admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration. |
| Related Documentation | • Specifying Access Privileges for Junos OS Operational Mode Commands  
• deny-commands on page 428  
• user on page 462 |
### allow-configuration

<table>
<thead>
<tr>
<th>Syntax</th>
<th>allow-configuration &quot;regular-expression&quot;;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit system login class class-name]</td>
</tr>
</tbody>
</table>
| Release Information | Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | Explicitly allow configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement do not grant such access by default. |
| Default | If you omit this statement and the deny-configuration statement, users can edit only those commands for which they have access privileges through the permissions statement. |
| Options | regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2.  
If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks. |
| Required Privilege Level | admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration. |
| Related Documentation | • Specifying Access Privileges Using allow/deny-configuration Statements  
• Regular Expressions for Allowing and Denying Junos OS Configuration Mode Hierarchies  
• deny-configuration on page 429  
• user on page 462 |
### announcement

**Syntax**

```plaintext
announcement text;
```

**Hierarchy Level**

[edit system login]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure a system login announcement. This announcement appears after a user logs in.

**Options**

- `text`—Text of the announcement. If the text contains any spaces, enclose it in quotation marks.

**Required Privilege Level**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration

**Related Documentation**

- Configuring the Junos OS to Display a System Login Announcement
- message on page 443

### archive-sites

**Syntax**

```plaintext
archive-sites {
  site-name;
}
```

**Hierarchy Level**

[edit accounting-options file filename]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure an archive site. If more than one site name is configured, an ordered list of archive sites for the accounting-data log files is created. When a file is archived, the router or switch attempts to transfer the file to the first URL in the list, moving to the next site only if the transfer does not succeed. The log file is stored at the archive site with a filename of the format `router-name_log-filename_timestamp`.

**Options**

- `site-name`—Any valid FTP URL to a destination. For information about specifying valid FTP URLs, see the Junos System Basics: Getting Started Configuration Guide.

**Required Privilege Level**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration

**Related Documentation**

- Configuring Archive Sites
authentication (Login)

Syntax

```
authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file URL filename;
  ssh-dsa "public-key";
  ssh-ecdsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level [edit system login user username]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Authentication methods that a user can use to log in to the router or switch. You can assign multiple authentication methods to a single user.

Options

- `encrypted-password "password"`—Message Digest 5 (MD5) or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password for each user.

  You cannot configure a blank password for `encrypted-password` using blank quotation marks (" "). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

- `load-key-file URL filename`—Load previously-generated RSA (SSH version 1 and SSH version 2) and DSA (SSH version 2) public keys from a named file at a specified URL location. The file contains one or more SSH keys.

- `plain-text-password`—When using this option, the command-line interface (CLI) prompts you for the password and then encrypts it.

- `ssh-dsa "public-key"`—SSH version 2 authentication. Specify the DSA public key. You can specify one or more public keys for each user.

- `ssh-ecdsa "public-key"`—SSH version 2 authentication. Specify the ECDSA public key. You can specify one or more public keys for each user.

- `ssh-rsa "public-key"`—SSH version 1 and SSH version 2 authentication. Specify the RSA public key. You can specify one or more public keys for each user.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Junos OS User Accounts
- root-authentication on page 452
**authentication-order**

**Syntax**
```
authentication-order [ authentication-methods ];
```

**Hierarchy Level**
```
[edit system]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order, starting with the first one, until the password matches.

**Default**
If you do not include the `authentication-order` statement, users are verified based on their configured passwords.

**Options**
```
authentication-methods—One or more authentication methods, listed in the order in which they should be tried. The method can be one or more of the following:
```

- **password**—Use the password configured for the user with the `authentication` statement at the `[edit system login user]` hierarchy level.
- **radius**—Use RADIUS authentication services.
- **tacplus**—Use TACACS+ authentication services.

**Required Privilege Level**
```
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
```

**Related Documentation**
- Configuring the Junos OS Authentication Order for RADIUS, TACACS+, and Local Password Authentication
- `authentication` on page 423
change-type

**Syntax**
change-type (character-sets | set-transitions);

**Hierarchy Level**
[edit system login password]

**Release Information**
Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Set requirements for using character sets in plain-text passwords. When you combine this statement with the `minimum-changes` statement, you can check for the total number of character sets included in the password or for the total number of character-set changes in the password. Newly created passwords must meet these requirements.

**Options**
Specify one of the following:
- `character-sets`—The number of character sets in the password. Valid character sets include uppercase letters, lowercase letters, numbers, punctuation, and other special characters.
- `set-transitions`—The number of transitions between character sets.

**Required Privilege**
- Level system—To view this statement in the configuration.
- Level system-control—To add this statement to the configuration.

**Related Documentation**
- `Special Requirements for Junos OS Plain-Text Passwords`
- `minimum-changes on page 445`

class (Assigning a Class to an Individual User)

**Syntax**
class class-name;

**Hierarchy Level**
[edit system login user username]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure a user's login class. You must configure one class for each user.

**Options**
class-name—One of the classes defined at the [edit system login class] hierarchy level.

**Required Privilege**
- Level admin—To view this statement in the configuration.
- Level admin-control—To add this statement to the configuration.

**Related Documentation**
- `Configuring Junos OS User Accounts`
class (Defining Login Classes)

Syntax

```
class class-name {
    allow-commands "regular-expression";
    ( allow-configuration | allow-configuration-regexps ) "regular expression 1" "regular expression 2";
    configuration-breadcrumbs;
    deny-commands "regular-expression";
    ( deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular expression 2";
    idle-timeout minutes;
    login-script filename;
    login-tip;
    permissions [ permissions ];
}
```

Hierarchy Level  [edit system login]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Define a login class.

Options  class-name—A name you choose for the login class.

The remaining statements are explained separately.

Required Privilege  Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Defining Junos OS Login Classes
- user on page 462
class-usage-profile

Syntax

```
class-usage-profile profile-name {
  file filename;
  interval minutes;
  source-classes {
    source-class-name;
  }
  destination-classes {
    destination-class-name;
  }
}
```

Hierarchy Level  [edit accounting-options]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Create a class usage profile, which is used to log class usage statistics to a file in the /var/log directory. The class usage profile logs class usage statistics for the configured source classes on every interface that has destination-class-usage configured.

For information about configuring source classes, see the Junos Routing Protocols Configuration Guide. For information about configuring source class usage, see the Junos Network Management Configuration Guide.

Options  `profile-name`—Name of the destination class profile.

The remaining statements are explained separately.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring Class Usage Profiles
counters

Syntax       counters {
             counter-name;
         }

Hierarchy Level [edit accounting-options filter-profile profile-name]

Release Information Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Names of counters for which filter profile statistics are collected. The packet and byte counts for the counters are logged to a file in the /var/log directory.

Options counter-name—Name of the counter.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation • Configuring the Counters

deny-commands

Syntax       deny-commands "regular-expression";

Hierarchy Level [edit system login class]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the operational mode commands that the user is denied permission to issue even though the permissions set with the permissions statement would allow it.

Default If you omit this statement and the allow-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.

Options regular-expression—Extended (modern) regular expression as defined in POSIX 1003.2.
If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • Specifying Access Privileges for Junos OS Operational Mode Commands
• allow-commands on page 420
• user on page 462
deny-configuration

**Syntax**

deny-configuration "regular-expression";

**Hierarchy Level**
[edit system login class]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Explicitly deny configuration access to the specified levels in the hierarchy even if the permissions set with the permissions statement grant such access by default. Note that the user cannot view a particular hierarchy if configuration access is denied for that hierarchy.

**Default**
If you omit this statement and the allow-configuration statement, users can edit those levels in the configuration hierarchy for which they have access privileges through the permissions statement.

**Options**
- **regular-expression**—Extended (modern) regular expression as defined in POSIX 1003.2.
  - If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

**Required Privilege Level**
- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

**Related Documentation**
- Specifying Access Privileges Using allow/deny-configuration Statements
- allow-configuration on page 421
- user on page 462
destination-classes

Syntax

```
destination-classes {  
destination-class-name;  
}
```

Hierarchy Level

[edit accounting-options class-usage-profile profile-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify the destination classes for which statistics are collected.

Options

`destination-class-name`—Name of the destination class to include in the source class usage profile.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Configuring a Class Usage Profile
**fields (for Interface Profiles)**

**Syntax**
```
fields {
    field-name;
}
```

**Hierarchy Level**
```
[edit accounting-options interface-profile profile-name]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Statistics to collect in an accounting-data log file for an interface.

**Options**
- `field-name`—Name of the field:
  - `input-bytes`—Input bytes
  - `input-errors`—Generic input error packets
  - `input-multicast`—Input packets arriving by multicast
  - `input-packets`—Input packets
  - `input-unicast`—Input unicast packets
  - `output-bytes`—Output bytes
  - `output-errors`—Generic output error packets
  - `output-multicast`—Output packets sent by multicast
  - `output-packets`—Output packets
  - `output-unicast`—Output unicast packets

**Required Privilege**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- *Configuring the Interface Profile*
# file (Associating with a Profile)

**Syntax**
```
file filename;
```

**Hierarchy Level**
- [edit accounting-options class-usage-profile profile-name]
- [edit accounting-options filter-profile profile-name]
- [edit accounting-options interface-profile profile-name]
- [edit accounting-options mib-profile profile-name]
- [edit accounting-options routing-engine-profile profile-name]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series Switches.

**Description**
Specify the accounting log file associated with the profile.

**Options**
- `filename`—Name of the log file. You must specify a filename already configured in the `file` statement at the [edit accounting-options] hierarchy level.

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- [Configuring the Interface Profile](#)
- [Configuring the Filter Profile](#)
- [Configuring the MIB Profile](#)
- [Configuring the Routing Engine Profile](#)
file (Configuring a Log File)

Syntax

```
file filename {
  archive-sites {
    site-name;
  }
  files number;
  nonpersistent;
  size bytes;
  source-classes time;
  transfer-interval minutes;
}
```

Hierarchy Level [edit accounting-options]


Description Specify a log file to be used for accounting data.

Options

- `filename`—Name of the file in which to write accounting data.
  
  The remaining statements are explained separately.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Accounting-Data Log Files
files

Syntax files number;

Hierarchy Level [edit accounting-options file filename]


Description Specify the maximum number of log files to be used for accounting data.

Options number—The maximum number of files. When a log file (for example, profilelog) reaches its maximum size, it is renamed profilelog.0, then profilelog.1, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. The minimum value for number is 3 and the default value is 10.

Required Privilege Level interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

Related Documentation • Configuring Accounting-Data Log Files
filter-profile

Syntax

filter-profile profile-name {
  counters {
    counter-name;
  }
  file filename;
  interval minutes;
}

Hierarchy Level

[edit accounting-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Create a profile to filter and collect packet and byte count statistics and write them to a file in the /var/log directory. To apply the profile to a firewall filter, you include the accounting-profile statement at the [edit firewall filter filter-name] hierarchy level. For more information about firewall filters, see the Junos Network Management Configuration Guide.

Options

profile-name—Name of the filter profile.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Filter Profile
format

Syntax format ( md5 | sha1 );

Hierarchy Level [edit system login password]

Release Information Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the authentication algorithm for plain-text passwords.

Default For Junos OS, the default encryption format is md5. For Junos-FIPS software, the default encryption format is sha1.

Options The hash algorithm that authenticates the password can be one of these algorithms:

- md5—Produces a 128-bit digest.
- sha1—Produces a 160-bit digest.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation • Special Requirements for Junos OS Plain-Text Passwords

full-name

Syntax full-name complete-name ;

Hierarchy Level [edit system login user]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the complete name of a user.

Options complete-name—Full name of the user. If the name contains spaces, enclose it in quotation marks.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • Configuring Junos OS User Accounts
• user on page 462
• user
idle-timeout (System-Login)

Syntax  
idle-timeout minutes;

Hierarchy Level  
[edit system login class class-name]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
For a login class, configure the maximum time that a session can be idle before the user is logged out of the router or switch. The session times out after remaining at the CLI operational mode prompt for the specified time.

Default  
If you omit this statement, a user is never forced off the system after extended idle times.

Options  
minutes—Maximum idle time.
Range: 0 through 4294967295 minutes

Required Privilege Level  
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation  
• Configuring the Timeout Value for Idle Login Sessions
• user on page 462
interface-profile

Syntax

```
interface-profile profile-name {
  fields {
    field-name;
  }
  file filename;
  interval minutes;
}
```

Hierarchy Level
[edit accounting-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Create a profile to filter and collect error and packet statistics and write them to a file in the /var/log directory. You can specify an interface profile for either a physical or a logical interface.

Options

- **profile-name**—Name of the interface profile.

  The remaining statements are explained separately.

Required Privilege Level
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

Related Documentation
- Configuring the Interface Profile
interval (Accounting Options)

Syntax  
interval minutes;

Hierarchy Level  
[edit accounting-options class-usage-profile profile-name],  
[edit accounting-options filter-profile profile-name],  
[edit accounting-options interface-profile profile-name],  
[edit accounting-options mib-profile profile-name],  
[edit accounting-options routing-engine-profile profile-name]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Specify how often statistics are collected for the accounting profile.

Options  
minutes—Length of time between each collection of statistics.  
Range: 1 through 2880 minutes  
Default: 30 minutes

Required Privilege Level  
interface—to view this statement in the configuration.  
interface-control—to add this statement to the configuration.

Related Documentation  
• Configuring the Interface Profile  
• Configuring the Filter Profile  
• Configuring the MIB Profile  
• Configuring the Routing Engine Profile
login

Syntax

```
login {
    announcement text;
    class class-name {
        allow-commands "regular-expression";
        allow-configuration-regexps "regular expression 1" "regular expression 2";
        configuration-breadcrumbs;
        deny-commands "regular-expression";
        (deny-configuration | deny-configuration-regexps ) "regular expression 1" "regular expression 2";
        idle-timeout minutes;
        login-script filename;
        login-tip;
        permissions [permissions ];
    }
    message text;
    password {
        change-type (set-transitions | character-set);
        format (md5 | sha1 | des);
        maximum-length length;
        minimum-changes number;
        minimum-length length;
    }
    retry-options {
        backoff-threshold number;
        backoff-factor seconds;
        minimum-time seconds;
        tries-before-disconnect number;
    }
    user username {
        full-name complete-name;
        uid uid-value;
        class class-name;
        authentication authentication;
        (encrypted-password "password" | plain-text-password);
        ssh-rsa "public-key";
        ssh-dsa "public-key";
    }
}
```

Hierarchy Level [edit system]


Description Configure user access to the router or switch.

NOTE: The remaining statements are explained separately.
login-alarms

**Syntax**
```
login-alarms;
```

**Hierarchy Level**
```
[edit system login class class-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Show system alarms automatically when an admin user logs in to the router or switch.

**Options**
class-name—Login class name.

**Required Privilege Level**
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**
- *Defining Junos OS Login Classes*
- *Configuring System Alarms to Appear Automatically Upon Login*

login-tip

**Syntax**
```
login-tip;
```

**Hierarchy Level**
```
[edit system login class class-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Enable CLI tips at login.

**Default**
Disabled.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- *Configuring CLI Tips*
maximum-length

Syntax  maximum-length length;

Hierarchy Level  [edit system login passwords]

Release Information  Statement introduced in Junos OS Release 7.4.
                      Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify the maximum number of characters allowed in plain-text passwords. Newly
              created passwords must meet this requirement.

Default  For Junos-FIPS software, the maximum number of characters for plain-text passwords
          is 20. For Junos OS, no maximum is set.

Options  length—The maximum number of characters the password can include.
          Range: 1 to 64 characters

Required Privilege Level  system—To view this statement in the configuration.
                          system-control—To add this statement to the configuration.

Related Documentation  • Special Requirements for Junos OS Plain-Text Passwords
                        • Example: Changing the Requirements for Junos OS Plain-Text Passwords
                        • password (Login) on page 448
message

Syntax  message text;

Hierarchy Level  [edit system login]

Release Information  Statement introduced before Junos OS Release 7.4.
  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure a system login message. This message appears before a user logs in.

  You can format the message using the following special characters:

  • \n—New line
  • \t—Horizontal tab
  • \’—Single quotation mark
  • \"—Double quotation mark
  • \\
—Backslash

Options  text—Text of the message.

Required Privilege  system—To view this statement in the configuration.
  system-control—To add this statement to the configuration

Related Documentation  • Configuring the Junos OS to Display a System Login Message
  • announcement on page 422
### mib-profile

**Syntax**

```
  mib-profile profile-name {
    file filename;
    interval minutes;
    object-names {
      mib-object-name;
    }
    operation operation-name;
  }
```

**Hierarchy Level**

[edit accounting-options]

**Release Information**

Statement introduced in Junos OS Release 8.2.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Create a MIB profile to collect selected MIB statistics and write them to a file in the `/var/log` directory.

---

**NOTE:** Do not configure MIB objects related to interface octets or packets for a MIB profile, because it can cause the SNMP walk or a CLI show command to time out.

---

**Options**

- `profile-name`—Name of the MIB statistics profile.

  The remaining statements are explained separately.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- *Configuring the MIB Profile*
**minimum-changes**

**Syntax**  
minimum-changes number;

**Hierarchy Level**  
[edit system login passwords]

**Release Information**  
Statement introduced in Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Specify the minimum number of character sets (or character set changes) required in plain-text passwords. Newly created passwords must meet this requirement.

This statement is used in combination with the change-type statement. If the change-type is **character-sets**, then the number of character sets included in the password is checked against the specified minimum. If change-type is **set-transitions**, then the number of character set changes in the password is checked against the specified minimum.

**Default**  
For Junos OS, the minimum number of changes is 1. For Junos-FIPS Software, the minimum number of changes is 3.

**Options**  
number—The minimum number of character sets (or character set changes) required for the password.

**Required Privilege Level**  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**

- *Special Requirements for Junos OS Plain-Text Passwords*
- *change-type on page 425*
### minimum-length

**Syntax**  
minimum-length length;

**Hierarchy Level**  
[edit system login passwords]

**Release Information**  
Statement introduced in Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Specify the minimum number of characters required in plain-text passwords. Newly created passwords must meet this requirement.

This statement can be used in combination with all of the other requirement options for plain-text passwords, such as `minimum-upper-cases`, `minimum-punctuations`, `minimum-lower-cases`, and so on.

Using several password minimum requirement options will cause the `minimum-length` to be reset if the total sum of the required minimums exceeds the `minimum-length` setting.

**Default**  
For Junos OS, the minimum number of characters for plain-text passwords is six. For Junos-FIPS software, the minimum number of characters for plain-text passwords is 10.

**Options**  
length—The minimum number of characters the password must include.  
Range: 6 to 20 characters

**Required Privilege Level**  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**  
- *Special Requirements for Junos OS Plain-Text Passwords*
- *Example: Changing the Requirements for Junos OS Plain-Text Passwords*
- *maximum-length on page 442*
object-names

Syntax  object-names {
         mib-object-name;
     }

Hierarchy Level  [edit accounting-options mib-profile profile-name]

Release Information  Statement introduced in Junos OS Release 8.2.
                  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify the name of each MIB object for which MIB statistics are collected for an
accounting-data log file.

Options  mib-object-name—Name of a MIB object. You can specify more than one MIB object
         name.

Required Privilege Level  interface—To view this statement in the configuration.
                   interface-control—To add this statement to the configuration.

Related Documentation  • Configuring the MIB Profile

operation

Syntax  operation operation-name;

Hierarchy Level  [edit accounting-options mib-profile profile-name]

Release Information  Statement introduced in Junos OS Release 8.2.
                  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify the name of the operation used to collect MIB statistics for an accounting-data
log file.

Options  operation-name—Name of the operation to use. You can specify a get, get-next, or walk
         operation.
                   Default: walk

Required Privilege Level  interface—To view this statement in the configuration.
                   interface-control—To add this statement to the configuration.

Related Documentation  • Configuring the MIB Profile
password (Login)

Syntax

```plaintext
password {
  change-type (set-transitions | character-set);
  format (md5 | sha1);
  maximum-length length;
  minimum-changes number;
  minimum-length length;
  minimum-lower-cases number;
  minimum-numerics number;
  minimum-punctuations number;
  minimum-upper-cases number;
}
```

Hierarchy Level

[edit system login]

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure special requirements such as character length and encryption format for plain-text passwords. Newly created passwords must meet these requirements.

Using several password minimum requirement options will cause the `minimum-length` to be reset if the total sum of the required minimums exceeds the `minimum-length` setting.

The individual statements are explained separately.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Special Requirements for Junos OS Plain-Text Passwords
- Example: Changing the Requirements for Junos OS Plain-Text Passwords
### permissions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>permissions [ permissions ];</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit system login class]</td>
</tr>
<tr>
<td>Description</td>
<td>Configure the login access privileges to be provided on the router or switch.</td>
</tr>
<tr>
<td>Options</td>
<td><strong>permissions</strong>—Privilege type. For a list of permission flag types, see <em>Understanding Junos OS Access Privilege Levels</em>.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
| Related Documentation | • *Configuring Access Privilege Levels*  
• *user on page 462* |
radius-options (edit system)

Syntax

```plaintext
radius-options {
  attributes {
    nas-ip-address ip-address;
  }
  password-protocol mschap-v2;
}
```

Hierarchy Level [edit system]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2.
MS-CHAPv2 password protocol configuration option introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

NOTE: The radius-options statement is not available on QFabric systems.

Description

Configure RADIUS options for the NAS-IP address for outgoing RADIUS packets and password protocol used in RADIUS packets.

Options

- **nas-ip-address ip-address**—IP address of the network access server (NAS) that requests user authentication.
- **password-protocol mschap-v2**—Protocol MS-CHAPv2, used for password authentication and password changing.

Required Privilege

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Authentication
- Configuring RADIUS Authentication
retry-options

Syntax
retry-options {
  backoff-factor seconds;
  backoff-threshold number;
  maximum-time seconds;
  minimum-time seconds;
  tries-before-disconnect number;
}

Hierarchy Level [edit system login]

Release Information
Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
maximum-time option introduced in Junos OS Release 9.6.
maximum-time option introduced in Junos OS Release 9.6 for EX Series switches.

Description
Maximum number of times a user can attempt to enter a password while logging in through SSH or Telnet before being disconnected.

Required Privilege
Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
• Limiting the Number of User Login Attempts for SSH and Telnet Sessions
• rate-limit on page 1503
root-authentication

Syntax

```plaintext
root-authentication {
  (encrypted-password "password" | plain-text-password);
  ssh-dsa "public-key";
  ssh-ecdsa "public-key";
  ssh-rsa "public-key";
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure the authentication methods for the root-level user, whose username is `root`.

Options

- **encrypted-password "password"**—MD5 or other encrypted authentication. Specify the MD5 or other password. You can specify only one encrypted password.

  You cannot configure a blank password for encrypted-password using blank quotation marks (`""`). You must configure a password whose number of characters range from 1 through 128 characters and enclose the password in quotation marks.

- **plain-text-password**—Plain-text password. The CLI prompts you for the password and then encrypts it. The CLI displays the encrypted version, and the software places the encrypted version in its user database. You can specify only one plain-text password.

- **ssh-dsa "public-key"**—SSH version 2 authentication. Specify the DSA (SSH version 2) public key. You can specify one or more public keys.

- **ssh-rsa "public-key"**—SSH version 1 authentication. Specify the RSA (SSH version 1 and SSH version 2) public key. You can specify one or more public keys.

Required Privilege

- **admin**—To view this statement in the configuration.
- **admin-control**—To add this statement to the configuration.

Related Documentation

- Configuring the Root Password
- authentication on page 423
root-login

Syntax  root-login (allow | deny | deny-password);

Hierarchy Level  [edit system services ssh]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  Control user access through SSH.

Default  Allow user access through SSH.

Options  allow—Allow users to log in to the router or switch as root through SSH.

deny—Disable users from logging in to the router or switch as root through SSH.

deny-password—Allow users to log in to the router or switch as root through SSH when the authentication method (for example, RSA authentication) does not require a password.

Required Privilege  Level  admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation  • Configuring SSH Service for Remote Access to the Router or Switch
Routing-Engine Profile

Syntax

```
route-engine-profile profile-name { fields { field-name; } file filename; interval minutes; }
```

Hierarchy Level

[edit accounting-options]

Release Information


Description

Create a Routing Engine profile to collect selected Routing Engine statistics and write them to a file in the /var/log directory.

Options

- **profile-name**—Name of the Routing Engine statistics profile.
- The remaining statements are explained separately.

Required Privilege

- Interface—To view this statement in the configuration.
- Interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Routing Engine Profile
### size

**Syntax**

```
size bytes;
```

**Hierarchy Level**

```
[edit accounting-options file filename]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**


**Options**

- `bytes`—Maximum size of each log file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a log file (for example, `profilelog`) reaches its maximum size, it is renamed `profilelog.0`, then `profilelog.1`, and so on, until the maximum number of log files is reached. Then the oldest log file is overwritten. If you do not specify a size, the file is closed, archived, and renamed when the time specified for the transfer interval is exceeded.

**Syntax:**

```
x to specify bytes, xk to specify KB, xm to specify MB, xg to specify GB
```

**Range:** 256 KB through 1 GB

**Required Privilege**

- **Level**

```
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
```

**Related Documentation**

- Configuring the Maximum Size of the File

### source-classes

**Syntax**

```
source-classes { 
  source-class-name;
}
```

**Hierarchy Level**

```
[edit accounting-options class-usage-profile profile-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Specify the source classes for which statistics are collected.

**Options**

- `source-class-name`—Name of the source class to include in the class usage profile.

**Required Privilege**

- **Level**

```
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
```

**Related Documentation**

- Configuring a Class Usage Profile
### start-time (Log File Transfer)

**Syntax**
```
start-time time;
```

**Hierarchy Level**
```
[edit accounting-options file filename]
```

**Release Information**
- Statement introduced in Junos OS Release 8.2.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Specify the start time for transfer of an accounting-data log file.

**Options**
- **time**—Start time for file transfer.
  
  **Syntax:**
  ```
  YYYY-MM-DD.hh:mm
  ```

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- [Configuring the Start Time for File Transfer](#)
**tacplus-options**

**Syntax**

```plaintext
tacplus-options {
    (exclude-cmd-attribute | no-cmd-attribute-value);
    service-name service-name;
    timestamp-and-timezone;
}
```

**Hierarchy Level**

[edit system]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Options for `no-cmd-attribute-value` and `exclude-cmd-attribute` introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 11.1 for QFX Series.
Option for `timestamp-and-timezone` introduced in Junos OS Release 12.2.

**Description**

Configure TACACS+ options for authentication and accounting.

**Options**

- `exclude-cmd-attribute`—Exclude the `cmd` attribute value completely from start and stop accounting records to enable logging of accounting records in the correct log file on a TACACS+ server.

- `no-cmd-attribute-value`—Set the `cmd` attribute value to an empty string in the TACACS+ accounting start and stop requests to enable logging of accounting records in the correct log file on a TACACS+ server.

- `service-name service-name`—Name of the authentication service used when you configure multiple TACACS+ servers to use the same authentication service.

**Default:** `junos-exec`

- `timestamp-and-timezone`—Include this statement if you want start time, stop time, and timezone attributes included in start/stop accounting records.

**Required Privilege Level**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring TACACS+ Authentication](#)
- [Configuring TACACS+ System Accounting](#)
- [Junos OS Authentication Order for RADIUS, TACACS+, and Password Authentication](#)
- [Configuring TACACS+ Authentication](#)
- [Configuring TACACS+ System Accounting](#)
tacplus-server

Syntax
tacplus-server server-address {
    secret password;
    single-connection;
    source-address source-address;
    timeout seconds;
}

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the TACACS+ server.

Options server-address—Address of the TACACS+ authentication server.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation • Configuring TACACS+ Authentication
traceoptions (Address-Assignment Pool)

Syntax
```
traceoptions {
    file filename {
        files number;
        size maximum-file-size;
        match regex;
            (world-readable | no-world-readable);
    }
    flag address-assignment;
    flag all;
    flag configuration;
    flag framework;
    flag ldap;
    flag local-authentication;
    flag radius;
}
```

Hierarchy Level
[edit system processes general-authentication-service]

Release Information
Flag for tracing address-assignment pool operations introduced in Junos OS Release 9.0.
option-name option introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure tracing options.

Options
- `file filename`—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory `/var/log`.

- `files number`—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the `size` option and a filename.

- `Range`: 2 through 1000
- `Default`: 3 files

- `flag flag`—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. You can include the following flags:
  - `address-assignment`—All address-assignment events
  - `all`—All tracing operations
  - `configuration`—Configuration events
  - `framework`—Authentication framework events
  - `ldap`—LDAP authentication events
  - `local-authentication`—Local authentication events

Copyright © 2013, Juniper Networks, Inc.
- **radius**—RADIUS authentication events

**match regex**—(Optional) Refine the output to include lines that contain the regular expression.

**no-world-readable**—(Optional) Restrict access to the originator of the trace operation only.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

**Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB
**Range:** 10 KB through 1 GB
**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege**

- **Level**
  - admin—To view this statement in the configuration.
  - admin-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring Address-Assignment Pools*

---

**transfer-interval**

**Syntax**

```plaintext
transfer-interval minutes;
```

**Hierarchy Level**

```plaintext
[edit accounting-options file filename]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Specify the length of time the file remains open and receives new statistics before it is closed and transferred to an archive site.

**Options**

- **minutes**—Time the file remains open and receives new statistics before it is closed and transferred to an archive site.

  **Range:** 5 through 2880 minutes
  **Default:** 30 minutes

**Required Privilege**

- **Level**
  - interface—To view this statement in the configuration.
  - interface-control—To add this statement to the configuration.

**Related Documentation**

- *Configuring the Transfer Interval of the File*
uid

**Syntax**  
uid uid-value;

**Hierarchy Level**  
[edit system login user]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Numeric identifier associated with the user account name, either assigned by an administrator or assigned automatically when you commit the user configuration. It is used by applications that request numeric identifiers, such as some RADIUS queries or secure applications such as flow-tap monitoring.

**Options**  
uid-value—Number associated with the login account. This value must be unique on the router or switch.  
**Range:** 100 through 64000

**Required Privilege Level**  
admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration.

**Related Documentation**  
- Configuring Junos OS User Accounts
user (Access)

Syntax

```
user username {
  authentication {
    class class-name;
    (encrypted-password "password" | plain-text-password);
    full-name complete-name;
    load-key-file URL filename;
    ssh-dsa "public-key" <from hostname>;
    ssh-rsa "public-key" <from hostname>;
    uid uid-value;
  }
}
```

Hierarchy Level  [edit system login]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure access permission for individual users.

Options  The remaining statements are explained separately.

Required Privilege

- Level  admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Junos OS User Accounts
- class on page 425
Routine Monitoring

Managing Users (J-Web Procedure)

You can use the Users Configuration page for user information to add new users to an EX Series switch. For each account, you define a login name and password for the user and specify a login class for access privileges.

To configure users:

   The User Management page displays details of users, the authentication order, the RADIUS servers and TACACS servers present.

2. Click Edit.

3. Click any of the following options on the Users tab:
   - **Add**—Select this option to add a user. Enter details as described in Table 83 on page 464.
   - **Edit**—Select this option to edit an existing user’s details. Enter details as described in Table 83 on page 464.
   - **Delete**—Select this option to delete a user.

4. Click an option on the Authentication Methods and Order tab:
   - Authentication Order—Drag and drop the authentication type from the Available Methods section to the Selected Methods. Click the up or down buttons to modify the authentication order.
   - RADIUS server—Click one of the following options:
     - **Add**—Select this option to add an authentication server. Enter details as described in Table 84 on page 465.
- **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 84 on page 465.
- **Delete**—Select this option to delete an authentication server from the list.

- **TACACS server**—Click one of the following options:
  - **Add**—Select this option to add an authentication server. Enter details as described in Table 84 on page 465.
  - **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 84 on page 465.
  - **Delete**—Select this option to delete an authentication server from the list.

**NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

### Table 83: User Management Configuration Page Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Username (required)</td>
<td>Specifies the name that identifies the user.</td>
<td>Type the username. It must be unique within the switching platform. Do not include spaces, colons, or commas in the username.</td>
</tr>
<tr>
<td>User Id</td>
<td>Specifies the user identification.</td>
<td>Type the user’s ID.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Specifies the user’s full name.</td>
<td>Type the user’s full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.</td>
</tr>
<tr>
<td>Login Class (required)</td>
<td>Defines the user’s access privilege.</td>
<td>Select the user’s login class from the list:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- read-only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- super-user/superuser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- unauthorized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This list also includes any user-defined login classes.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the login password for this user.</td>
<td>Type the login password for this user. The login password must meet these criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- The password must be at least 6 characters long.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- It can include alphabetic, numeric, and special characters, but not control characters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- It must contain at least one change of case or character class.</td>
</tr>
</tbody>
</table>
### Table 83: User Management Configuration Page Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Password</td>
<td>Verifies the login password for this user.</td>
<td>Retype the login password for this user.</td>
</tr>
</tbody>
</table>

### Table 84: Add an Authentication Server

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the server.</td>
<td>Type the server’s 32-bit IP address, in dotted decimal notation.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password of the server.</td>
<td>Type the password of the server.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Verifies that the password of the server is entered correctly.</td>
<td>Retype the password of the server.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specifies the port with which the server is associated.</td>
<td>Type the port number.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Specifies the source address of the server.</td>
<td>Type the server’s 32-bit IP address, in dotted decimal notation.</td>
</tr>
<tr>
<td>Retry Attempts</td>
<td>Specifies the number of login retries allowed after a login failure.</td>
<td>Type the number.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only 1 retry is permitted for a TACACS server.</td>
<td></td>
</tr>
<tr>
<td>Time out</td>
<td>Specifies the time interval to wait before the connection to the server is closed.</td>
<td>Type the interval in seconds.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 415

**Operational Commands**
**request message**

**Syntax**

request message all message "text"
request message message "text" (terminal terminal-name | user user-name)

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display a message on the screens of all users who are logged in to the router or switch or on specific screens.

**Options**

- all—Display a message on the terminal of all users who are currently logged in.
- message "text"—Message to display.
- terminal terminal-name—Name of the terminal on which to display the message.
- user user-name—Name of the user to whom to direct the message.

**Required Privilege Level**

maintenance

**List of Sample Output**

request message message on page 466

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

request message message

user@host> request message message "Maintenance window in 10 minutes" user maria
Message from user@host on tty0 at 20:27 ...
Maintenance window in 10 minutes
EOF
show subscribers

Syntax
show subscribers
<detail | extensive | terse>
<aci-interface-set-name aci-interface-set-name>
<address address>
<agent-circuit-identifier agent-circuit-identifier-substring>
<client-type client-type>
<count>
<interface interface>
<logical-system logical-system>
<mac-address mac-address>
<physical-interface physical-interface-name>
<profile-name profile-name>
<routing-instance routing-instance>
<stacked-vlan-id stacked-vlan-id>
<subscriber-state subscriber-state>
<user-name user-name>
<vci vci-identifier>
<vpi vpi-identifier>
<vlan-id vlan-id>

Release Information
Command introduced in Junos OS Release 9.3.
Command introduced in Junos OS Release 9.3 for EX Series switches.
client-type, mac-address, subscriber-state, and extensive options introduced in Junos OS Release 10.2.
count option usage with other options introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 11.1 for the QFX Series.
The physical-interface and user-name options introduced in Junos OS Release 12.3.
Options vci and vpi introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
Options vci and vpi supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description
Display information for active subscribers.

Options
detail | extensive | terse—(Optional) Display the specified level of output.

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.168.17.1). If you specify the IP address as a prefix with a netmask (for example, 192.168.171/32), the router displays a message that the IP address is invalid, and rejects the command.
**agent-circuit-identifier-substring**—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified substring.

**client-type**—(Optional) Display subscribers whose client type matches the specified client type (DHCP, L2TP, PPP, PPPOE, VLAN, or static).

**count**—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the count option alone or with the address, client-type, interface, logical-system, mac-address, profile-name, routing-instance, stacked-vlan-id, subscriber-state, or vlan-id options.

**id**—(Optional) Display a specific subscriber session whose session ID matches the specified subscriber ID. You can display subscriber IDs by using the show subscribers extensive or the show subscribers interface extensive commands.

**interface**—(Optional) Display subscribers whose interface matches the specified interface.

**logical-system**—(Optional) Display subscribers whose logical system matches the specified logical system.

**mac-address**—(Optional) Display subscribers whose MAC address matches the specified MAC address.

**physical-interface-name**—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

**profile-name**—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

**routing-instance**—(Optional) Display subscribers whose routing instance matches the specified routing instance.

**subscriber-state**—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

**user-name**—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

**vci-identifier**—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is 0 through 255.

**vpi-identifier**—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is 0 through 65535.

**vlan-id**—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID.

**stacked-vlan-id**—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.
NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>Related Documentation</th>
</tr>
</thead>
</table>
| view                     | show subscribers summary
                          | Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration

List of Sample Output

- show subscribers (IPv4) on page 473
- show subscribers (IPv6) on page 473
- show subscribers (IPv4 and IPv6 Dual Stack) on page 473
- show subscribers (LNS on MX Series Routers) on page 474
- show subscribers (L2TP Switched Tunnels) on page 474
- show subscribers client-type dhcp detail on page 474
- show subscribers count on page 474
- show subscribers address detail (IPv6) on page 474
- show subscribers detail (IPv4) on page 475
- show subscribers detail (IPv6) on page 475
- show subscribers detail (IPv6 Static Demux Interface) on page 476
- show subscribers detail (L2TP LNS Subscribers on MX Series Routers) on page 476
- show subscribers detail (L2TP Switched Tunnels) on page 476
- show subscribers detail (Tunneled Subscriber) on page 477
- show subscribers detail (IPv4 and IPv6 Dual Stack) on page 477
- show subscribers detail (ACI Interface Set Session) on page 478
- show subscribers detail (PPPoE Subscriber Session with ACI Interface Set) on page 478
- show subscribers extensive on page 478
- show subscribers extensive (RPF Check Fail Filter) on page 479
- show subscribers extensive (L2TP LNS Subscribers on MX Series Routers) on page 479
- show subscribers extensive (IPv4 and IPv6 Dual Stack) on page 479
- show subscribers extensive (Effective Shaping-Rate) on page 480
- show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set) on page 481
- show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring) on page 481
- show subscribers interface extensive on page 482
- show subscribers logical-system terse on page 482
- show subscribers physical-interface count on page 483
- show subscribers routing-instance inst1 count on page 483
- show subscribers stacked-vlan-id detail on page 483
- show subscribers stacked-vlan-id vlan-id detail (Combined Output) on page 483
- show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface) on page 483
- show subscribers user-name detail on page 483
- show subscribers vlan-id on page 484
Output Fields

Table 85 on page 470 lists the output fields for the show subscribers command. Output fields are listed in the approximate order in which they appear.

**Table 85: show subscribers Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface.</td>
</tr>
<tr>
<td></td>
<td>The * character indicates a continuation of addresses for the same session.</td>
</tr>
<tr>
<td>IP Address/VLAN ID</td>
<td>Subscriber IP address or VLAN ID associated with the subscriber in the form tpid.vlan-id</td>
</tr>
<tr>
<td></td>
<td>No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is <strong>Tunnel-switched</strong>.</td>
</tr>
<tr>
<td>UserName</td>
<td>Name of subscriber.</td>
</tr>
<tr>
<td>LS:RI</td>
<td>Logical system and routing instance associated with the subscriber.</td>
</tr>
<tr>
<td>Type</td>
<td>Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Subscriber IPv4 address.</td>
</tr>
<tr>
<td>IP Netmask</td>
<td>Subscriber IP netmask.</td>
</tr>
<tr>
<td>Primary DNS Address</td>
<td>IP address of primary DNS server.</td>
</tr>
<tr>
<td>Secondary DNS Address</td>
<td>IP address of secondary DNS server.</td>
</tr>
<tr>
<td>Primary WINS Address</td>
<td>IP address of primary WINS server.</td>
</tr>
<tr>
<td>Secondary WINS Address</td>
<td>IP address of secondary WINS server.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Subscriber IPv6 address, or multiple addresses.</td>
</tr>
<tr>
<td>IPv6 Prefix</td>
<td>Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.</td>
</tr>
<tr>
<td>IPv6 User Prefix</td>
<td>IPv6 prefix obtained through ND/RA.</td>
</tr>
<tr>
<td>IPv6 Address Pool</td>
<td>Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.</td>
</tr>
<tr>
<td>IPv6 Network Prefix Length</td>
<td>Length of the network portion of the IPv6 address.</td>
</tr>
<tr>
<td>IPv6 Prefix Length</td>
<td>Length of the subscriber IPv6 prefix.</td>
</tr>
</tbody>
</table>
Table 85: show subscribers Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical System</td>
<td>Logical system associated with the subscriber.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Routing instance associated with the subscriber.</td>
</tr>
<tr>
<td>Interface Type</td>
<td>Whether the subscriber interface is <em>Static</em> or <em>Dynamic</em>.</td>
</tr>
<tr>
<td>Interface Set</td>
<td>Internally generated name of the dynamic ACI interface set used by the subscriber session.</td>
</tr>
<tr>
<td>Interface Set Type</td>
<td>Interface type of the ACI interface set: <em>Dynamic</em>. This is the only ACI interface set type currently supported.</td>
</tr>
<tr>
<td>Interface Set Session ID</td>
<td>Identifier of the dynamic ACI interface set entry in the session database.</td>
</tr>
<tr>
<td>Underlying Interface</td>
<td>Name of the underlying interface for the subscriber session.</td>
</tr>
<tr>
<td>Dynamic Profile Name</td>
<td>Dynamic profile used for the subscriber.</td>
</tr>
<tr>
<td>Dynamic Profile Version</td>
<td>Version number of the dynamic profile used for the subscriber.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address associated with the subscriber.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the subscriber session <em>(Init, Configured, Active, Terminating, Tunneled)</em>.</td>
</tr>
<tr>
<td>L2TP State</td>
<td>Current state of the L2TP session, <em>Tunneled</em> or <em>Tunnel-switched</em>. When the value is <em>Tunnel-switched</em>, two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.</td>
</tr>
<tr>
<td>Tunnel switch Profile Name</td>
<td>Name of the L2TP tunnel switch profile that initiates tunnel switching.</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>IP address of the local gateway (LAC).</td>
</tr>
<tr>
<td>Remote IP Address</td>
<td>IP address of the remote peer (LNS).</td>
</tr>
<tr>
<td>VLAN Id</td>
<td>VLAN ID associated with the subscriber in the form tpid.vlan-id.</td>
</tr>
<tr>
<td>Stacked VLAN id</td>
<td>Stacked VLAN ID associated with the subscriber in the form tpid.vlan-id.</td>
</tr>
<tr>
<td>RADIUS Accounting ID</td>
<td>RADIUS accounting ID associated with the subscriber.</td>
</tr>
<tr>
<td>Agent Circuit ID</td>
<td>Option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.</td>
</tr>
<tr>
<td>Agent Remote ID</td>
<td>Option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.</td>
</tr>
<tr>
<td>DHCP Relay IP Address</td>
<td>IP address used by the DHCP relay agent.</td>
</tr>
</tbody>
</table>
## Table 85: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM VPI</td>
<td>(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber’s physical interface.</td>
</tr>
<tr>
<td>ATM VCI</td>
<td>(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.</td>
</tr>
<tr>
<td>Login Time</td>
<td>Date and time at which the subscriber logged in.</td>
</tr>
<tr>
<td>Effective shaping-rate</td>
<td>Actual downstream traffic shaping rate for the subscriber, in kilobits per second.</td>
</tr>
<tr>
<td>IPv4 rpf-check Fail Filter Name</td>
<td>Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.</td>
</tr>
<tr>
<td>IPv6 rpf-check Fail Filter Name</td>
<td>Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.</td>
</tr>
<tr>
<td>DHCP Options</td>
<td>len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.</td>
</tr>
<tr>
<td>Session ID</td>
<td>ID number for a subscriber service session.</td>
</tr>
<tr>
<td>Underlying Session ID</td>
<td>For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.</td>
</tr>
<tr>
<td>Service Sessions</td>
<td>Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.</td>
</tr>
<tr>
<td>Service Session Name</td>
<td>Service session profile name.</td>
</tr>
<tr>
<td>Session Timeout (seconds)</td>
<td>Number of seconds of access provided to the subscriber before the session is automatically terminated.</td>
</tr>
<tr>
<td>Idle Timeout (seconds)</td>
<td>Number of seconds subscriber can be idle before the session is automatically terminated.</td>
</tr>
<tr>
<td>IPv6 Delegated Address Pool</td>
<td>Name of the pool used for DHCPv6 prefix delegation.</td>
</tr>
<tr>
<td>IPv6 Delegated Network Prefix Length</td>
<td>Length of the prefix configured for the IPv6 delegated address pool.</td>
</tr>
<tr>
<td>IPv6 Interface Address</td>
<td>Address assigned by the Framed-Ipv6-Prefix AAA attribute.</td>
</tr>
<tr>
<td>IPv6 Framed Interface Id</td>
<td>Interface ID assigned by the Framed-Interface-Id AAA attribute.</td>
</tr>
<tr>
<td>ADF IPv4 Input Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
</tbody>
</table>
### Table 85: show subscribers Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADF IPv4 Output Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
<tr>
<td>ADF IPv6 Input Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
<tr>
<td>ADF IPv6 Output Filter Name</td>
<td>Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.</td>
</tr>
<tr>
<td>IPv4 Input Filter Name</td>
<td>Name assigned to the IPv4 input filter (client or service session).</td>
</tr>
<tr>
<td>IPv4 Output Filter Name</td>
<td>Name assigned to the IPv4 output filter (client or service session).</td>
</tr>
<tr>
<td>IPv6 Input Filter Name</td>
<td>Name assigned to the IPv6 input filter (client or service session).</td>
</tr>
<tr>
<td>IPv6 Output Filter Name</td>
<td>Name assigned to the IPv6 output filter (client or service session).</td>
</tr>
<tr>
<td>IFL Input Filter Name</td>
<td>Name assigned to the logical interface input filter (client or service session).</td>
</tr>
<tr>
<td>IFL Output Filter Name</td>
<td>Name assigned to the logical interface output filter (client or service session).</td>
</tr>
</tbody>
</table>

### Sample Output

#### show subscribers (IPv4)

```
user@host> show subscribers
Interface               IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824     100                                    default:default
demux0.1073741824       100.0.0.10           WHOLESALER-CLIENT default:default
demux0.1073741825       101.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826       102.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

#### show subscribers (IPv6)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name           LS:RI
ge-1/0/0.0         2001::c0:0:0:0/74    WHOLESALER-CLIENT   default:default
*             2002::1/128          subscriber-25       default:default
```

#### show subscribers (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers
Interface           IP Address/VLAN ID         User Name
LS:RI
 demux0.1073741834   0x8100.1002 0x8100.1
 demux0.1073741835   0x8100.1001 0x8100.1
 pp0.1073741836      61.1.1.1                 dualstackuser1@ISP1.com
```
show subscribers (LNS on MX Series Routers)
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name         LS:RI
si-4/0/0.1         192.168.4.1          xyz@example.com   default:default

show subscribers (L2TP Switched Tunnels)
user@host> show subscribers
Interface           IP Address/VLAN ID    User Name              LS:RI
si-2/1/0.1073741842 Tunnel-switched       ap@lts.com        default:default
si-2/1/0.1073741843 Tunnel-switched       ap@lts.com        default:default

show subscribers client-type dhcp detail
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 100.20.10.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:94:00:01:f3
State: Active
Radius Accounting ID: jnpr :2560
Login Time: 2009-08-25 14:43:56 PDT

show subscribers count
user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188

show subscribers address detail (IPv6)
user@host> show subscribers address 100.16.12.137 detail
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 100.16.12.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 1016:0:0:c88::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:0d:02:01:00:01
Session Timeout (seconds): 3162400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: jnpr demux0.8201:6544
Session ID: 6544
Agent Circuit ID: ifl3720
Agent Remote ID: ifl3720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1

show subscribers detail (IPv4)

user@host> show subscribers detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Primary DNS Address: 192.168.17.1
Secondary DNS Address: 192.168.17.2
Primary WINS Address: 192.168.22.1
Secondary WINS Address: 192.168.22.2
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Session Timeout (seconds): 3600
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 21 2c
Service Sessions: 2

show subscribers detail (IPv6)

user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00

show subscribers detail (IPv6 Static Demux Interface)

user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: demux0.1@jnpr.net
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

user@host> show subscribers detail
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001

show subscribers detail (L2TP Switched Tunnels)

user@host> show subscribers detail
Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.50.1.1
Remote IP Address: 192.168.20.3
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.30.1.1
Remote IP Address: 172.20.1.10
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST

show subscribers detail (Tunneled Subscriber)

user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512

show subscribers detail (IPv4 and IPv6 Dual Stack)

user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST
Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
show subscribers detail (ACI Interface Set Session)

user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.5
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:64:39:01:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST

show subscribers extensive

user@host> show subscribers extensive
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48

show subscribers extensive (RPF Check Fail Filter)

user@host> show subscribers extensive
...
Type: VLAN
  Logical System: default
  Routing Instance: default
  Interface: ae0.1073741824
  Interface type: Dynamic
  Dynamic Profile Name: vlan-prof
  State: Active
  Session ID: 9
  VLAN Id: 100
  Login Time: 2011-08-26 08:17:00 PDT
  IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
  IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

user@host> show subscribers extensive
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out

show subscribers extensive (IPv4 and IPv6 Dual Stack)

user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
show subscribers extensive (Effective Shaping-Rate)

user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
Effective shaping-rate: 31000000k
...

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
**Interface Set Type**: Dynamic  
**Interface Set Session ID**: 13  
**Underlying Interface**: ge-1/0/0.4001  
**Dynamic Profile Name**: aci-vlan-pppoe-profile  
**Dynamic Profile Version**: 1  
**MAC Address**: 00:00:65:26:01:02  
**State**: Active  
**Radius Accounting ID**: 14  
**Session ID**: 14  
**Agent Circuit ID**: aci-ppp-vlan-10  
**Login Time**: 2012-03-12 10:41:57 PDT  

**show subscribers interface extensive**

```
user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: test1@test.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST
Type: DHCP
User Name: test1@test.com
IP Address: 172.16.200.6
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

**show subscribers logical-system terse**

```
user@host> show subscribers logical-system test1 terse
```
show subscribers physical-interface count

user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998

show subscribers routing-instance inst1 count

user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183

show subscribers stacked-vlan-id detail

user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT

show subscribers user-name detail

user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
IP Address: 100.0.0.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
show subscribers vlan-id

user@host> show subscribers vlan-id 100
Interface       IP Address              User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825

show subscribers vlan-id detail

user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

dmshow subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

user@host> show subscribers vpi 40 vci 50 extensive
Type: PPPoE
User Name: testuser
IP Address: 100.0.0.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:65:23:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
Troubleshooting Procedures

- Troubleshooting Loss of the Root Password on page 485

**Troubleshooting Loss of the Root Password**

**Problem**  
If you forget the root password for the switch, you can use the password recovery procedure to reset the root password.

**Solution**  
To recover the root password:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.

2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port on the back of the switch. See Figure 1 on page 379

**Figure 2: Connecting to the Console Port on the EX Series Switch**

3. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate COM port to use (for example, COM1).
4. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.

6. When the following prompt appears, press the Spacebar to access the switch's bootstrap loader command prompt:
   Hit [Enter] to boot immediately, or space bar for command prompt.
   Booting [kernel] in 1 second...

7. At the following prompt, type `boot -s` to start up the system in single-user mode:
   ```
   loader> boot -s
   ```

8. At the following prompt, type `recovery` to start the root password recovery procedure:
   ```
   Enter full path name of shell or 'recovery' for root password recovery or RETURN for /bin/sh: recovery
   ```
   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

9. Enter configuration mode in the CLI:
   ```
   user@switch> configure
   ```

10. Set the root password. For example:
    ```
        user@switch# set system root-authentication plain-text-password
    ```

11. At the following prompt, enter the new root password. For example:
    ```
        New password: juniper!
        Retype new password:
    ```

12. At the second prompt, reenter the new root password.

13. If you are finished configuring the network, commit the configuration.
    ```
        root@switch# commit
        commit complete
    ```

14. Exit configuration mode in the CLI.
    ```
        root@switch# exit
    ```

15. Exit operational mode in the CLI.
    ```
        root@switch> exit
    ```

16. At the prompt, enter `y` to reboot the switch.
    ```
        Reboot the system? [y/n] y
    ```

Related Documentation
- Connecting and Configuring an EX Series Switch (CLI Procedure)
• **Connecting and Configuring an EX Series Switch (J-Web Procedure)**

• For information about configuring an encrypted root password, configuring SSH keys to authenticate root logins, and configuring special requirements for plain-text passwords, see the *Junos OS System Basics Configuration Guide*. 
PART 6

Configuration and File Management

- Overview on page 491
- Configuration on page 501
- Administration on page 523
- Troubleshooting Procedures on page 565
CHAPTER 14

Overview

- Software Overview on page 491
- Configuration Files Overview on page 493

Software Overview

- Understanding Software Infrastructure and Processes on page 491

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 491
- Junos OS Processes on page 492

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.

- Routing Engine—Provides three main functions:
  - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network.
- Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

Junos OS Processes

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 61 on page 112 describes the primary Junos OS processes.

Table 86: Junos OS Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis process</td>
<td>chassisd</td>
<td>Detects hardware on the system that is used to configure network interfaces. Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered. Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</td>
</tr>
<tr>
<td>Ethernet switching process</td>
<td>eswd</td>
<td>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces. Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>Forwarding process</td>
<td>pfem</td>
<td>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</td>
</tr>
<tr>
<td>Interface process</td>
<td>dcd</td>
<td>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</td>
</tr>
<tr>
<td>Management process</td>
<td>mgd</td>
<td>Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the switch. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</td>
</tr>
<tr>
<td>Routing protocol process</td>
<td>rpd</td>
<td>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</td>
</tr>
</tbody>
</table>
Configuration Files Overview

- Understanding Configuration Files for EX Series Switches on page 493
- Using the CLI Viewer in the J-Web Interface to View Configuration Text on page 494
- Using the CLI Editor in the J-Web Interface to Edit Configuration Text on page 494
- Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text on page 494
- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Understanding Autoinstallation of Configuration Files on page 497
- Configuration Files Terms on page 499

Understanding Configuration Files for EX Series Switches

A configuration file stores the complete configuration of a switch. The current configuration of a switch is called the active configuration. You can alter this current configuration and you can also return to a previous configuration or to a rescue configuration. For more information, see “Configuration Files Terms” on page 499.

Juniper Networks Junos operating system (Junos OS) saves the 50 most recently committed configuration files on the switch so that you can return to a previous configuration. The configuration files are named:

- juniper.conf.gz—The current active configuration.
- juniper.conf.1.gz to juniper.conf.49.gz—Rollback configurations.

To make changes to the configuration file, you have to work in the configuration mode in the CLI or use the configuration tools in the J-Web interface. When making changes to a configuration file, you are viewing and changing the candidate configuration file. The candidate configuration allows you to make configuration changes without causing operational changes to the active configuration or causing potential damage to your current network operations. Once you commit the changes made to the candidate configuration, the system updates the active configuration.
Using the CLI Viewer in the J-Web Interface to View Configuration Text

To view the entire configuration file contents in text format, select Configure > CLITools > CLI Viewer. The main pane displays the configuration in text format.

Each level in the hierarchy is indented to indicate each statement’s relative position in the hierarchy. Each level is generally set off with braces, with an open brace ({) at the beginning of each hierarchy level and a closing brace (}) at the end. If the statement at a hierarchy level is empty, the braces are not displayed. Each leaf statement ends with a semicolon (;), as does the last statement in the hierarchy.

This indented representation is used when the configuration is displayed or saved as an ASCII file. However, when you load an ASCII configuration file, the format of the file is not so strict. The braces and semicolons are required, but the indentation and use of new lines are not required in ASCII configuration files.

Related Documentation
- Understanding J-Web Configuration Tools on page 392

Using the CLI Editor in the J-Web Interface to Edit Configuration Text

Use the CLI Editor to edit configuration if you know the Junos OS CLI or prefer a command interface.

To edit the entire configuration in text format:

CAUTION: We recommend that you use this method to edit and commit the configuration only if you have experience editing configurations through the CLI.

1. Select Configure > CLITools > CLI Editor. The main pane displays the configuration in a text editor.

2. Navigate to the hierarchy level you want to edit.

   You can edit the candidate configuration using standard text editor operations—insert lines (by using the Enter key), delete lines, and modify, copy, and paste text.

3. Click Commit to load and commit the configuration.

   The switching platform checks the configuration for the correct syntax before committing it.

Related Documentation
- CLI User Interface Overview on page 387
- Understanding J-Web Configuration Tools on page 392

Using the Point and Click CLI Tool in the J-Web Interface to Edit Configuration Text

To edit the configuration on a series of pages of clickable options that steps you through the hierarchy, select Configure > CLITools > Point&Click CLI. The side pane displays the
top level of the configured hierarchy, and the main pane displays configured hierarchy options and the Icon Legend.

To expand or hide the hierarchy of all the statements in the side pane, click **Expand all** or **Hide all**. To expand or hide an individual statement in the hierarchy, click the expand (+) or collapse (−) icon to the left of the statement.

**TIP:** Only those statements included in the committed configuration are displayed in the hierarchy.

The configuration information in the main pane consists of configuration options that correspond to configuration statements. Configuration options that contain subordinate statements are identified by the term **Nested**.

To include, edit, or delete statements in the candidate configuration, click one of the links described in Table 87 on page 495. Then specify configuration information by typing in a field, selecting a value from a list, or clicking a check box (toggle).

### Table 87: J-Web Edit Point & Click Configuration Links

<table>
<thead>
<tr>
<th>Link</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add new entry</td>
<td>Displays fields and lists for a statement identifier, allowing you to add a new identifier to a statement.</td>
</tr>
<tr>
<td>Configure</td>
<td>Displays information for a configuration option that has not been configured, allowing you to include a statement.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the corresponding statement or identifier from the configuration. All subordinate statements and identifiers contained within a deleted statement are also discarded.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays information for a configuration option that has already been configured, allowing you to edit a statement.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Displays fields and lists for an existing statement identifier, allowing you to edit the identifier.</td>
</tr>
</tbody>
</table>

As you navigate through the configuration, the hierarchy level is displayed at the top of the main pane. You can click a statement or identifier in the hierarchy to display the corresponding configuration options in the main pane.

The main pane includes icons that display information about statements and identifiers when you place your cursor over them. Table 88 on page 495 describes these icons.

### Table 88: J-Web Edit Point & Click Configuration Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Displays a comment about a statement.</td>
</tr>
<tr>
<td>I</td>
<td>Indicates that a statement is inactive.</td>
</tr>
<tr>
<td>M</td>
<td>Indicates that a statement has been added or modified but has not been committed.</td>
</tr>
</tbody>
</table>
Table 88: J-Web Edit Point & Click Configuration Icons (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Indicates that the statement or identifier is required in the configuration.</td>
</tr>
<tr>
<td>?</td>
<td>Provides online help information.</td>
</tr>
</tbody>
</table>

After typing or selecting your configuration edits, click a button in the main pane (described in Table 89 on page 496) to apply your changes or cancel them, refresh the display, or discard parts of the candidate configuration. An updated configuration does not take effect until you commit it.

Table 89: J-Web Edit Point & Click Configuration Buttons

<table>
<thead>
<tr>
<th>Button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>Updates the display with any changes to the configuration made by other users.</td>
</tr>
<tr>
<td>Commit</td>
<td>Verifies edits and applies them to the current configuration file running on the switch.</td>
</tr>
<tr>
<td>Discard</td>
<td>Removes edits applied to or deletes existing statements or identifiers from the candidate configuration.</td>
</tr>
</tbody>
</table>

### Understanding Automatic Refreshing of Scripts on EX Series Switches

You can automatically refresh `commit`, `event`, and `op` scripts using operational mode commands on EX Series switches. The commands are:

- `request system scripts refresh-from commit`
- `request system scripts refresh-from event`
- `request system scripts refresh-from op`

The existing Junos operating system (Junos OS) command-line interface (CLI) `refresh` and `refresh-from` configuration mode statements have been extended to work with Junos XML management protocol and NETCONF XML management protocol sessions.

**Related Documentation**
- CLI User Interface Overview on page 387
- Understanding J-Web Configuration Tools on page 392
- Understanding Autoinstallation of Configuration Files on page 497
- CLI User Interface Overview on page 387
- Junos OS NETCONF XML Management Protocol Guide
Understanding Autoinstallation of Configuration Files

Autoinstallation is the automatic configuration of a device over the network from a preexisting configuration file that you create and store on a configuration server—typically a Trivial File Transfer Protocol (TFTP) server. You can use autoinstallation to configure new devices automatically and to deploy multiple devices from a central location in the network.

You enable autoinstallation so that the switches in your network implement autoinstallation when they are powered on. To configure autoinstallation, you specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

This topic describes:

• Typical Uses for Autoinstallation on page 497
• Autoinstallation Configuration Files and IP Addresses on page 497
• Typical Autoinstallation Process on a New Switch on page 498

Typical Uses for Autoinstallation

Typical uses for autoinstallation of the software include:

• To deploy and update multiple devices from a central location in the network.
• To update a device—Autoinstallation occurs when a device that has been manually configured for autoinstallation is powered on.

Autoinstallation Configuration Files and IP Addresses

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the switch.

You can set up the following configuration files for autoinstallation on the switch:

• network.conf—Default configuration file for autoinstallation, in which you specify IP addresses and associated hostnames for devices on the network.
• switch.conf—Default configuration file for autoinstallation with a minimum configuration sufficient for you to telnet to the device and configure it manually.
• hostname.conf—Host-specific configuration file for autoinstallation on a device that contains all the configuration information necessary for the switch. In the filename, hostname is replaced with the hostname assigned to the switch.

If the server with the autoinstallation configuration file is not on the same LAN segment as the new device, or if a specific device is required by the network, you must configure an intermediate device directly attached to the new switch, through which the new switch can send TFTP, Boot Protocol (BOOTP), and Domain Name System (DNS) requests. In this case, you specify the IP address of the intermediate device as the location to receive TFTP requests for autoinstallation.
Typical Autoinstallation Process on a New Switch

When the switch configured for autoinstallation is powered on, it performs the following autoinstallation tasks:

1. The switch sends out DHCP or BOOTP requests on each connected interface simultaneously to obtain an IP address.
   
   If a DHCP server responds to these requests, it provides the switch with some or all of the following information:
   
   - An IP address and subnet mask for the autoinstallation interface.
   - The location of the (typically) TFTP server, Hypertext Transfer Protocol (HTTP) server, or FTP server on which the configuration file is stored.
   - The name of the configuration file to be requested from the TFTP server.
   - The IP address or hostname of the TFTP server.
   
   If the DHCP server provides the server’s hostname, a DNS server must be available on the network to resolve the name to an IP address.
   
   - The IP address of an intermediate device if the configuration server is on a different LAN segment from the switch.

2. After the switch acquires an IP address, the autoinstallation process on the switch attempts to download a configuration file in the following ways:
   
   a. If the DHCP server specifies the host-specific configuration file `hostname.conf`, the switch uses that filename in the TFTP server request. The autoinstallation process on the new switch makes three unicast TFTP requests for `hostname.conf`. If these attempts fail, the switch broadcasts three requests to any available TFTP server for the file.
   
   b. If the switch does not locate a `hostname.conf` file, the autoinstallation process sends three unicast TFTP requests for a `network.conf` file that contains the switch’s hostname-to-IP-address mapping information. If these attempts fail, the switch broadcasts three requests to any available TFTP server for the file.
   
   c. If the switch fails to find a `network.conf` file that contains a hostname entry for the switch, the autoinstallation process sends out a DNS request and attempts to resolve the switch’s IP address to a hostname.
   
   d. If the switch determines its hostname, it sends a TFTP request for the `hostname.conf` file.
   
   e. If the switch is unable to map its IP address to a hostname, it sends TFTP requests for the default configuration file `switch.conf`. The TFTP request procedure is the same as for the `network.conf` file.

3. After the switch locates a configuration file on a TFTP server, the autoinstallation process downloads the file, installs the file on the switch, and commits the configuration.
## Configuration Files Terms

Table 90 on page 499 lists the various configuration file terms used for EX Series switches and their definitions.

### Table 90: Configuration File Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>active configuration</td>
<td>The current committed configuration of a switch.</td>
</tr>
<tr>
<td>candidate configuration</td>
<td>A working copy of the configuration that allows users to make configurational changes without causing any operational changes until this copy is committed.</td>
</tr>
<tr>
<td>configuration group</td>
<td>Group of configuration statements that can be inherited by the rest of the configuration.</td>
</tr>
<tr>
<td>commit a configuration</td>
<td>Have the candidate configuration checked for proper syntax, activated, and marked as the current configuration file running on the switching platform.</td>
</tr>
<tr>
<td>configuration hierarchy</td>
<td>The Junos OS configuration consists of a hierarchy of statements. There are two types of statements: container statements, which contain other statements, and leaf statements, which do not contain other statements. All the container and leaf statements together form the configuration hierarchy.</td>
</tr>
<tr>
<td>default configuration</td>
<td>The default configuration contains the initial values set for each configuration parameter when a switch is shipped.</td>
</tr>
<tr>
<td>rescue configuration</td>
<td>Well-known configuration that recovers a switch from a configuration that denies management access. You set a current committed configuration to be the rescue configuration through the J-Web interface or CLI.</td>
</tr>
<tr>
<td>roll back a configuration</td>
<td>Return to a previously committed configuration.</td>
</tr>
</tbody>
</table>

### Related Documentation

- Configuring Autoinstallation of Configuration Files (CLI Procedure) on page 509
- Connecting and Configuring an EX Series Switch (CLI Procedure)
- Connecting and Configuring an EX Series Switch (J-Web Procedure)
- Configuration Files Terms on page 499

---

Copyright © 2013, Juniper Networks, Inc.
• Reverting to the Rescue Configuration for the EX Series Switch on page 507
• Understanding Configuration Files for EX Series Switches on page 493
CHAPTER 15

Configuration

- Configuration Tasks on page 501
- Configuration Statements on page 513

Configuration Tasks

- Uploading a Configuration File (CLI Procedure) on page 501
- Uploading a Configuration File (J-Web Procedure) on page 503
- Loading a Previous Configuration File (CLI Procedure) on page 503
- Reverting to the Default Factory Configuration for the EX Series Switch on page 504
- Reverting to the Rescue Configuration for the EX Series Switch on page 507
- Setting or Deleting the Rescue Configuration (CLI Procedure) on page 508
- Setting or Deleting the Rescue Configuration (J-Web Procedure) on page 509
- Configuring Autoinstallation of Configuration Files (CLI Procedure) on page 509
- Using the Commit Options to Commit Configuration Changes (J-Web Procedure) on page 511

Uploading a Configuration File (CLI Procedure)

You can create a configuration file on your local system, copy the file to the EX Series switch and then load the file into the CLI. After you have loaded the configuration file, you can commit it to activate the configuration on the switch. You can also edit the configuration interactively using the CLI and commit it at a later time.

To upload a configuration file from your local system:

1. Create the configuration file using a text editor such as Notepad, making sure that the syntax of the configuration file is correct. For more information about testing the syntax of a configuration file see the Junos OS System Basics and Services Command Reference.

2. In the configuration text file, use an option to perform the required action when the file is loaded. Table 91 on page 502 lists and describes some options for the load command.
Table 91: Options for the load command

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>merge</strong></td>
<td>Combines the current active configuration and the configuration in <em>filename</em> or the one that you type at the terminal. A <em>merge</em> operation is useful when you are adding a new section to an existing configuration. If the active configuration and the incoming configuration contain conflicting statements, the statements in the incoming configuration override those in the active configuration.</td>
</tr>
<tr>
<td><strong>override</strong></td>
<td>Discards the current candidate configuration and loads the configuration in <em>filename</em> or the one that you type at the terminal. When you use the <em>override</em> option and commit the configuration, all system processes reparse the configuration. You can use the <em>override</em> option at any level of the hierarchy.</td>
</tr>
</tbody>
</table>
| **replace** | Searches for the *replace* tags, deletes the existing statements of the same name, if any, and replaces them with the incoming configuration. If there is no existing statement of the same name, the *replace* operation adds the statements marked with the *replace* tag to the active configuration. 

*NOTE:* For this operation to work, you must include *replace* tags in the text file or in the configuration you type at the terminal. |

3. Press Ctrl+A to select all the text in the configuration file.
4. Press Ctrl+C to copy the contents of the configuration text file to the Clipboard.
5. Log in to the switch using your username and password.
6. To enter configuration mode:
   ```
   user@switch> configure
   ```
   You will see this output, with the hash or pound mark indicating configuration mode.
   ```
   Entering configuration mode
   [edit]
   user@switch#
   ```
7. Load the configuration file:
   ```
   [edit]
   user@switch# load merge terminal
   ```
8. At the cursor, paste the contents of the Clipboard using the mouse and the Paste icon:
   ```
   [edit]
   user@switch# load merge terminal
   [Type "D at a new line to end input]
   >Cursor is here. Paste the contents of the clipboard here<
   ```
10. Press Ctrl+D to set the end-of-file marker.

To view results of the configuration steps before committing the configuration, type the *show* command at the user prompt.

To commit these changes to the active configuration, type the *commit* command at the user prompt. You can also edit the configuration interactively using the CLI and commit it at a later time.
Uploading a Configuration File (J-Web Procedure)

You can create a configuration file on your local system, copy the file to the EX Series switch and then load the file into the CLI. After you have loaded the configuration file, you can commit it to activate the configuration on the switch. You can also edit the configuration interactively using the CLI and commit it at a later time.

To upload a configuration file from your local system:

1. Select **Maintain > Config Management > Upload**.
   The main pane displays the File to Upload box.

2. Specify the name of the file to upload using one of the following methods:
   - Type the absolute path and filename in the File to Upload box.
   - Click **Browse** to navigate to the file.

3. Click **Upload and Commit** to upload and commit the configuration.
   The switch checks the configuration for the correct syntax before committing it.

Loading a Previous Configuration File (CLI Procedure)

You can return to a previously committed configuration file if you need to revert to a previous configuration. The EX Series switch saves the last 50 committed configurations, including the rollback number, date, time, and name of the user who issued the `commit` configuration command.

**Syntax**

```
rollback <number>
```

**Options**

- **none**— Return to the most recently saved configuration.
- **number**—Configuration to return to.
  - **Range**: 0 through 49. The most recently saved configuration is number 0, and the oldest saved configuration is number 49.
  - **Default**: 0

To return to a configuration prior to the most recently committed one:
1. Specify the rollback number (here, 1 is entered and the configuration returns to the previously committed configuration):

```
[edit]
user@switch# rollback 1
load complete
```

2. Activate the configuration you have loaded:

```
[edit]
user@switch# commit
```

**Related Documentation**

- Managing Configuration Files Through the Configuration History (J-Web Procedure) on page 523
- Configuration Files Terms on page 499
- For more information on rollback, see Junos OS CLI User Guide.

## Reverting to the Default Factory Configuration for the EX Series Switch

If for any reason the current active configuration fails, you can revert to the factory-default configuration. You can also roll back to a previous configuration, as described in "Loading a Previous Configuration File (CLI Procedure)" on page 503, or revert to the rescue configuration, as described in “Reverting to the Rescue Configuration for the EX Series Switch” on page 507.

**TIP:** If you have lost the root password, it is not necessary to revert to the factory-default configuration to reset it. See “Troubleshooting Loss of the Root Password” on page 379.

The factory-default configuration contains the basic configuration settings for the switch. This is the first configuration of the switch and it is loaded when the switch is first powered on. For the factory-default configuration file for your switch, see the complete list under the Configuration tab of Configuration File Management on EX Series Switches.

**TIP:** You can run the EZsetup script to complete the initial configuration of the switch after reverting to the factory-default configuration. (The EZsetup script is available only on fixed configuration switches, it is not available on modular switches.) For information on completing the initial configuration using either the CLI or the J-Web interface, see Connecting and Configuring an EX Series Switch (CLI Procedure) or Connecting and Configuring an EX Series Switch (J-Web Procedure).

You can revert to the factory-default configuration by using the Menu button to the right of the LCD panel or by using the request system zeroize operational command or the load factory-default configuration command. (If your switch model does not have an LCD panel, use these commands.) You can also use the load factory-default command to revert to the factory-default configuration file that contains all default settings except
the root password setting, which is retained. These procedures are described in the following sections:

- Reverting to the Factory-Default Configuration by Using the LCD Panel on page 505
- Reverting to the Factory-Default Configuration by Using the request system zeroize Command on page 506
- Reverting to the Factory-Default Configuration by Using the load factory-default Command on page 506

Reverting to the Factory-Default Configuration by Using the LCD Panel

To set the switch to the factory-default configuration, use the LCD panel and buttons on the front panel of the switch shown in Figure 3 on page 505. If the switch model does not have an LCD panel, use one of the CLI commands described in the following sections.

Figure 3: EX Series Switch LCD Panel

NOTE: To revert a member switch of a Virtual Chassis to the factory-default configuration, first disconnect the cables connected to the Virtual Chassis ports (VCPs) to avoid affecting Virtual Chassis configuration parameters (member ID, mastership priority, and setting of VCP uplinks) on other members. See Disconnecting a Fiber-Optic Cable from an EX Series Switch, Disconnecting a Virtual Chassis Cable from an EX4200 Switch, or Disconnecting a Virtual Chassis Cable from an EX4500 Switch.

To revert to the factory-default configuration by using the LCD panel:

1. Press the Menu button until you see MAINTENANCE MENU on the panel.
2. Press the Enter button.
3. Press Menu until you see FACTORY DEFAULT.
4. Press Enter. The display says RESTORE DEFAULT?
5. Press Enter. The screen flashes FACTORY DEFAULT IN PROGRESS and returns to the idle menu.
6. Complete the initial configuration of the switch. See Connecting and Configuring an EX Series Switch (CLI Procedure) or Connecting and Configuring an EX Series Switch (J-Web Procedure)
Reverting to the Factory-Default Configuration by Using the request system zeroize Command

The request system zeroize command is a standard Junos OS operational mode command that removes all configuration information and resets all key values. The operation unlinks all user-created data files, including customized configuration and log files, from their directories. The switch then reboots and reverts to the factory-default configuration.

To completely erase user-created data so that it is unrecoverable, use the request system zeroize media command.

CAUTION: Before issuing request system zeroize, use the request system snapshot command to back up the files currently used to run the switch to a secondary device.

To revert to the factory-default configuration by using the request system zeroize command:

1. user@switch> request system zeroize
   warning: System will be rebooted and may not boot without configuration
   Erase all data, including configuration and log files? [yes,no] (yes)
2. Type yes to remove configuration and log files and revert to the factory default configuration.
3. Complete the initial configuration of the switch. See Connecting and Configuring an EX Series Switch (CLI Procedure) or Connecting and Configuring an EX Series Switch (J-Web Procedure)

Reverting to the Factory-Default Configuration by Using the load factory-default Command

The load factory-default command is a standard Junos OS configuration command that replaces the current active configuration with the factory-default configuration (except the root password setting, which by default is not set but which you must set in order to commit the new configuration in this procedure).

If you want to run the EZsetup script to complete the initial configuration of the switch after you revert to the factory-default configuration, do not use the load factory-default command. Instead do the reversion using either the LCD panel or the request system zeroize. If you use the load factory-default command to revert to the factory-default configuration, the configuration for the root password is retained and the EZsetup script will not run. (The EZsetup script is available only on fixed configuration switches, it is not available on modular switches.)

NOTE: The load factory-default command by itself is not supported on EX3300, EX4200, EX4550 and EX4500 switches configured in a Virtual Chassis.
To revert to the factory-default configuration by using the `load factory-default` command:

1. [edit]
   ```
   user@switch# load factory-default
   ```
2. [edit]
   ```
   user@switch# delete system commit factory-settings
   ```
3. [edit]
   ```
   user@switch# set system root-authentication plain-text-password
   ```
4. [edit]
   ```
   user@switch# commit
   ```
5. Check the member ID and mastership priority with the `show virtual-chassis` command and check to see whether there are remaining settings for uplink VCPs by using the `show virtual-chassis vc-port` command.

### Related Documentation
- Connecting and Configuring an EX Series Switch (CLI Procedure)
- Connecting and Configuring an EX Series Switch (J-Web Procedure)
- Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
- Understanding Configuration Files for EX Series Switches on page 493
- For more information about the `load factory-default` command, see Junos OS CLI User Guide.

### Reverting to the Rescue Configuration for the EX Series Switch

If someone inadvertently commits a configuration that denies management access to an EX Series switch and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration by using the LCD panel on the switch. The rescue configuration is a previously committed, valid configuration.

You can also revert to the default factory configuration, as described in “Reverting to the Default Factory Configuration for the EX Series Switch” on page 504.

Before you begin to revert to the rescue configuration:

- Ensure that you have physical access to the switch.
- A rescue configuration for the switch must have been previously set.

To revert the switch to the rescue configuration:

1. At the LCD panel on the switch, press `Menu` until you see MAINTENANCE MENU.
2. Press `Enter`.
3. Press `Menu` until you see Load Rescue.
4. Press `Enter`.
5. When Commit Rescue is displayed, press `Enter`. 
The LCD panel displays the message **Commit Rescue in Progress**. When the reversion is complete, it displays the idle menu.

**NOTE:** If there is no rescue configuration saved on the switch, the message **Commit rescue failed** is displayed.

**Setting or Deleting the Rescue Configuration (CLI Procedure)**

A rescue configuration is a well-known configuration that recovers a switch from a configuration that denies management access. You set a current committed configuration to be the rescue configuration through the J-Web interface or CLI.

If someone inadvertently commits a configuration that denies management access to an EX Series switch and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration by using the LCD panel on the switch. The rescue configuration is a previously committed, valid configuration. We recommend that the rescue configuration include the IP address (accessible from the network) for the management port.

To set the current active configuration as the rescue configuration:

```
user@switch> request system configuration rescue save
```

To delete an existing rescue configuration:

```
user@switch> request system configuration rescue delete
```

**Related Documentation**

- Setting or Deleting the Rescue Configuration (J-Web Procedure) on page 509
- Reverting to the Rescue Configuration for the EX Series Switch on page 507
- Loading a Previous Configuration File (CLI Procedure) on page 503
- Configuration Files Terms on page 499

For information on `show system configuration rescue`, see *[Junos OS System Basics and Services Command Reference]*.
Setting or Deleting the Rescue Configuration (J-Web Procedure)

A rescue configuration is a well-known configuration that recovers a switch from a configuration that denies management access. You set a current committed configuration to be the rescue configuration through the J-Web interface or CLI.

If someone inadvertently commits a configuration that denies management access to an EX Series switch and the console port is not accessible, you can overwrite the invalid configuration and replace it with the rescue configuration by using the LCD panel on the switch. The rescue configuration is a previously committed, valid configuration. We recommend that the rescue configuration include the IP address (accessible from the network) for the management port.

To view, set, or delete the rescue configuration using the J-Web interface, select Maintain > Config Management > Rescue. On the Rescue page, you can perform the following tasks:

- View the current rescue configuration—Click View rescue configuration.
- Set the current running configuration as the rescue configuration—Click Set rescue configuration.
- Delete the current rescue configuration—Click Delete rescue configuration.

Related Documentation

- Setting or Deleting the Rescue Configuration (CLI Procedure) on page 508
- Reverting to the Rescue Configuration for the EX Series Switch on page 507
- Configuration Files Terms on page 499

Configuring Autoinstallation of Configuration Files (CLI Procedure)

Autoinstallation is the automatic configuration of a device over the network from a pre-existing configuration file that you create and store on a configuration server—typically a Trivial File Transfer Protocol (TFTP) server. You can use autoinstallation to automatically deploy multiple devices from a central location in the network.

To specify autoinstallation to run when you power on a switch already installed in your network, you can enable it by specifying one or more interfaces, protocols, and configuration servers to be used for autoinstallation.

Before you explicitly enable and configure autoinstallation on the switch, perform these tasks as needed for your network's configuration:

- Have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the switch
- Configure a DHCP server on your network to meet your network requirements. You can configure a switch to operate as a DHCP server. For more information, see “Configuring a DHCP Server on Switches (CLI Procedure)” on page 1250.
- Create one of the following configuration files, and store it on a TFTP server (or HTTP server or FTP server) in the network:
A host-specific file with the name `hostname.conf` for each switch undergoing autoinstallation. Replace `hostname` with the name of a switch. The `hostname.conf` file typically contains all the configuration information necessary for the switch with this hostname.

A default configuration file named `switch.conf` with the minimum configuration necessary to enable you to telnet into the new switch for further configuration.

Physically attach the switch to the network using a Gigabit Ethernet port.

If you configure the DHCP server to provide only the TFTP server hostname, add an IP address-to-hostname mapping entry for the TFTP server to the DNS database file on the Domain Name System (DNS) server in the network.

If the switch is not on the same network segment as the DHCP server (or other device providing IP address resolution), configure an existing device as an intermediate device to receive TFTP and DNS requests and forward them to the TFTP server and the DNS server. You must configure the LAN or serial interface on the intermediate device with the IP addresses of the hosts providing TFTP and DNS services. Connect this interface to the switch.

If you are using `hostname.conf` files for autoinstallation, you must also complete the following tasks:

1. Configure the DHCP server to provide a `hostname.conf` filename to each switch. Each switch uses its `hostname.conf` filename to request a configuration file from the TFTP server. Copy the necessary `hostname.conf` configuration files to the TFTP server.

2. Create a default configuration file named `network.conf`, and copy it to the TFTP server. This file contains IP-address-to-hostname mapping entries. If the DHCP server does not send a `hostname.conf` filename to a new switch, the switch uses `network.conf` to resolve its hostname based on its IP address.

   Alternatively, you can add the IP-address-to-hostname mapping entry for the switch to a DNS database file.

   The switch uses the hostname to request a `hostname.conf` file from the TFTP server.

To configure autoinstallation:

1. Specify the URL address of one or more servers from which to obtain configuration files.

   ```
   [edit system]
   user@switch# set autoinstallation configuration-servers tftp://tftpconfig.sp.com
   ```

   **NOTE:** You can also use an FTP address, for example, `ftp://user:password@sftpconfig.sp.com`.

2. Configure one or more Ethernet interfaces to perform autoinstallation and one or two procurement protocols for each interface. The switch uses the protocols to send a request for an IP address for the interface:

   ```
   [edit system]
   ```
Using the Commit Options to Commit Configuration Changes (J-Web Procedure)

You can use the single-commit feature to commit all outstanding configuration changes in the J-Web interface on EX Series switches simultaneously. This helps in reducing the time J-Web takes for committing configurations because when changes are committed at every step, rollback configurations pile up.

For example, suppose you want to delete a firewall filter and add a new one. With immediate commits, you would need to commit your changes twice for this action. Using single commit, you can decrease the number of commits to one, thus saving time for working on other configurations.

When you edit a configuration, you work on a copy of the current configuration, which is your candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, allowing other users to edit those configurations, but they do not take effect on the switch until you commit the changes. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration when you commit the candidate configuration, changes made by all users take effect.

You can configure the commit options to either commit all configuration changes together or commit each configuration change immediately using the J-Web Commit Preference page.

NOTE: There are some pages on which configuration changes must be committed immediately. For such pages, if you configure the commit options for a single commit, the system displays warning notifications that remind you to commit your changes immediately. An example of such a page is the Interface Page (Configure > Interface).

To configure the commit options on an EX Series switch using the J-Web interface:

1. Select Commit Options.

   NOTE: All action links except Preference are disabled unless you edit, add, or delete a configuration.

2. Choose an action. See Table 92 on page 512 for details on the actions.

3. Configure the commit options by selecting Preference. See Table 93 on page 512 for details on preference options.
Table 92: Commit Options

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Commit | Commits the candidate configuration of the current user session, along with changes from other user sessions. | 1. Select Commit Options > Commit. Changes are committed after the system validates your configuration. A window displays that the configuration was successfully committed or that the commit failed.  
2. Click OK. Click Details to view the commit log. |
| Compare | Displays the XML log of pending uncommitted configurations on the device. | 1. Select Commit Options > Compare. The XML log of pending configurations on the devices are displayed similar to the CLI interface, in a “human-readable” form.  
2. Click Close. |
| Discard | Discards the candidate configuration of your current session, along with changes from other user sessions. | 1. Select Commit Options > Discard.  
2. Click OK to confirm the discard action. Your changes are discarded after the system validates your configuration. |
| Preference | Indicates your choice of committing all global configurations together or committing each configuration change immediately. | 1. Select Commit Options > Preference. The Commit Preference page is displayed.  
2. Configure the commit options by selecting your preference. See Table 93 on page 512 for details on preference options. |

Table 93: Commit Preference Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate and commit configuration changes</td>
<td>Sets the system to validate and force an immediate commit on every screen after every configuration change.</td>
</tr>
</tbody>
</table>
| Validate configuration changes | Loads all the configuration changes for an accumulated single commit. If there are errors in loading the configuration, the errors are logged. This is the default mode.  
Once you select this option, you need to select Commit Options > Commit to commit your changes. |

Related Documentation
- J-Web User Interface for EX Series Switches Overview on page 389
- EX Series Switch Software Features Overview on page 27
Configuration Statements

archival

Syntax  archival {
    configuration {
        archive-sites {
            file://<path>/<filename>;
            ftp://username@host:<port>url-path password password;
            http://username@host:<port>url-path password password;
            pasvftp://username@host:<port>url-path password password;
            scp://username@host:<port>url-path password password;
        }
        transfer-interval interval;
        transfer-on-commit;
    }
}

Hierarchy Level  [editsystem]

Release Information  Statement introduced before Junos OS Release 7.4.
                    Statement introduced in Junos OS Release 9.0 for EX Series switches.
                    Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  Configure copying of the currently active configuration to an archive site. An archive site can be a file, or an FTP or SCP location.

NOTE: The edit system archival hierarchy is not available on QFabric systems.

Options  The remaining statements are explained separately.

NOTE: The [edit system archival] hierarchy is not available on QFabric systems.

Required Privilege Level  admin—To view this statement in the configuration.
                           admin-control—To add this statement to the configuration.

Related Documentation  Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site

%archive-sites (Configuration File)

Syntax
archive-sites {
    file://<path>/<filename>;
    ftp://username@host:<port>/url-path password password;
    http://username@host:<port>/url-path password password;
    pasvftp://username@host:<port>/url-path password password;
    scp://username@host:<port>/url-path password password;
}

Hierarchy Level
[edit system archival configuration]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Specify where to transfer the current configuration files. When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example, "scp://username:<password>@[ipv6-host-address]:<port>/url-path"

If you specify more than one archive site, the router or switch attempts to transfer the configuration files to the first archive site in the list, moving to the next only if the transfer fails.

The destination filename is saved in the following format, where $n$ corresponds to the number of the compressed configuration rollback file that has been archived:

```
router-name_juniper.conf.$n.gz_YYYYMMDD_HHmmss.
```

NOTE: The time included in the destination filename is always in Coordinated Universal Time (UTC) regardless of whether the time on the router or switch is configured as UTC or the local time zone. The default time zone on the router or switch is UTC.

NOTE: The [edit system archival] hierarchy is not available on QFabric systems.

Options
The prefix used in the configuration statement determines the form of transfer:

- `file://` — transfer on a path to a named file
- `ftp://` — transfer using active FTP server
- `pasvftp://` — transfer to a device that only accepts passive FTP services
scp:// —transfer to a known host using background SCP file transfers

**Required Privilege**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site
- Junos OS Commit Model for Router or Switch Configuration
- configuration on page 518
- transfer-on-commit on page 522
autoinstallation

Syntax

autoinstallation {
    configuration-servers {
        url;
    }
    interfaces {
        interface-name {
            bootp;
            rarp;
        }
    }
}

Hierarchy Level
[edit system]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

Description
For ACX Series routers, J Series Services routers, and EX Series switches only. Download a configuration file automatically from an FTP, Hypertext Transfer Protocol (HTTP), or Trivial FTP (TFTP) server. When you power on a router or switch configured for autoinstallation, it requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server. Once the router or switch has an address, it sends a request to a configuration server and downloads and installs a configuration.

Options
The remaining statements are explained separately.

Required Privilege Level
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation
- ACX Series Autoinstallation Overview
- Before You Begin Autoinstallation on an ACX Series Universal Access Router
- Autoinstallation Configuration of ACX Series Universal Access Routers
- USB Autoinstallation on ACX Series Routers
- Verifying Autoinstallation on ACX Series Universal Access Routers
- show system autoinstallation status
- Upgrading Software Using Automatic Software Download
- J Series Services Router Basic LAN and WAN Access Configuration Guide
- configuration-servers on page 519
- idle-timeout on page 437
**synchronize (Commit configuration)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>synchronize;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit system commit]</td>
</tr>
</tbody>
</table>
| Release Information | Statement introduced in Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches. |
| Description | For devices with multiple Routing Engines only. Configure a commit command to automatically result in a commit synchronize action between dual Routing Engines within the same chassis. The Routing Engine on which you execute the commit command (the requesting Routing Engine) copies and loads its candidate configuration to the other (the responding) Routing Engines. All Routing Engines then perform a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on all Routing Engines.  
Starting with Junos OS Release 9.3, accounting of events and operations on a backup Routing Engine is not supported on accounting servers such as TACACS+ or RADIUS. Logging of accounting events is supported only for events and operations on a master Routing Engine. |
| Required Privilege | system—To view this statement in the configuration.  
system-control—To add this statement to the configuration. |
| Related Documentation | • Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically |
configuration

Syntax

configuration {
    transfer-interval interval;
    transfer-on-commit;
    archive-sites {
        file://<path>/<filename>;
        ftp://username@host:<port>url-path password password;
        http://username@host:<port>url-path password password;
        pasvftp://username@host:<port>url-path password password;
        scp://username@host:<port>url-path password password;
    }
}

Hierarchy Level [edit system archival]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the router or switch to periodically transfer its currently active configuration (or after each commit).

NOTE: The [edit system archival] hierarchy is not available on QFabric systems.

Options

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site
- archive
- archive-sites on page 514
- transfer-interval on page 521
- transfer-on-commit on page 522
**configuration-servers**

| Syntax          | configuration-servers {  
|                 |    url;  
<table>
<thead>
<tr>
<th></th>
<th>}</th>
</tr>
</thead>
</table>

**Hierarchy Level**  
[edit system autoinstallation]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
For J Series Services Routers and EX Series switches only, configure the URL address of a server from which to obtain configuration files. Examples of URLs:

- `tftp://hostname/path/filename`
- `ftp://username:prompt@ftp.hostname.net/path/filename`

**Required Privilege Level**  
- system—To view this statement in the configuration.  
- system-control—To add this statement to the configuration.

**Related Documentation**  
- [Upgrading Software Using Automatic Software Download](#)  
- [Getting Started Guide for your router model](#)  
  - autoinstallation on page 516  
  - idle-timeout on page 437
interfaces

Syntax  
```
interfaces {
    interface-name {
        bootp;
        rarp;
        slarp;
    }
}
```

Hierarchy Level  
[edit system autoinstallation]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
For J Series Services Routers and EX Series switches only. Configure the interface on which to perform autoinstallation. A request for an IP address is sent from the interface. Specify the IP address procurement protocol.

Options  
```
rapboot — Send requests over serial interfaces with Frame Relay.
rap — Send requests over Ethernet interfaces.
slarp — (On J Series Services Routers only) Send requests over serial interfaces with HDLC.
```

Required Privilege Level  
```
system — To view this statement in the configuration.
system-control — To add this statement to the configuration.
```

Related Documentation  
```
• Upgrading Software Using Automatic Software Download
• J Series Services Router Basic LAN and WAN Access Configuration Guide
• autoinstallation on page 516
```
transfer-interval (Configuration)

Syntax  
```
transfer-interval interval;
```

Hierarchy Level  
[edit system archival configuration]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Configure the router or switch to periodically transfer its currently active configuration to an archive site.

NOTE: The [edit system archival] hierarchy is not available on QFabric systems.

Options  
```
interval — Interval at which to transfer the current configuration to an archive site.
```
Range: 15 through 2880 minutes

NOTE: The [edit system archival] hierarchy is not available on QFabric systems.

Required Privilege  
Level
```
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
```

Related Documentation
- Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site
- archive
- configuration on page 518
- transfer-on-commit on page 522
transfer-on-commit

Syntax    transfer-on-commit;

Hierarchy Level    [edit system archival configuration]

Release Information    Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description    Configure the router or switch to transfer its currently active configuration to an archive site each time you commit a candidate configuration.

NOTE: When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([ ]). For example, “ftp://username:password@[ipv6-host-address]:<port>/url-path”.

NOTE: The [edit system archival] hierarchy is not available on QFabric systems.

Required Privilege Level    system—To view this statement in the configuration.
    system-control—To add this statement to the configuration.

Related Documentation    • Using Junos OS to Configure a Router or Switch to Transfer Its Configuration to an Archive Site
    • archive
    • configuration on page 518
    • transfer-interval on page 521
CHAPTER 16

Administration

- Routine Monitoring on page 523
- Operational Commands on page 527

Routine Monitoring

- Managing Configuration Files Through the Configuration History (J-Web Procedure) on page 523
- Verifying Autoinstallation Status on page 526

Managing Configuration Files Through the Configuration History (J-Web Procedure)

Use the Configuration History function to manage configuration files.

1. Displaying Configuration History on page 523
2. Displaying Users Editing the Configuration on page 524
3. Comparing Configuration Files with the J-Web Interface on page 525
4. Downloading a Configuration File with the J-Web Interface on page 525
5. Loading a Previous Configuration File with the J-Web Interface on page 525

Displaying Configuration History

To manage configuration files with the J-Web interface, select Maintain > Config Management > History. The main pane displays History — Database Information page.

Table 94 on page 524 summarizes the contents of the display.

The configuration history display allows you to:

- View a configuration.
- Compare two configurations.
- Download a configuration file to your local system.
- Roll back the configuration to any of the previous versions stored on the switch.
Table 94: J-Web Configuration History Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Version of the configuration file.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>Date and time the configuration was committed.</td>
</tr>
<tr>
<td>User</td>
<td>Name of the user who committed the configuration.</td>
</tr>
<tr>
<td>Client</td>
<td>Method by which the configuration was committed:</td>
</tr>
<tr>
<td></td>
<td>• cli—A user entered a Junos OS CLI command.</td>
</tr>
<tr>
<td></td>
<td>• junoscript—A Junos XML protocol client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way.</td>
</tr>
<tr>
<td></td>
<td>• snmp—An SNMP set request started the operation.</td>
</tr>
<tr>
<td></td>
<td>• other—Another method was used to commit the configuration.</td>
</tr>
<tr>
<td>Comment</td>
<td>Comment.</td>
</tr>
<tr>
<td>Log Message</td>
<td>Method used to edit the configuration:</td>
</tr>
<tr>
<td></td>
<td>• Imported via paste—Configuration was edited and loaded with the Configure &gt; CLI Tools &gt; Edit Configuration Text option.</td>
</tr>
<tr>
<td></td>
<td>• Imported upload [filename]—Configuration was uploaded with the Configure &gt; CLI Tools &gt; Point Click Editor option.</td>
</tr>
<tr>
<td></td>
<td>• Modified via J-Web Configure — Configuration was modified with the J-Web Configure menu.</td>
</tr>
<tr>
<td></td>
<td>• Rolled back via user-interface—Configuration was rolled back to a previous version through the user interface specified by user-interface, which can be Web Interface or CLI.</td>
</tr>
<tr>
<td>Action</td>
<td>Action to perform with the configuration file. The action can be Download or Rollback.</td>
</tr>
</tbody>
</table>

Displaying Users Editing the Configuration

To display a list of users editing the switching platform configuration, select Config Management > History. The list is displayed as Database Information in the main pane. Table 95 on page 524 summarizes the Database Information display.

Table 95: J-Web Configuration Database Information Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of user editing the configuration.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time of day the user logged in to the switch.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>Elapsed time since the user issued a configuration command from the CLI.</td>
</tr>
<tr>
<td>Terminal</td>
<td>Terminal on which the user is logged in.</td>
</tr>
<tr>
<td>PID</td>
<td>Process identifier assigned to the user by the switching platform.</td>
</tr>
<tr>
<td>Edit Flags</td>
<td>Designates a private or exclusive edit.</td>
</tr>
</tbody>
</table>
### Table 95: J-Web Configuration Database Information

**Summary (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit Path</td>
<td>Level of the configuration hierarchy that the user is editing.</td>
</tr>
</tbody>
</table>

### Comparing Configuration Files with the J-Web Interface

To compare any two of the past 50 committed configuration files:

1. Select **Config Management > History**. A list of the current and the previous 49 configurations is displayed as Configuration History in the main pane.
2. Select the check boxes to the left of the two configuration versions you want to compare.
3. Click **Compare**.

The main pane displays the differences between the two configuration files at each hierarchy level as follows:

- Lines that have changed are highlighted side by side in green.
- Lines that exist only in the more recent configuration file are displayed in red on the left.
- Lines that exist only in the older configuration file are displayed in blue on the right.

### Downloading a Configuration File with the J-Web Interface

To download a configuration file from the switch to your local system:

1. Select **Config Management > History**. A list of current and previous 49 configurations is displayed as Configuration History in the main pane.
2. In the Action column, click **Download** for the version of the configuration you want to download.
3. Select the options your Web browser provides that allow you to save the configuration file to a target directory on your local system.

The file is saved as an ASCII file.

### Loading a Previous Configuration File with the J-Web Interface

To load (roll back) and commit a previous configuration file stored on the switching platform:

1. Select **Config Management > History**. A list of current and previous 49 configurations is displayed as Configuration History in the main pane.
2. In the Action column, click **Rollback** for the version of the configuration you want to load.

The main pane displays the results of the rollback operation.
NOTE: When you click Rollback, the switch loads and commits the selected configuration. This behavior is different from the switch's behavior that occurs after you enter the rollback configuration mode command from the CLI. In the latter case, the configuration is loaded but not committed.

Related Documentation
- Loading a Previous Configuration File (CLI Procedure) on page 503
- Understanding Configuration Files for EX Series Switches on page 493
- Understanding J-Web Configuration Tools on page 392

Verifying Autoinstallation Status

**Purpose**
Display the status of the autoinstallation feature.

**Action**
From the CLI, enter the `show system autoinstallation status` command.

**Sample Output**

```
user@switch> show system autoinstallation status
Autoinstallation status:
Master state: Active
Last committed file: None
Configuration server of last committed file: 10.25.100.1
Interface:
  Name: ge-0/0/0
  State: Configuration Acquisition
  Acquired:
    Address: 192.168.124.75
    Hostname: host-ge-000
    Hostname source: DNS
    Configuration filename: switch-ge-000.conf
    Configuration filename server: 10.25.100.3
  Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
  Interface:
    Name: ge-0/0/1
    State: None
    Address acquisition:
    Protocol: DHCP Client
    Acquired address: None
    Protocol: RARP Client
    Acquired address: None
```

**Meaning**
The output shows the settings configured for autoinstallation. Verify that the values displayed are correct for the switch when it is deployed on the network.

**Related Documentation**
- Configuring Autoinstallation of Configuration Files (CLI Procedure) on page 509
Operational Commands
clear log

Syntax  
clear log filename  
<all>

Release Information  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Remove contents of a log file.

Options  
filename—Name of the specific log file to delete.  
all—(Optional) Delete the specified log file and all archived versions of it.

Required Privilege  
Level clear

Related Documentation  
• show log on page 1091

List of Sample Output  
clear log on page 528

Output Fields  
See file list for an explanation of output fields.

Sample Output

clear log

The following sample commands list log file information, clear the contents of a log file,  
and then display the updated log file information:

```
user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
-------------------------------------------------------------------------
-rw-r-----  1 root  wheel      26450 Jun 23 18:47 /var/log/sampled
total 1
user@host> clear log lcc0-re0:sampled
lcc0-re0:
-------------------------------------------------------------------------
user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
-------------------------------------------------------------------------
-rw-r-----  1 root  wheel         57 Sep 15 03:44 /var/log/sampled
total 1
```
clear system commit

Syntax

clear system commit

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Clear any pending commit operation.

Options

This command has no options.

Required Privilege Level

maintenance (or the actual user who scheduled the commit)

Related Documentation

- show system commit on page 557

List of Sample Output

- clear system commit on page 529
- clear system commit (None Pending) on page 529
- clear system commit (User Does Not Have Required Privilege Level) on page 529

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system commit

user@host> clear system commit
Pending commit cleared.

clear system commit (None Pending)

user@host> clear system commit
No commit scheduled.

clear system commit (User Does Not Have Required Privilege Level)

user@host> clear system commit
error: Permission denied
file archive

Syntax

```
file archive destination destination source source
<compress>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Archive, and optionally compress, one or multiple local system files as a single file, locally or at a remote location.

Options

**destination destination**—Destination of the archived file or files. Specify the destination as a URL or filename. The Junos OS adds one of the following suffixes if the destination filename does not already have it:

- For archived files—The suffix .tar
- For archived and compressed files—The suffix .tgz

**source source**—Source of the original file or files. Specify the source as a URL or filename.

**compress**—(Optional) Compress the archived file with the GNU zip (gzip) compression utility. The compressed files have the suffix .tgz.

Required Privilege Level

maintenance

List of Sample Output

- file archive (Multiple Files) on page 530
- file archive (Single File) on page 530
- file archive (with Compression) on page 531

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

**file archive (Multiple Files)**

The following sample command archives all message files in the local directory `/var/log/messages` as the single file `messages-archive.tar`.

```
user@host> file archive source /var/log/messages* destination /var/log/messages-archive.tar /usr/bin/tar: Removing leading / from absolute path names in the archive.
user@host>
```

**file archive (Single File)**

The following sample command archives one message file in the local directory `/var/log/messages` as the single file `messages-archive.tar`.

```
user@host> file archive source /var/log/messages destination /var/log/messages-archive.tar
```
The following sample command archives and compresses all message files in the local directory `/var/log/messages` as the single file `messages-archive.tgz`.

```
user@host> file archive compress source /var/log/messages* destination /var/log/messages-archive.tgz
```

/usr/bin/tar: Removing leading / from absolute path names in the archive.
**file checksum md5**

**Syntax**

```
file checksum md5 <pathname> filename
```

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Calculate the Message Digest 5 (MD5) checksum of a file.

**Options**

- `pathname`—(Optional) Path to a filename.
- `filename`—Name of a local file for which to calculate the MD5 checksum.

**Required Privilege Level**

maintenance

**Related Documentation**

- Configuring Checksum Hashes for a Commit Script in the Junos OS Configuration and Operations Automation Guide
- Configuring Checksum Hashes for an Event Script in the Junos OS Configuration and Operations Automation Guide
- Configuring Checksum Hashes for an Op Script in the Junos OS Configuration and Operations Automation Guide
- Executing an Op Script from a Remote Site in the Junos OS Configuration and Operations Automation Guide
- file checksum sha-256 on page 534
- file checksum sha1 on page 533
- op on page 169

**List of Sample Output**

file checksum md5 on page 532

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
user@host> file checksum md5 jbundle-5.3R2.4-export-signed.tgz
MD5 (jbundle-5.3R2.4-export-signed.tgz) = 2a3b69e43f9bd4893729cc16f505a0f5
```
file checksum sha1

Syntax

file checksum sha1 <pathname> filename

Release Information

Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Calculate the Secure Hash Algorithm (SHA-1) checksum of a file.

Options

pathname—(Optional) Path to a filename.
filename—Name of a local file for which to calculate the SHA-1 checksum.

Required Privilege

maintenance

Related Documentation

- Configuring Checksum Hashes for a Commit Script in the Junos OS Configuration and Operations Automation Guide
- Configuring Checksum Hashes for an Event Script in the Junos OS Configuration and Operations Automation Guide
- Configuring Checksum Hashes for an Op Script in the Junos OS Configuration and Operations Automation Guide
- Executing an Op Script from a Remote Site in the Junos OS Configuration and Operations Automation Guide
- file checksum md5 on page 532
- file checksum sha-256 on page 534
- op on page 169

List of Sample Output

file checksum sha1 on page 533

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum sha1

user@host> file checksum sha1 /var/db/scripts/opscript.slax
SHA1 (/var/db/scripts/commitscript.slax) = ba9e47120c7ce55c5ff29af73ead370e162c676
file checksum sha-256

Syntax  file checksum sha-256 <pathname> filename

Release Information  Command introduced in Junos OS Release 9.5.
                    Command introduced in Junos OS Release 9.5 for EX Series switches.
                    Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  Calculate the Secure Hash Algorithm 2 family (SHA-256) checksum of a file.

Options  pathname—(Optional) Path to a filename.
          filename—Name of a local file for which to calculate the SHA-256 checksum.

Required Privilege  Level  maintenance

Related Documentation  • Configuring Checksum Hashes for a Commit Script in the Junos OS Configuration and Operations Automation Guide
                      • Configuring Checksum Hashes for an Event Script in the Junos OS Configuration and Operations Automation Guide
                      • Configuring Checksum Hashes for an Op Script in the Junos OS Configuration and Operations Automation Guide
                      • Executing an Op Script from a Remote Site in the Junos OS Configuration and Operations Automation Guide
                      • file checksum md5 on page 532
                      • file checksum sha1 on page 533
                      • op on page 169

List of Sample Output  file checksum sha-256 on page 534

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum sha-256

user@host> file checksum sha-256 /var/db/scripts/commitscript.slax
SHA256 (/var/db/scripts/commitscript.slax) = 94c2b061fb55399e15babd2529453815601a602b5c98e5c12ed929c9d343dd71
**file compare**

**Syntax**  
```  
file compare (files filename filename)  
<context | unified>  
<ignore-white-space>  
```

**Release Information**  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**  
Compare two local files and describe the differences between them in default, context, or unified output styles:

- **Default**—In the first line of output, c means lines were changed between the two files, d means lines were deleted between the two files, and a means lines were added between the two files. The numbers preceding this alphabetical marker represent the first file, and the lines after the alphabetical marker represent the second file. A left angle bracket (<) in front of output lines refers to the first file. A right angle bracket (>) in front of output lines refers to the second file.

- **Context**—The display is divided into two parts. The first part is the first file; the second part is the second file. Output lines preceded by an exclamation point (!) have changed. Additions are marked with a plus sign (+), and deletions are marked with a minus sign (-).

- **Unified**—The display is preceded by the line number from the first and the second file (xx,xxx,x). Before the line number, additions to the file are marked with a plus sign (+), and deletions to the file are marked with a minus sign (-). The body of the output contains the affected lines. Changes are viewed as additions plus deletions.

**Options**
```
files filename—Names of two local files to compare.  
context—(Optional) Display output in context format.  
ignore-white-space—(Optional) Ignore changes in the amount of white space.  
unified—(Optional) Display output in unified format.  
```

**Required Privilege Level**  
none

**List of Sample Output**
```
file compare files on page 536  
file compare files context on page 536  
file compare files unified on page 536  
file compare files unified ignore-white-space on page 536  
```

**Output Fields**  
When you enter this command, you are provided feedback on the status of your request.
Sample Output

file compare files

```
user@host> file compare files /tmp/one /tmp/two
100c100
<             full-name "File 1";
---
>             full-name "File 2";
102c102
<             class foo; # 'foo' is not defined
---
>             class super-user;
```

defile compare files context

```
user@host> file compare files /tmp/one /tmp/two context
*** /tmp/one    Wed Dec  3 17:12:50 2003
--- /tmp/two    Wed Dec  3 09:13:14 2003
***************
*** 97,104 ****
}
}user bill {
!
  full-name "Bill Smith";
!
  class foo; # 'foo' is not defined
  authentication {
    encrypted-password SECRET;
  }
--- 97,105 ----
}user bill {
!
  full-name "Bill Smith";
!
  uid 1089;
!
  class super-user;
  authentication {
    encrypted-password SECRET;
  }
```

defile compare files unified

```
user@host> file compare files /tmp/one /tmp/two unified
*** /tmp/one    Wed Dec  3 17:12:50 2003
--- /tmp/two    Wed Dec  3 09:13:14 2003
+++ /tmp/two    Wed Dec  3 09:13:14 2003
@@ -97,8 +97,9 @@
}
}user bill {
-
-  full-name "Bill Smith";
-  class foo; # 'foo' is not defined
+  full-name "Bill Smith";
+  uid 1089;
+  class super-user;
  authentication {
    encrypted-password SECRET;
  }
```

defile compare files unified ignore-white-space

```
user@host> file compare files /tmp/one /tmp/two unified ignore-white-space
user bill {
  full-name "Bill Smith";
  uid 1089;
- class foo; # 'foo' is not defined
+ class super-user;
  authentication {
    encrypted-password <SECRET>; # SECRET-DATA
  }
}
**file copy**

**Syntax**

```
file copy source destination
<source-address address>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
`source-address` option added in Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

**Description**

Copy files from one location to another location on the local device or to a location on a remote device reachable by the local device.

**Required Privilege Level**

maintenance

**Related Documentation**

- Format for Specifying Filenames and URLs in Junos OS CLI Commands
- Default Directories for Junos OS File Storage on the Router or Switch
- Copying a Configuration File from One Routing Engine to the Other

**List of Sample Output**

Copy a File from the Local Device to a Personal Computer on page 538
Copy a Configuration File between Routing Engines on page 538
Copy a Log File between Routing Engines on page 538
Copy a File from a TX Matrix Plus Router to a T1600 Router Connected to the TX Matrix Plus on page 539
Copy a File Using File Transfer Protocol on page 539
Copy a File Using File Transfer Protocol and Requiring a Password on page 539
Copy a File Using Secure Copy Protocol (scp) on page 539

**Sample Output**

The following are examples of a variety of file copy scenarios.

**Copy a File from the Local Device to a Personal Computer**

```
user@host> file copy /var/tmp/rpd.core.4 mypc:/c/junipero/tmp
...transferring.file...... | 0 KB | 0.3 kB/s | ETA: 00:00:00 | 100%
```

**Copy a Configuration File between Routing Engines**

The following sample command copies a configuration file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy /config/juniper.conf re1:/var/tmp/copied-juniper.conf
```

**Copy a Log File between Routing Engines**

The following sample command copies a log file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy lcc0-re0:/var/log/chassis lcc0-re1:/var/tmp
```
Copy a File from a TX Matrix Plus Router to a T1600 Router Connected to the TX Matrix Plus

The following sample command copies a text file from Routing Engine 1 on the switch-fabric chassis sfc0 to Routing Engine 1 on the line-card chassis lcc0:

```
user@host> filecopy sfc0-re1:/tmp/sample.txt lcc0-re1:/var/tmp
```

Copy a File Using File Transfer Protocol

To use anonymous FTP to copy a local file to a remote system, enter the following command:

```
user@host> filecopy filename ftp://hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
user@host> filecopy /config/juniper.conf ftp://hostname/juniper.conf
Receiving ftp: //hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using File Transfer Protocol and Requiring a Password

To use FTP where you require more privacy and are prompted for a password, enter the following command:

```
root@host> filecopy filename ftp://user@hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
root@host> filecopy /config/juniper.conf ftp://user@hostname/juniper.conf
Password for user@hostname: ******
Receiving ftp: //user@hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using Secure Copy Protocol (scp)

To use scp to copy a local file to a remote system, enter the following command:

```
root@host> filecopy filename scp://user@hostname/path/filename
```

In the following example, `/config/juniper.conf` is the local file, user is the username, and `ssh-host` is the scp server:

```
root@host> filecopy /config/juniper.conf scp://user@ssh-host/tmp/juniper.conf
user@ssh-host's password: ******
juniper.conf         100%
|*********************************************************************************|
|00:00|
```

2198 bytes transferred in 0.0 seconds (2.69 MBps)
file delete

Syntax

```
file delete filename
<purge>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Delete a file on the local router or switch.

Options

- `filename`—Name of the file to delete. For a routing matrix, include chassis information in the filename if the file to be deleted is not local to the Routing Engine from which the command is issued.
- `purge`—(Optional) Overwrite regular files before deleting them.

Required Privilege

```
maintenance
```

List of Sample Output

- file delete on page 540
- file delete (Routing Matrix) on page 540

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
file delete

user@host> file list /var/tmp
dcd.core
rpdp.core
snmpd.core

user@host> file delete /var/tmp/snmpd.core
user@host> file list /var/tmp
dcd.core
rpdp.core

file delete (Routing Matrix)

user@host> file list lcc0-re0:/var/tmp
dcd.core
rpdp.core
snmpd.core

user@host> file delete lcc0-re0:/var/tmp/snmpd.core
user@host> file list /var/tmp
dcd.core
rpdp.core
```
file list

Syntax

file list
<detail | recursive>
<filename>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display a list of files on the local router or switch.

Options
none—Display a list of all files for the current directory.

detail | recursive—(Optional) Display detailed output or descend recursively through the
directory hierarchy, respectively.

filename—(Optional) Display a list of files. For a routing matrix, the filename must include
the chassis information.

Additional Information
The default directory is the home directory of the user logged in to the router or switch.
To view available directories, enter a space and then a backslash (/) after the file list
command. To view files within a specific directory, include a backslash followed by the
directory and, optionally, subdirectory name after the file list command.

Required Privilege
Level
maintenance

List of Sample Output
file list on page 541
file list (Routing Matrix) on page 541

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
file list

user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core

file list (Routing Matrix)

user@host> file list lcc0-re0:/var/tmp
lcc0-re0:
______________________________
/var/tmp/:
.gdbinit
.pccardd
Test/
chassisd*
chassisd.nathan*
check_time*
cores/
diagTestPrep*
diagtest*
diagtest.regress*
do_switchovers*
dump_test*
err.manoj.log
esw_clearstats*
esw_counter*
esw_debug*
esw_debug_ge*
esw_filt_test*
esw_filter_tnp_addr*
esw_getstats*
esw_phy*
esw_stats*
file rename

**Syntax**

```
file rename source destination
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Rename a file on the local router or switch.

**Options**

- **destination**—New name for the file.
- **source**—Original name of the file. For a routing matrix, the filename must include the chassis information.

**Required Privilege Level**

maintenance

**List of Sample Output**

- file rename on page 543
- file rename (Routing Matrix) on page 543

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

The following example lists the files in /var/tmp, renames one of the files, and then displays the list of files again to reveal the newly named file.

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core
user@host> file rename /var/tmp/dcd.core /var/tmp/dcd.core.990413
user@host> file list /var/tmp
dcd.core.990413
rpd.core
snmpd.core
```

The following example lists the files in /var/tmp, renames one of the files, and then displays the list of files again to reveal the newly named file.

```
user@host> file list lcc0-rel:/var/tmp
lcc0-rel:
------------------------------------------------------------
/var/tmp:
.pccardd
sartre.conf
```
snmpd
syslogd.core-tarball.0.tgz

user@host> file rename lcc0-re0:/var/tmp/snmpd /var/tmp/snmpd.rr
user@host> file list lcc0-rel:/var/tmp
lcc0-rel:
--------------------------------------------------------------------------
/var/tmp:
.pccardd
.sartre.conf
.snmpd.rr
.syslogd.core-tarball.0.tgz
file show

Syntax
file show filename
<encoding (base64 | raw)>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display the contents of a file.

Options
filename—Name of a file. For a routing matrix, the filename must include the chassis information.
encoding (base64 | raw)—(Optional) Encode file contents with base64 encoding or show raw text.

Required Privilege
maintenance

List of Sample Output
file show on page 545
file show (Routing Matrix) on page 545

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

file show

user@host> file show /var/log/messages
Apr 13 21:00:08 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:00:40 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:02:48 romney last message repeated 4 times
Apr 13 21:07:04 romney last message repeated 8 times
Apr 13 21:07:13 romney /kernel: so-1/1/0: Clearing SONET alarm(s) RDI-P
Apr 13 21:07:29 romney /kernel: so-1/1/0: Asserting SONET alarm(s) RDI-P
...

file show (Routing Matrix)

user@host> file show lcc0-re0:/var/tmp/.gdbinit
lcc0-re0:
--------------------------------------------------------------------------
# Settings
--------------------------------------------------------------------------
set print pretty
--------------------------------------------------------------------------
# Basic stuff
--------------------------------------------------------------------------
#define msgbuf
   printf "%s", msgbufp->msg_ptr
end
# hex dump of a block of memory
# usage: dump address length
define dump
  p $arg0, $arg1
  set $ch = $arg0
  set $j = 0
  set $n = $arg1
  while ($j < $n)
    #printf "%x %x ",&$ch[$j],$ch[$j]
    printf "%x ",$ch[$j]
    set $j = $j + 1
    if (!$j % 16)
      printf "\n"
  end
end
end
**request system configuration rescue delete**

**Syntax**
request system configuration rescue delete

**Release Information**
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Delete an existing rescue configuration.

**NOTE:** The [edit system configuration] hierarchy is not available on QFabric systems.

**Options**
This command has no options.

**Required Privilege Level**
maintenance

**Related Documentation**
- request system configuration rescue save on page 548
- request system software rollback on page 633
- show system commit on page 557

**List of Sample Output**
request system configuration rescue delete on page 547

**Output Fields**
This command produces no output.

**Sample Output**
request system configuration rescue delete

user@host> request system configuration rescue delete
**request system configuration rescue save**

**Syntax**

request system configuration rescue save

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Save the most recently committed configuration as the rescue configuration so that you can return to it at any time by using the `rollback` command.

**NOTE:** The `[edit system configuration]` hierarchy is not available on QFabric systems.

**Options**

This command has no options.

**Required Privilege Level**

maintenance

**Related Documentation**

- request system software delete on page 629
- request system software rollback on page 633
- show system commit on page 557

**List of Sample Output**

request system configuration rescue save on page 548

**Output Fields**

This command produces no output.

**Sample Output**

request system configuration rescue save

user@host> request system configuration rescue save
request system scripts refresh-from commit

**Syntax**
```
request system scripts refresh-from commit file file-name url url-path
```

**Release Information**
Command introduced in Junos OS Release 10.1 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Automatically download the initial Junos OS configuration and a set of standard commit scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:
```
<request-script-refresh-from>
  <type>commit</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

**Options**
- **file** `file-name`—Name of the file to be downloaded.
- **url** `url-path`—URL of the file to be downloaded.

**Required Privilege**
```
Level maintenance
```

**Related Documentation**
- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- *Junos OS NETCONF XML Management Protocol Guide*

**List of Sample Output**
```
request system scripts refresh-from commit file config.txt url http://host1.juniper.net on page 549
```

**Sample Output**
```
user@switch> request system scripts refresh-from commit file config.txt url http://host1.juniper.net
user@switch>
```
request system scripts refresh-from event

Syntax  
request system scripts refresh-from event file file-name url url-path

Release Information  
Command introduced in Junos OS Release 10.1 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Automatically download the initial Junos OS configuration and a set of standard event scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:

```
<request-script-refresh-from>
  <type>event</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

Options  
- file file-name—Name of the file to be downloaded.
- url url-path—URL of the file to be downloaded.

Required Privilege Level  
maintenance

Related Documentation  
- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Junos OS NETCONF XML Management Protocol Guide

List of Sample Output  
request system scripts refresh-from event file config.txt url http://host1.juniper.net on page 550

Sample Output  
request system scripts refresh-from event file config.txt url http://host1.juniper.net

```
user@switch> request system scripts refresh-from event file config.txt url http://host1.juniper.net
user@switch>
```
request system scripts refresh-from op

Syntax

```
request system scripts refresh-from op file file-name url url-path
```

Release Information

Command introduced in Junos OS Release 10.1 for EX Series switches.

Description

Automatically download the initial Junos OS configuration and a set of standard op scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:

```
<request-script-refresh-from>
  <type>op</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

Options

- **file** *file-name*—Name of the file to be downloaded.
- **url** *url-path*—URL of the file to be downloaded.

Required Privilege Level

maintenance

Related Documentation

- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Junos OS NETCONF XML Management Protocol Guide

List of Sample Output

```
request system scripts refresh-from op file config.txt url http://host1.juniper.net on page 551
```

Sample Output

```
user@switch> request system scripts refresh-from op file config.txt url http://host1.juniper.net
user@switch>
```
request system zeroize

Syntax

```
request system zeroize
<media>
```

Release Information

Command introduced before Junos OS Release 9.0.
Command introduced in Junos OS Release 11.2 for EX Series switches.
Option media added in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 12.2 for MX Series devices.
Command introduced in Junos OS Release 12.3 for the QFX Series.

Description

NOTE: The media option is not available on the QFX Series.

Remove all configuration information on the Routing Engines and reset all key values. If the device has dual Routing Engines, the command is broadcast to all Routing Engines on the device. The command removes all data files, including customized configuration and log files, by unlinking the files from their directories. The command removes all user-created files from the system including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication, IPsec, RADIUS, TACACS+, and SNMP.

This command reboots the device and sets it to the factory default configuration. After the reboot, you cannot access the device through the management Ethernet interface. Log in through the console as root and start the Junos OS command-line interface (CLI) by typing cli at the prompt.

To completely erase user-created data so that it is unrecoverable, use the media option.

Options

```
media—(Optional) In addition to removing all configuration and log files, the media option causes memory and the media to be scrubbed, removing all traces of any user-created files. Every storage device attached to the system is scrubbed, including disks, flash drives, removable USBs, and the like. The duration of the scrubbing process is dependent on the size of the media being erased. As a result, the request system zeroize media operation can take considerably more time than the request system zeroize operation. However, the critical security parameters are all removed at the beginning of the process.
```

Required Privilege Level

maintenance

Related Documentation

- request system snapshot on page 614
- request system snapshot
- Reverting to the Default Factory Configuration for the EX Series Switch on page 504
- Reverting to the Rescue Configuration for the EX Series Switch on page 507
- Reverting to the Default Factory Configuration
Reverting to the Rescue Configuration
Reverting to the Default Factory Configuration by Using the request system zeroize Command

List of Sample Output
request system zeroize on page 553
request system zeroize media on page 554

Sample Output
request system zeroize

user@host> request system zeroize
warning: System will be rebooted and may not boot without configuration
Erase all data, including configuration and log files? [yes,no] (no) yes

0 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 5d19h20m26s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Mar 11 2011 - 04:39:06)
Board: EX4200-24T 2.11
EPLD: Version 6.0 (0x85)
DRAM: Initializing (1024 MB)
FLASH: 8 MB

Firmware Version: --- 01.00.00 ---
USB: scanning bus for devices... 2 USB Device(s) found
     scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.4
(user@juniper.net, Fri Mar 11 03:03:36 UTC 2011)
Memory: 1024MB
bootsequencing is enabled
bootsuccess is set
new boot device = disk0s1:
Loading /boot/defaultsl/loader.conf
/kernel data=0x915c84+0xa1260 syms=[0x4+0x7cbd0+0x4+0xb1c19]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel]...
Kernel entry at 0x8000000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
The Regents of the University of California. All rights reserved.
JUNOS 11.1R1.8 #0: 2011-03-09 20:14:25 UTC
user@juniper.net:/volume/build/junos/11.1/release/11.1R1.8/obj-powerpc/bsd/kernels/
JUNIPER-EX/kernel
Timecounter "decrementer" frequency 50000000 Hz quality 0
   cpu0: Freescale e500v2 core revision 2.2
   cpu0: HID0 80004080
...

request system zeroize media

user@host> request system zeroize media
warning: System will be rebooted and may not boot without configuration
   Erase all data, including configuration and log files? [yes,no] (no) yes
warning: ipsec-key-management subsystem not running - not needed by configuration.
warning: zeroizing fpc0

{master:0}
root> Waiting (max 60 seconds) for system process `vnlru' to stop...done
   .
   .
Syncing disks, vnodes remaining...2 4 2 4 3 2 1 1 0 0 0 done

syncing disks... All buffers synced.
Uptime: 14m50s
recorded reboot as normal shutdown
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)
Board: EX4200-48PX 1.1
EPLD:  Version 8.0 (0x82)
DRAM:  Initializing (512 MB)
FLASH:  8 MB
NAND:  No NAND device found!!!
       0 MiB
Firmware Version: --- 01.00.00 ---
USB:   scanning bus for devices... 2 USB Device(s) found
       scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2
(vtseng@svl-junos-pool27.juniper.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
   Booting [/kernel] in 1 second... Booting [/kernel]...
   Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
   All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
   The Regents of the University of California. All rights reserved.
JUNOS 11.4R1.2 #0: 2011-10-27 18:05:39 UTC
# Chapter 16: Administration

... user@juniper.net:/volume/build/junos/11.4/release/11.4R1.2/obj-powerpc/bsd/kernels/JUNIPER-EX/kernel
can’t re-use a leaf (all_slot_serialid)!
Timecounter "decrementer" frequency 50000000 Hz quality 0
cpu0: Freescale e500v2 core revision 2.2
cpu0: HDIO 80004080<EMCP,TBEN,EN_MAS7_UPDATE>
real memory = 511705088 (488 MB)
avail memory = 500260864 (477 MB)
ETHERNET SOCKET BRIDGE initialising
Initializing EXSERIES platform properties ...
... Automatic reboot in progress...
Media check on da0 on ex platforms
** /dev/da0s2a
FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20055 free (31 frags, 2503 blocks, 0.0% fragmentation)
zeroizing /dev/da0s1a ...
... zeroizing /dev/da0s3d ...
... zeroizing /dev/da0s4d ...
... zeroizing /dev/da0s4e ...
syncing disks... All buffers synced.
Uptime: 3m40s
Rebooting...

U-Boot 1.1.6 (Apr 21 2011 - 13:58:42)
Board: EX4200-48PX 1.1
EPLD: Version 8.0 (0x82)
DRAM: Initializing (512 MB)
FLASH: 8 MB
NAND: No NAND device found!!!
0 MiB
Firmware Version: --- 01.00.00 ---
USB: scanning bus for devices... 2 USB Device(s) found
scanning bus for storage devices... 1 Storage Device(s) found

ELF file is 32 bit
Consoles: U-Boot console

FreeBSD/PowerPC U-Boot bootstrap loader, Revision 2.2
(vtseng@svl-junos-pool27.juniper.net, Fri Feb 26 17:48:51 PST 2010)
Memory: 512MB
Loading /boot/defaults/loader.conf
/kernel data=0x9abfdc+0xb06e4 syms=[0x4+0x83b30+0x4+0xbd7c6]

Hit [Enter] to boot immediately, or space bar for command prompt.
Booting [/kernel] in 1 second... Booting [/kernel]...
Kernel entry at 0x800000e0 ...
GDB: no debug ports present
KDB: debugger backends: ddb
KDB: current backend: ddb
Copyright (c) 1996-2011, Juniper Networks, Inc.
All rights reserved.
can't re-use a leaf (all_slot_serialid)!

Timecounter "decrementer" frequency 50000000 Hz quality 0

cpu0: Freescale e500v2 core revision 2.2

real memory = 511705088 (488 MB)
avail memory = 500260864 (477 MB)

etheren t socket BRIDGE initialising

Automatic reboot in progress...

Media check on da0 on ex platforms
** /dev/da0s1a

FILE SYSTEM CLEAN; SKIPPING CHECKS
clean, 20064 free (48 frags, 2502 blocks, 0.1% fragmentation)
zeroizing /dev/da0s2a ...

Creating initial configuration...mgd: error: Cannot open configuration file: /config/juniper.conf
mgd: warning: activating factory configuration
mgd: commit complete
mgd: ----------------------------------------------------------
mgd: Please login as 'root'. No password is required.
mgd: To start Initial Setup, type 'ezsetup' at the JUNOS prompt.
mgd: To start JUNOS CLI, type 'cli' at the JUNOS prompt.
mgd: ----------------------------------------------------------

Setting initial options: debugger_on_panic=NO debugger_on_break=NO.
Starting optional daemons: ,
Doing initial network setup: ...

Amnesiac (ttyu0)
show system commit

**Syntax**
show system commit

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Display the system commit history and any pending commit operation.

**Options**
This command has no options.

**Required Privilege**
view

**Related Documentation**
- clear system commit on page 529
- show system commit (On a Particular Time) on page 558
- show system commit (At the Next Reboot) on page 558
- show system commit (Rollback Pending) on page 558
- show system commit (QFX Series) on page 558

**List of Sample Output**
show system commit on page 558
show system commit (At a Particular Time) on page 558
show system commit (At the Next Reboot) on page 558
show system commit (Rollback Pending) on page 558
show system commit (QFX Series) on page 558

**Output Fields**
Table 96 on page 557 describes the output fields for the `show system commit` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junos XML protocol</td>
<td>Displays the last 50 commit operations listed, most recent to first. The identifier <strong>Junos XML protocol</strong> designates a configuration created for recovery using the <strong>request system configuration rescue save</strong> command.</td>
</tr>
<tr>
<td>Junos XML protocol</td>
<td>Date and time of the commit operation.</td>
</tr>
<tr>
<td>Junos XML protocol</td>
<td>User who executed the commit operation.</td>
</tr>
<tr>
<td>Junos XML protocol</td>
<td>Method used to execute the commit operation:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Junos XML protocol</strong>—CLI interactive user performed the commit operation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Junos XML protocol</strong>—Junos XML protocol client performed the commit operation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>synchronize</strong>—The <strong>commit synchronize</strong> command was performed on the other Routing Engine.</td>
</tr>
<tr>
<td></td>
<td>• <strong>snmp</strong>—An SNMP <strong>set</strong> request caused the commit operation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>button</strong>—A button on the router or switch was pressed to commit a rescue configuration for recovery.</td>
</tr>
<tr>
<td></td>
<td>• <strong>autoinstall</strong>—A configuration obtained through autoinstallation was committed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>other</strong>—When there is no login name associated with the session, the values for user and client default to root and other. For example, during a reboot after package installation, mgd commits the configuration as a system commit, and there is no login associated with the commit.</td>
</tr>
</tbody>
</table>
Sample Output

show system commit

```
user@host> show system commit
commit requested by root via cli at Tue May 7 15:59:00 2002
```

show system commit (At a Particular Time)

```
user@host> show system commit
commit requested by root via cli at Tue May 7 15:59:00 2002
```

show system commit (At the Next Reboot)

```
user@host> show system commit
commit requested by root via cli at reboot
```

show system commit (Rollback Pending)

```
user@host> show system commit
commit requested by root via cli at Tue May 7 15:59:00 2002
```

show system commit (QFX Series)

```
user@switch> show system commit
commit requested by root via cli at Tue May 7 15:59:00 2002
```
show system configuration archival

Syntax
show system configuration archival

Release Information
Introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display directory and number of files queued for archival transfer.

NOTE: The [edit system configuration] hierarchy is not available on QFabric systems.

Options
This command has no options.

Required Privilege Level
maintenance

List of Sample Output
show system configuration archival on page 559

Sample Output
show system configuration archival

user@host> show system configuration archival
/var/transfer/config/: total 8
**show system configuration rescue**

**Syntax**
show system configuration rescue

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Display a rescue configuration, if one exists.

**NOTE:** The [edit system configuration] hierarchy is not available on QFabric systems.

**Options**
This command has no options.

**Required Privilege**
maintenance

**Related Documentation**
- show system configuration archival on page 559

**List of Sample Output**
show system configuration rescue on page 560

**Sample Output**

```plaintext
show system configuration rescue

user@switch> show system configuration rescue
version "7.3"; groups {
    global {
        system {
            host-name router1;
            domain-name customer.net;
            domain-search [ customer.net ];
            backup-router 192.168.124.254;
            name-server {
                172.17.28.11;
                172.17.28.101;
                172.17.28.100;
                172.17.28.10;
            }
        }
        login {
            user regress {
                uid 928;
                class ;
                shell csh;
                authentication {
                    encrypted-password "$1$kPU..$w.4FGRAGanJ8U4Yq6sbj7."; ##
                }
            }
        }
    }
}
```
ftp;
  rlogin;
  rsh;
  telnet;
}
}
}
show system rollback

Syntax
show system rollback number
<compare number>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display the contents of a previously committed configuration, or the differences between two previously committed configurations.

NOTE: The show system rollback command is a purely operational mode command and cannot be issued with run from the configuration mode.

Options
number—Number of a configuration to view. The output displays the configuration. The range of values is 0 through 49.

compare number—(Optional) Number of another previously committed (rollback) configuration to compare to rollback number. The output displays the differences between the two configurations. The range of values is 0 through 49.

Required Privilege
view

List of Sample Output
show system rollback compare on page 562

Sample Output
show system rollback compare

user@host> show system rollback 3 compare1
[edit]
+ interfaces {
+    ge-1/1/1 {
+        unit 0 {
+            family inet {
+                filter {
+                    input mf_plp;
+                }
+            } address 14.1.1.1/30;
+        }
+    }
+    ge-1/2/1 {
+        unit 0 {
+            family inet {
+                filter {
+                    input mf_plp;
+                }
+            } address 13.1.1.1/30;
+        }
+}
+     }
+   }
+  ge-1/3/0 {
+    unit 0 {
+      family inet {
+        filter {
+          input mf_plp;
+        }
+        address 12.1.1.1/30;
+      }
+    }
+  }
+}
+
test configuration

**Syntax**

```plaintext
test configuration filename
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Verify that the syntax of a configuration file is correct. If the configuration contains any syntax or commit check errors, a message is displayed to indicate the line number and column number in which the error was found.

**Options**

- `filename`—Name of the configuration file.
- `syntax-only`—Check the syntax of a partial configuration file, without checking for commit errors. This option introduced in Junos OS Release 12.1.

**Required Privilege**

- Level: `view`

**List of Sample Output**

`test configuration on page 564`

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```plaintext
user@host> test configuration terminal
[Type ^D to end input]
system {
  host-name bluesky;
  paris-23;
  login;
}
terminal:3:(8) syntax error: paris
[edit system]
  'paris-23;'
syntax error
terminal:4:(11) statement must contain additional statements: ;
[edit system login]
  'login ;'
  statement must contain additional statements
configuration syntax failed
```
Troubleshooting Procedures

- Troubleshooting Loss of the Root Password on page 565

**Troubleshooting Loss of the Root Password**

**Problem**

If you forget the root password for the switch, you can use the password recovery procedure to reset the root password.

**NOTE:** You need physical access to the switch to recover the root password.

**Solution**

To recover the root password:

1. Power off your switch by unplugging the power cord or turning off the power at the wall switch.

2. Insert one end of the Ethernet cable into the serial port on the management device and connect the other end to the console port on the back of the switch. See Figure 1 on page 379

**Figure 4: Connecting to the Console Port on the EX Series Switch**

3. On the management device, start your asynchronous terminal emulation application (such as Microsoft Windows Hyperterminal) and select the appropriate **COM** port to use (for example, **COM1**).
4. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

5. Power on your switch by plugging in the power cord or turning on the power at the wall switch.

6. When the following prompt appears, press the Spacebar to access the switch’s bootstrap loader command prompt:
   Hit [Enter] to boot immediately, or space bar for command prompt.
   Booting [kernel] in 1 second...

7. At the following prompt, type `boot -s` to start up the system in single-user mode:
   `loader> boot -s`

8. At the following prompt, type `recovery` to start the root password recovery procedure:
   Enter full path name of shell or 'recovery' for root password recovery or RETURN for `/bin/sh: recovery`
   A series of messages describe consistency checks, mounting of filesystems, and initialization and checkout of management services. Then the CLI prompt appears.

9. Enter configuration mode in the CLI:
   `user@switch> configure`

10. Set the root password. For example:
    `user@switch# set system root-authentication plain-text-password`

11. At the following prompt, enter the new root password. For example:
    `New password: juniper1`
        Retype new password:

12. At the second prompt, reenter the new root password.

13. If you are finished configuring the network, commit the configuration.
    `root@switch# commit`
        commit complete

14. Exit configuration mode in the CLI.
    `root@switch# exit`

15. Exit operational mode in the CLI.
    `root@switch> exit`

16. At the prompt, enter `y` to reboot the switch.
    `Reboot the system? [y/n] y`

Related Documentation

- Connecting and Configuring an EX Series Switch (CLI Procedure)
• **Connecting and Configuring an EX Series Switch (J-Web Procedure)**

• For information about configuring an encrypted root password, configuring SSH keys to authenticate root logins, and configuring special requirements for plain-text passwords, see the *Junos OS System Basics Configuration Guide*. 
PART 7

Software Installation

- Overview on page 571
- Configuration on page 589
- Administration on page 597
- Troubleshooting Procedures on page 657
Overview

- Installation Overview on page 571
- Software Overview on page 578
- Licenses Overview on page 580

Installation Overview

- Understanding Software Installation on EX Series Switches on page 571
- Understanding System Snapshot on EX Series Switches on page 573
- Understanding Resilient Dual-Root Partitions on Switches on page 575
- Junos OS Package Names on page 578

Understanding Software Installation on EX Series Switches

A Juniper Networks EX Series Ethernet Switch is delivered with the Juniper Networks Junos operating system (Junos OS) preinstalled. As new features and software fixes become available, you must upgrade your software to use them. You can also downgrade Junos OS to a previous release.

This topic covers:

- Overview of the Software Installation Process on page 571
- Software Package Security on page 572
- Installing Software on a Virtual Chassis on page 572
- Installing Software on Switches with Redundant Routing Engines on page 572
- Installing Software Using Automatic Software Download on page 573
- Troubleshooting Software Installation on page 573

Overview of the Software Installation Process

An EX Series switch is delivered with Junos OS preinstalled. When you connect power to the switch, it starts (boots) from the installed software.

You upgrade Junos OS on an EX Series switch by copying a software package to your switch or another system on your local network, then use either the J-Web interface or the command-line interface (CLI) to install the new software package on the switch.
Finally, you reboot the switch; it boots from the upgraded software. After a successful upgrade, you should back up the new current configuration to a secondary device.

During a successful upgrade, the upgrade package removes all files from /var/tmp and completely reinstalls the existing software. It retains configuration files, and similar information, such as secure shell and host keys, from the previous version. The previous software package is preserved in a separate disk partition, and you can manually revert back to it if necessary. If the software installation fails for any reason, such as loss of power during the installation process, the system returns to the originally active installation when you reboot.

**Software Package Security**

All Junos OS releases are delivered in signed packages that contain digital signatures to ensure official Juniper Networks software. For more information about signed software packages, see the [Junos OS Installation and Upgrade Guide](#).

**Installing Software on a Virtual Chassis**

You can connect individual EX Series switches together to form one unit and manage the unit as a single device, called a Virtual Chassis. The Virtual Chassis operates as a single network entity composed of member switches. Each member switch in a Virtual Chassis must be running the same version of Junos OS. See “EX Series Switch Software Features Overview” on page 27 for a list of switches that can be used in a Virtual Chassis.

For ease of management, a Virtual Chassis provides flexible methods to upgrade software releases. You can deploy a new software release to all member switches of a Virtual Chassis or to only a particular member switch.

You can also upgrade the software on an EX4200, EX4500, mixed EX4200 and EX4500, and EX8200 Virtual Chassis using nonstop software upgrade (NSSU). NSSU takes advantage of graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) to ensure no disruption to the control plane during the upgrade. You can minimize disruption to network traffic by defining link aggregation groups (LAGs) such that the member links of each LAG reside on different line cards (on EX8200 Virtual Chassis) or on different members (on EX4200, EX4500, mixed EX4200 and EX4500 Virtual Chassis). During an NSSU, the line cards and Virtual Chassis members are upgraded one at a time, so that traffic continues to flow through the other line cards or members while that line card or member is being upgraded.

**Installing Software on Switches with Redundant Routing Engines**

You can install software on a switch with redundant Routing Engines in one of two ways:

- **Perform an NSSU**—An NSSU upgrades both Routing Engines with a single command and with a minimum of network disruption. An NSSU takes advantage of GRES and NSR to ensure no disruption to the control plane. You can minimize disruption to network traffic by defining LAGs such that the member links of each LAG reside on different line cards. The line cards are upgraded one at a time, so that traffic continues to flow through the other line cards while a line card is being upgraded.

  You cannot use NSSU to downgrade the software running on a switch.
For more information about NSSU, see *Understanding Nonstop Software Upgrade on EX Series Switches*. See “EX Series Switch Software Features Overview” on page 27 for a list of switches that support NSSU.

- Upgrade each Routing Engine manually—You can perform a Junos OS installation on each Routing Engine separately, starting with the backup Routing Engine. You can use this procedure to downgrade the software running on a switch. See *Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)*.

**Installing Software Using Automatic Software Download**

The automatic software download feature uses the DHCP message exchange process to download and install software packages. Users can define a path to a software package on the DHCP server and then the DHCP server communicates this path to EX Series switches acting as DHCP clients as part of the DHCP message exchange process. The DHCP clients that have been configured for automatic software download receive these messages and, when the software package name in the DHCP server message is different from that of the software package that booted the DHCP client switch, download and install the software package. See *Upgrading Software Using Automatic Software Download*.

**Troubleshooting Software Installation**

If Junos OS loads but the CLI is not working for any reason, or if the switch has no software installed, you can use the recovery installation procedure to install the software on the switch. See “Troubleshooting Software Installation” on page 657.

---

**NOTE:** You can also use this procedure to load two versions of Junos OS in separate partitions on the switch.

---

**Related Documentation**

- *Downloading Software Packages from Juniper Networks*
- *Installing Software on EX Series Switches (J-Web Procedure)*
- *Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)*
- *Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)*
- *Understanding Nonstop Software Upgrade on EX Series Switches*

**Understanding System Snapshot on EX Series Switches**

You can create copies of the software running a Juniper Networks EX Series Ethernet Switch using the system snapshot feature. The system snapshot feature takes a “snapshot” of the files currently used to run the switch and copies them to an alternate storage location. You can then use this snapshot to boot the switch at the next bootup or as a backup boot option.

The switch can boot from either internal flash media or external (USB) flash media. The contents of the snapshot vary depending on whether you create the snapshot on the media that the switch booted from or on the media that it did not boot from:
Snapshots are particularly useful for moving files onto USB flash drives. You cannot use the `copy` command or any other file-moving technique to move files from an internal memory source to USB memory on the switch.

- If you create the snapshot on the media that the switch did not boot from, the following partitions on the boot media are included in the snapshot: `root`, `altroot`, `var`, `var/tmp`, `config`.

  The `root` partition is the primary boot partition, and the `altroot` partition is the backup boot partition.

- If you create the snapshot on the media that the switch booted from, the root partition that the switch booted from is copied to the alternate root partition. The `var`, `var/tmp`, and `config` partitions are not copied as part of the snapshot because they already exist on the boot media.

The system snapshot feature has the following limitations:

- You cannot use snapshots to move files to any destination outside the switch other than an installed external USB flash drive or switches that are members of the same Virtual Chassis as the switch on which you created the snapshot.

- Snapshot commands, like all commands executed on a Virtual Chassis, are executed on the local member switch. If different member switches request the snapshot, the snapshot command is pushed to the Virtual Chassis member creating the snapshot and is executed on that member, and the output is then returned to the switch that initiated the process. For instance, if the command to create an external snapshot on member 3 is entered on member 1, the snapshot of internal memory on member 3 is taken on external memory on member 3. The output of the process is seen on member 1. No files move between the switches.

Related Documentation

- Understanding Software Installation on EX Series Switches on page 571
- Creating a Snapshot and Using It to Boot an EX Series Switch on page 591
Understanding Resilient Dual-Root Partitions on Switches

Resilient dual-root partitioning, introduced on Juniper Networks EX Series Ethernet Switches in Juniper Networks Junos operating system (Junos OS) Release 10.4R3, provides additional resiliency to switches in the following ways:

- Allows the switch to boot transparently from the second (alternate) root partition if the system fails to boot from the primary root partition.
- Provides separation of the root Junos OS file system from the /var file system. If corruption occurs in the /var file system (a higher probability than in the root file system because of the greater frequency in /var of reads and writes), the root file system is insulated from the corruption.

NOTE: For instructions on upgrading Junos OS (from a release prior to Release 10.4R3) to a release that supports resilient dual-root partitions, see the release notes (New Features in Junos OS Release 11.2 for EX Series Switches).

This topic covers:

- Resilient Dual-Root Partition Scheme (Junos OS Release 10.4R3 and Later) on page 575
- Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature on page 576
- Earlier Partition Scheme (Junos OS Release 10.4R2 and Earlier) on page 577
- Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases on page 577

Resilient Dual-Root Partition Scheme (Junos OS Release 10.4R3 and Later)

EX Series switches that ship with Junos OS Release 10.4R3 or later are configured with a root partition scheme that is optimized for resiliency, as shown in Table 97 on page 575.

Table 97: Resilient Dual-Root Partition Scheme

<table>
<thead>
<tr>
<th>Slice 1</th>
<th>Slice 2</th>
<th>Slice 3</th>
<th>Slice 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>s2a</td>
<td>s3e</td>
<td>s3d</td>
</tr>
<tr>
<td>/</td>
<td>/</td>
<td>/var</td>
<td>/var/tmp</td>
</tr>
</tbody>
</table>

(root Junos OS) (root Junos OS)

In the resilient dual-root partition scheme, the /var file system is contained in a separate slice (Slice 3) from the root file systems; the /config directory is contained in its own slice (Slice 4), and switches ship from the factory with identical Junos OS images in Slice 1 and Slice 2. The /var file system, which has a greater frequency of reads and writes than the root file systems and is therefore more likely to have corruption issues, is isolated from the root directories and the /config directory. If the switch fails to boot from the
active partition, the switch automatically boots from the alternate root partition and triggers an alarm.

**Automatic Fixing of Corrupted Primary Root Partition with the Automatic Snapshot Feature**

Resilient dual-root partitioning also provides the *automatic snapshot* feature. You can enable the automatic snapshot feature for the system to automatically fix the corrupt Junos OS file in the primary root partition. If you enable the automatic snapshot feature, the switch automatically takes a snapshot of the Junos OS root file system in the alternate root partition and copies it onto the primary root partition, thereby repairing the corrupt file in the primary root partition. The automatic snapshot procedure takes place whenever the system reboots from the alternate root partition, regardless of whether the reboot is due to a command or due to a corruption of the primary root partition.

**NOTE:**
- On EX4550 switches, the automatic snapshot feature is enabled by default.
- On other EX Series switches, you can enable the automatic snapshot feature by configuring the `auto-snapshot` statement at the `[edit system]` hierarchy level.
- If the automatic snapshot feature is enabled in a Virtual Chassis configuration, the automatic snapshot procedure takes place whenever any member of the Virtual Chassis has rebooted from its alternate root partition.

The automatic snapshot feature provides an additional layer of fault protection if you maintain the same version of Junos OS in both partitions of resilient dual-root partitions. The repair happens automatically. Therefore, when `auto-snapshot` is enabled, the switch does not issue an alarm to indicate that the system has been rebooted from the alternate partition. However, it does log the event. You cannot execute a manual snapshot when an automatic snapshot procedure is in process. The login banner indicates that an automatic snapshot operation is in progress and that banner is removed when the snapshot operation is complete. The next reboot happens from the primary partition.

**NOTE:** EX Series switches that ship with Junos OS Release 10.4R3 or later are configured with identical Junos OS images in the primary root partition (Slice 1) and the alternate root partition (Slice 2).

However, if you do *not* maintain the same version of Junos OS in both partitions, you might want to disable the automatic snapshot feature. If you have an older version of Junos OS in the alternate partition and the system reboots from the alternate root partition, the automatic snapshot feature replaces the newer Junos OS version with the older version.

When automatic snapshot is disabled and the system reboots from the alternate root partition, it also triggers an alarm indicating that the system has rebooted from its alternate partition.
Earlier Partition Scheme (Junos OS Release 10.4R2 and Earlier)

The partition scheme used in Junos OS 10.4R2 and earlier is shown in Table 98 on page 577.

Table 98: Earlier Partition Scheme

<table>
<thead>
<tr>
<th>Slice 1</th>
<th>Slice 2</th>
<th>Slice 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>s2a</td>
<td>s3a</td>
</tr>
<tr>
<td>s1f</td>
<td>s2f</td>
<td>s3d</td>
</tr>
<tr>
<td>/</td>
<td>/var</td>
<td>/var</td>
</tr>
<tr>
<td>(root Junos OS)</td>
<td>(empty until initial software upgrade)</td>
<td>(empty until initial software upgrade)</td>
</tr>
</tbody>
</table>

This is the partitioning scheme for a switch shipped with Release 10.4R2 or earlier (or after you reformat the disk during a downgrade from Release 10.4R3 or later to Release 10.4R2 or earlier). In this partitioning scheme, the switch comes from the factory with only one Junos OS image installed in the root Junos OS partition of Slice 1. The first time that you perform a software upgrade, the new Junos OS image is installed in Slice 2. If the switch fails to boot, you must manually trigger it to boot from the alternate partition (rebooting from the alternate partition does not occur automatically).

Understanding Upgrading or Downgrading Between Resilient Dual-Root Partition Releases and Earlier Releases

Upgrading from Release 10.4R2 or earlier to Release 10.4R3 or later differs from other upgrades in two important ways:

- You must install a new loader software package in addition to installing the new Junos OS image.
- Rebooting after the upgrade reformats the disk from three partitions to four partitions. See Table 97 on page 575.

You can perform all operations for this special software upgrade from the CLI.

CAUTION: Back up any important log files because the /var/log files are not saved or restored during an upgrade from Release 10.4R2 or earlier to a release that supports resilient dual-root partitions (Release 10.4R3 or later).

We recommend that you also save your /config files and any important log files to an external medium because if there is a power interruption during the upgrade process, they might be lost.

Related Documentation

- Resilient Dual-Root Partitions Frequently Asked Questions
- EX Series Virtual Chassis Overview
- EX8200 Virtual Chassis Overview
Junos OS Package Names

You upgrade the Juniper Networks Junos operating system (Junos OS) on a Juniper Networks EX Series Ethernet Switch by copying a software package to your switch or another system on your local network, then install the new software package on the switch.

A software package name is in the following format:

\texttt{package-name-m.nZx.y-domestic-signed.tgz}

where:

- \texttt{package-name} is the name of the package—for example, \texttt{jinstall-ex-4200}.
- \texttt{m.n} is the software release, with \texttt{m} representing the major release number and \texttt{n} representing the minor release number—for example, \texttt{9.5}.
- \texttt{Z} indicates the type of software release, where \texttt{R} indicates released software and \texttt{B} indicates beta-level software.
- \texttt{x.y} represents the version of the major software release (\texttt{x}) and an internal tracking number (\texttt{y})—for example, \texttt{1.6}.
- \texttt{domestic-signed} is appended to all EX Series package names. For most Junos packages, \texttt{domestic} is used for the United States and Canada and \texttt{export} for worldwide distribution. However, for EX Series software, \texttt{domestic} is used for worldwide distribution as well.

A sample EX Series software package name is:

\texttt{jinstall-ex-4200-9.5R1.6-domestic-signed.tgz}

Related Documentation

- \textit{Installing Software on EX Series Switches (J-Web Procedure)}
- \textit{Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)}
- \textit{Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)}
- \textit{Downloading Software Packages from Juniper Networks}
- \textit{Understanding Software Installation on EX Series Switches on page 571}

Software Overview

- \textit{Understanding Software Infrastructure and Processes on page 579}
Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 579
- Junos OS Processes on page 579

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.
- Routing Engine—Provides three main functions:
  - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network
  - Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
  - Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

Junos OS Processes

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 61 on page 112 describes the primary Junos OS processes.
### Table 99: Junos OS Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis process</td>
<td>chassisd</td>
<td>Detects hardware on the system that is used to configure network interfaces. Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered. Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</td>
</tr>
<tr>
<td>Ethernet switching process</td>
<td>eswd</td>
<td>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces. Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>Forwarding process</td>
<td>pfern</td>
<td>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</td>
</tr>
<tr>
<td>Interface process</td>
<td>dcd</td>
<td>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</td>
</tr>
<tr>
<td>Management process</td>
<td>mgd</td>
<td>Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the switch. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</td>
</tr>
<tr>
<td>Routing protocol process</td>
<td>rpd</td>
<td>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- For more information about processes, see *Junos OS Network Operations Guide*
- For more information about basic system parameters, supported protocols, and software processes, see *Junos OS System Basics Configuration Guide*

**Licenses Overview**

- Understanding Software Licenses for EX Series Switches on page 581
Understanding Software Licenses for EX Series Switches

To enable and use some of the Juniper Networks operating system (Junos OS) features, you must purchase, install, and manage separate software licenses. If the switch has the appropriate software license, you can configure and use these features.

The Junos OS feature license (that is, the purchased authorization code) is universal. However, to conform to Junos OS feature licensing requirements, you must install a unique license key (a combination of the authorization code and the switch’s serial number) on each switch.

For a Virtual Chassis deployment, two license keys are recommended for redundancy—one for the device in the master role and the other for the device in the backup role:

- In an EX8200 Virtual Chassis, the devices in the master and backup roles are always XRE200 External Routing Engines.
- In all other Virtual Chassis, the devices in the master and backup roles are switches.

You do not need additional license keys for Virtual Chassis member switches that are in the linecard role or for the redundant Routing Engine (RE) modules or the redundant Switch Fabric and Routing Engine (SRE) modules in an EX8200 member switch.

This topic describes:

- Purchasing a Software Feature License on page 581
- Features Requiring a License on EX2200 Switches on page 582
- Features Requiring a License on EX3300 Switches on page 583
- Features Requiring a License on EX4300 Switches on page 584
- Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches on page 585
- License Warning Messages on page 586

Purchasing a Software Feature License

The following sections list features that require separate licenses. To purchase a software license, contact your Juniper Networks sales representative (http://www.juniper.net/us/en/contact-us/sales-offices). You will be asked to supply the chassis serial number of your switch; you can obtain the serial number by running the show chassis hardware command.
NOTE: You are required to provide the 12-digit serial number when purchasing a license for an XRE200 External Routing Engine in an EX8200 Virtual Chassis.

The serial number listed on the XRE200 External Routing Engine serial ID label is 16 digits long. Use the last 12 digits of the 16-digit serial number to purchase the license.

You can use the `show chassis hardware` command output to display the 12-digit serial number of the XRE200 External Routing Engine.

**Features Requiring a License on EX2200 Switches**

For EX2200 switches, the following features can be added to basic Junos OS by installing an enhanced feature license (EFL):

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- OSPFv1/v2 (with four active interfaces)
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Real-time performance monitoring (RPM)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 100 on page 582 lists the EFLs that you can purchase for EX2200 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX2200 switch.

**Table 100: Junos OS EFL Part Number on EX2200 Switches**

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>EFL Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200-C-12P-2G</td>
<td>EX-12-EFL</td>
</tr>
<tr>
<td>EX2200-C-12T-2G</td>
<td></td>
</tr>
<tr>
<td>EX2200-24T-4G</td>
<td>EX-24-EFL</td>
</tr>
<tr>
<td>EX2200-24P-4G</td>
<td></td>
</tr>
<tr>
<td>EX2200-24T-DC-4G</td>
<td></td>
</tr>
<tr>
<td>EX2200-48T-4G</td>
<td>EX-48-EFL</td>
</tr>
<tr>
<td>EX2200-48P-4G</td>
<td></td>
</tr>
</tbody>
</table>
Features Requiring a License on EX3300 Switches

Two types of licenses are available on EX3300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX3300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- IPv6 routing protocols: Multicast Listener Discovery version 1 and 2 (MLD v1/v2), OSPFv3, PIM multicast, VRRPv6, virtual router support for unicast and filter-based forwarding (FBF)
- OSPFv1/v2
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Q-in-Q tunneling (IEEE 802.1ad)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 101 on page 583 lists the EFLs that you can purchase for EX3300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX3300 switch.

Table 101: Junos OS EFL Part Number on EX3300 Switches

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>EFL Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3300-24T</td>
<td>EX-24-EFL</td>
</tr>
<tr>
<td>EX3300-24P</td>
<td>EX-24-EFL</td>
</tr>
<tr>
<td>EX3300-24T-DC</td>
<td>EX-24-EFL</td>
</tr>
<tr>
<td>EX3300-48T</td>
<td>EX-48-EFL</td>
</tr>
<tr>
<td>EX3300-48T-BF</td>
<td>EX-48-EFL</td>
</tr>
<tr>
<td>EX3300-48P</td>
<td>EX-48-EFL</td>
</tr>
</tbody>
</table>

To use the following feature on EX3300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- IPv6 routing protocols: IPv6 BGP and IPv6 for MBGP
- Virtual routing and forwarding (VRF) BGP

Table 102 on page 584 lists the AFLs that you can purchase for EX3300 switch models. For EX3300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX3300 switch.
### Features Requiring a License on EX4300 Switches

Two types of licenses are available on EX4300 switches: enhanced feature licenses (EFLs) and advanced feature licenses (AFLs).

To use the following features on the EX4300 switches, you must install an EFL:

- Bidirectional Forwarding Detection (BFD)
- Connectivity fault management (IEEE 802.1ag)
- IGMP (Internet Group Management Protocol) version 1 (IGMPv1), IGMPv2, and IGMPv3
- Multicast Source Discovery Protocol (MSDP)
- OSPFv2/v3
- Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
- Real-time performance monitoring (RPM)
- RIPng (RIP next generation)
- Unicast reverse-path forwarding (RPF)
- Virtual Router
- Virtual Router Redundancy Protocol (VRRP)

Table 103 on page 584 lists the EFLs that you can purchase for EX4300 switch models. If you have the license, you can run all of the enhanced software features mentioned above on your EX4300 switch.

### Table 102: Junos OS AFL Part Number on EX3300 Switches

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>AFL Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3300-24T</td>
<td>EX-24-AFL</td>
</tr>
<tr>
<td>EX3300-24P</td>
<td></td>
</tr>
<tr>
<td>EX3300-24T-DC</td>
<td></td>
</tr>
<tr>
<td>EX3300-48T</td>
<td>EX-48-AFL</td>
</tr>
<tr>
<td>EX3300-48P</td>
<td></td>
</tr>
<tr>
<td>EX3300-48T-BF</td>
<td></td>
</tr>
<tr>
<td>EX3300-48P</td>
<td></td>
</tr>
</tbody>
</table>

### Table 103: Junos OS EFL Part Number on EX4300 Switches

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>EFL Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX4300-24T</td>
<td>EX4300-24-EFL</td>
</tr>
<tr>
<td>EX4300-24P</td>
<td></td>
</tr>
<tr>
<td>EX4300-48P</td>
<td>EX4300-48-EFL</td>
</tr>
<tr>
<td>EX4300-48T</td>
<td></td>
</tr>
<tr>
<td>EX4300-48T-AFI</td>
<td></td>
</tr>
<tr>
<td>EX4300-48T-DC</td>
<td></td>
</tr>
<tr>
<td>EX4300-48T-DC-AFI</td>
<td></td>
</tr>
</tbody>
</table>
To use the following features on EX4300 switches, you must install an AFL:

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)

**Table 104 on page 585** lists the AFLs that you can purchase for EX4300 switch models. For EX4300 switches, you must purchase and install a corresponding EFL along with the AFL to enable the advanced license features. If you have both these licenses, you can run all of the advanced software features mentioned above on your EX4300 switch.

**Table 104: Junos OS AFL Part Number on EX4300 Switches**

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>AFL Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX4300-24T</td>
<td>EX4300-24-AFL</td>
</tr>
<tr>
<td>EX4300-24P</td>
<td>EX4300-24-AFL</td>
</tr>
<tr>
<td>EX4300-48P</td>
<td>EX4300-48-AFL</td>
</tr>
<tr>
<td>EX4300-48T</td>
<td>EX4300-48-AFL</td>
</tr>
<tr>
<td>EX4300-48T-AFI</td>
<td>EX4300-48-AFL</td>
</tr>
<tr>
<td>EX4300-48T-DC</td>
<td>EX4300-48-AFL</td>
</tr>
<tr>
<td>EX4300-48T-DC-AFI</td>
<td>EX4300-48-AFL</td>
</tr>
</tbody>
</table>

**Features Requiring a License on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches**

To use the following features on EX3200, EX4200, EX4500, EX4550, EX8200, and EX9200 switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP) and multiprotocol BGP (MBGP)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP, IPv6 for MBGP
- Logical systems (available only on EX9200 switches)
- MPLS with RSVP-based label-switched paths (LSPs) and MPLS-based circuit cross-connects (CCC) (Not supported on EX9200 switches)

To use the following features on Juniper Networks EX6200 Ethernet Switches, you must install an advanced feature license (AFL):

- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)
- IPv6 routing protocols: IS-IS for IPv6, IPv6 BGP

**Table 105 on page 586** lists the AFLs that you can purchase for EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 switches. If you have the license, you can run all of the advanced software features mentioned above on your EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, or EX9200 switch.
Table 105: Junos OS AFL Part Number on EX3200, EX4200, EX4500, EX4550, EX6200, EX8200, and EX9200 Switches

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>AFL Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3200-24P</td>
<td>EX-24-AFL</td>
</tr>
<tr>
<td>EX3200-24T</td>
<td></td>
</tr>
<tr>
<td>EX4200-24F</td>
<td></td>
</tr>
<tr>
<td>EX4200-24P</td>
<td></td>
</tr>
<tr>
<td>EX4200-24PX</td>
<td></td>
</tr>
<tr>
<td>EX4200-24T</td>
<td></td>
</tr>
<tr>
<td>EX3200-48P</td>
<td>EX-48-AFL</td>
</tr>
<tr>
<td>EX3200-48T</td>
<td></td>
</tr>
<tr>
<td>EX4200-48F</td>
<td></td>
</tr>
<tr>
<td>EX4200-48P</td>
<td></td>
</tr>
<tr>
<td>EX4200-48PX</td>
<td></td>
</tr>
<tr>
<td>EX4200-48T</td>
<td></td>
</tr>
<tr>
<td>EX4500-40F-BF</td>
<td>EX-48-AFL</td>
</tr>
<tr>
<td>EX4500-40F-BF-C</td>
<td></td>
</tr>
<tr>
<td>EX4500-40F-FB</td>
<td></td>
</tr>
<tr>
<td>EX4500-40F-FB-C</td>
<td></td>
</tr>
<tr>
<td>EX4550</td>
<td>EX4550-AFL</td>
</tr>
<tr>
<td>EX6210</td>
<td>EX6210-AFL</td>
</tr>
<tr>
<td>EX8208</td>
<td>EX8208-AFL</td>
</tr>
<tr>
<td>EX8216</td>
<td>EX8216-AFL</td>
</tr>
<tr>
<td>EX-XRE200</td>
<td>EX-XRE200-AFL</td>
</tr>
<tr>
<td>EX9204</td>
<td>EX9204-AFL</td>
</tr>
<tr>
<td>EX9208</td>
<td>EX9208-AFL</td>
</tr>
<tr>
<td>EX9214</td>
<td>EX9214-AFL</td>
</tr>
</tbody>
</table>

License Warning Messages

For using features that require a license, you must install and configure a license key. To obtain a license key, use the contact information provided in your certificate.

If you have not purchased the AFL or EFL and installed the license key, you receive warnings when you try to commit the configuration:

```
[edit protocols]
  'bgp'
    warning: requires 'bgp' license
error: commit failed: (statements constraint check failed)
```
The system generates system log (syslog) alarm messages notifying you that the feature requires a license—for example:

Sep 3 05:59:11   craftd[806]:  Minor alarm set, BGP Routing Protocol usage requires a license
Sep 3 05:59:11   alarmd[805]:  Alarm set: License color=Yellow, class=CHASSIS, reason=BGP Routing Protocol usage requires a license
Sep 3 05:59:11   alarmd[805]:  LICENSE_EXPIRED: License for feature bgp(47) expired

Output of the `show system alarms` command displays the active alarms:

```
user@switch> show system alarms
1 alarm currently active
  Alarm time  Class  Description
2009-09-03 06:00:11 UTC  Minor  BGP Routing Protocol usage requires a license
```

Related Documentation
- Managing Licenses for the EX Series Switch (CLI Procedure) on page 592
- Managing Licenses for the EX Series Switch (J-Web Procedure) on page 593
- Monitoring Licenses for the EX Series Switch on page 602
- License Key Components for the EX Series Switch on page 601
- EX Series Switch Software Features Overview on page 27
CHAPTER 19

Configuration

- Registering the Switch on page 589
- Booting the Switch on page 589
- Managing Licenses on page 592

Registering the Switch

Registering the EX Series Switch with the J-Web Interface on page 589

Registering the EX Series Switch with the J-Web Interface

You can register your EX Series switch with the J-Web interface so that you can request technical assistance as and when required. To register an EX Series switch:

1. In the J-Web interface, select Maintain > Customer Support > Product Registration. For an EX8200 Virtual Chassis configuration, select the member from the list.

2. Click Register. Enter the serial number in the page that is displayed.

Related Documentation

- EX Series Switch Software Features Overview on page 27

Booting the Switch

- Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive on page 590
- Creating a Snapshot and Using It to Boot an EX Series Switch on page 591
Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive

There are two methods of getting Junos OS onto a USB flash drive before using the software to boot the switch. You can pre-install the software onto the USB flash drive before inserting the USB flash drive into the USB port, or you can use the system snapshot feature to copy files from internal switch memory to the USB flash drive.

To move files into USB flash memory using a system snapshot and use those files to boot the switch, see “Creating a Snapshot and Using It to Boot an EX Series Switch” on page 591. We recommend that you use this method to boot the switch from a USB flash drive if your switch is running properly.

If you need to pre-install the software onto the USB flash drive, you can use the method described in this topic. Pre-installing the Junos OS onto a USB flash drive to boot the switch can be done at any time and is particularly useful when the switch boots to the loader prompt because the switch cannot locate the Junos OS in internal flash memory.

Ensure that you have the following tools and parts available to boot the switch from a USB flash drive:

- A USB flash drive that meets the EX Series switch USB port specifications. See USB Port Specifications for an EX Series Switch.
- A computer or other device that you can use to download the software package from the Internet and copy it to the USB flash drive.

To download a Junos OS package onto a USB flash drive before inserting the USB flash drive:

1. Download the Junos OS package that you would like to place onto the EX Series switch from the Internet onto the USB flash drive using your computer or other device. See Downloading Software Packages from Juniper Networks.
2. Remove the USB flash drive from the computer or other device.
3. Insert the USB flash drive into the USB port on the switch.
4. This step can only be performed when the prompt for the loader script (loader>) is displayed. The loader script starts when the Junos OS loads but the CLI is not working for any reason or if the switch has no software installed.

Install the software package onto the switch:

```plaintext
loader> install source
```

where source represents the name and location of the Junos OS package on the USB flash drive. The Junos OS package on a flash drive is commonly stored in the root drive as the only file—for example, `file:///jinstall-ex-4200-9.4R1.5-domestic-signed.tgz`.

Related Documentation

- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)
- Installing Software on EX Series Switches (J-Web Procedure)
- See Rear Panel of an EX3200 Switch for USB port location.
See Rear Panel of an EX4200 Switch for USB port location.

See Switch Fabric and Routing Engine (SRE) Module in an EX8208 Switch for USB port location.

See Routing Engine (RE) Module in an EX8216 Switch for USB port location.

Understanding Software Installation on EX Series Switches on page 571

Creating a Snapshot and Using It to Boot an EX Series Switch

The system snapshot feature takes a “snapshot” of the files currently used to run the switch and copies them to an alternate storage location. You can then use this snapshot to boot the switch at the next bootup or as a backup boot option.

This topic includes the following tasks:

- Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch on page 591
- Creating a Snapshot on an Internal Flash Drive and Using it to Boot the Switch on page 591
- Creating a Snapshot on the Alternate Slice of the Boot Media on page 592

Creating a Snapshot on a USB Flash Drive and Using It to Boot the Switch

You can create a snapshot on USB flash memory after a switch is booted by using files stored in internal memory.

Ensure that you have the following tools and parts available before creating a snapshot on a USB flash drive:

- A USB flash drive that meets the switch USB port specifications. See USB Port Specifications for an EX Series Switch.

To create a snapshot on USB flash memory and use it to boot the switch:

1. Place the snapshot into USB flash memory:

   user@switch> request system snapshot partition media external

2. (Optional) Perform this step if you want to boot the switch now using the snapshot stored on the USB flash drive. If you created the snapshot as a backup, do not perform this step.

   - To reboot the switch using the most recently created snapshot:

     user@switch> request system reboot media external

   - To reboot the switch using a snapshot in a specific partition on the USB flash drive:

     user@switch> request system reboot media external slice alternate

Creating a Snapshot on an Internal Flash Drive and Using it to Boot the Switch

You can create a snapshot in internal memory after a switch is booted by using files stored in external memory.
To create a snapshot in internal memory and use it to boot the switch:

1. Place the snapshot files in internal memory:
   
   ```
   user@switch> request system snapshot partition media internal
   ```

2. (Optional) Perform this step if you want to boot the switch now using the newly created snapshot. If you created the snapshot as a backup, do not perform this step.
   
   - To reboot the switch using the most recently created snapshot:
     
     ```
     user@switch> request system reboot media internal
     ```
   
   - To reboot the switch using a snapshot in a specific partition in internal memory:
     
     ```
     user@switch> request system reboot media internal slice alternate
     ```

### Creating a Snapshot on the Alternate Slice of the Boot Media

The alternate slice of the boot media contains a backup software image that the switch can boot from if it is unable to boot from the primary slice. When you upgrade software, the new software image gets copied only to the primary slice of the boot media.

To create a snapshot of the currently booted software image on the backup slice of the boot media:

```
user@switch> request system reboot slice alternate
```

**Related Documentation**

- Verifying That a System Snapshot Was Created on an EX Series Switch on page 597
- Understanding System Snapshot on EX Series Switches on page 573

### Managing Licenses

- Managing Licenses for the EX Series Switch (CLI Procedure) on page 592
- Managing Licenses for the EX Series Switch (J-Web Procedure) on page 593

**Managing Licenses for the EX Series Switch (CLI Procedure)**

To enable and use some Junos OS features on an EX Series switch, you must purchase, install, and manage separate software licenses. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy. After you have configured the features, you see a warning message if the switch does not have a license for the feature.

Before you begin managing licenses, be sure that you have:

- Obtained the needed licenses. For information about how to purchase software licenses, contact your Juniper Networks sales representative.
• Understand what makes up a license key. For more information, see “License Key Components for the EX Series Switch” on page 601.

This topic includes the following tasks:

• Adding New Licenses on page 593
• Deleting Licenses on page 593
• Saving License Keys on page 593

Adding New Licenses

To add one or more new license keys on the switch, with the CLI:

1. Add the license key or keys:
   • To add one or more license keys from a file or URL, specify the filename of the file or the URL where the key is located:
     
     user@switch> request system license add filename | url

   • To add a license key from the terminal:
     
     user@switch> request system license add terminal

2. When prompted, enter the license key, separating multiple license keys with a blank line.
   
   If the license key you enter is invalid, an error appears in the CLI output when you press Ctrl+d to exit the license entry mode.

Deleting Licenses

To delete one or more license keys from the switch with the CLI, specify the license ID:

user@switch> request system license delete license-id

You can delete only one license at a time.

Saving License Keys

To save the installed license keys to a file (which can be a URL) or to the terminal:

user@switch> request system license save filename | url

For example, the following command saves the installed license keys to a file named license.conf:

user@switch> request system license save ftp://user@switch/license.conf

Related Documentation

• Managing Licenses for the EX Series Switch (J-Web Procedure) on page 593
• Monitoring Licenses for the EX Series Switch on page 602
• Understanding Software Licenses for EX Series Switches on page 581

Managing Licenses for the EX Series Switch (J-Web Procedure)

To enable and use some Junos OS features on an EX Series switch, you must purchase, install, and manage separate software licenses. Each switch requires one license. For a
Virtual Chassis deployment, two licenses are recommended for redundancy. After you have configured the features, you see a warning message if the switch does not have a license for the feature.

Before you begin managing licenses, be sure that you have:

- Obtained the needed licenses. For information about how to purchase software licenses, contact your Juniper Networks sales representative.
- Understand what makes up a license key. For more information, see "License Key Components for the EX Series Switch" on page 601.

This topic includes the following tasks:

- Adding New Licenses on page 594
- Deleting Licenses on page 594
- Displaying License Keys on page 594
- Downloading Licenses on page 595

Adding New Licenses

To add one or more new license keys on the switch, with the J-Web license manager:

1. In the J-Web interface, select Maintain > Licenses.
2. Under Installed Licenses, click Add to add a new license key or keys.
3. Do one of the following, using a blank line to separate multiple license keys:
   - In the License File URL box, type the full URL to the destination file containing the license key or keys to be added.
   - In the License Key Text box, paste the license key text, in plain-text format, for the license to be added.
4. Click OK to add the license key or keys.

A list of features that use the license key is displayed. The table also lists the ID, state, and version of the license key.

Deleting Licenses

To delete one or more license keys from a switch with the J-Web license manager:

1. In the J-Web interface, select Maintain > Licenses.
2. Select the check box of the license or licenses you want to delete.
3. Click Delete.

Displaying License Keys

To display the license keys installed on a switch with the J-Web license manager:

1. In the J-Web interface, select Maintain > Licenses.
2. Under Installed Licenses, click **Display Keys** to display all the license keys installed on the switch.

A screen displaying the license keys in text format appears. Multiple licenses are separated by a blank line.

**Downloading Licenses**

To download the license keys installed on the switch with the J-Web license manager:

1. In the J-Web interface, select **Maintain > Licenses**.

2. Under Installed Licenses, click **Download Keys** to download all the license keys installed on the switch to a single file.

3. Select **Save it to disk** and specify the file to which the license keys are to be written. You can also download the license file to your system.

**Related Documentation**

- Managing Licenses for the EX Series Switch (CLI Procedure) on page 592
- Monitoring Licenses for the EX Series Switch on page 602
- Understanding Software Licenses for EX Series Switches on page 581
CHAPTER 20

Administration

- Routine Monitoring on page 597
- Monitoring Licenses on page 601
- Operational Commands on page 603

Routine Monitoring

- Verifying That a System Snapshot Was Created on an EX Series Switch on page 597
- Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 598

Verifying That a System Snapshot Was Created on an EX Series Switch

**Purpose**   Verify that a system snapshot was created with the proper files on an EX Series switch.

**Action**   View the snapshot:

```
user@switch> show system snapshot media external
Information for snapshot on   external (/dev/da1s1a) (backup)
Creation date: Mar 19 03:37:18 2012
JUNOS version on snapshot:
  jbase  : ex-12.1I20120111_0048_user
  jcrypto-ex: 12.1I20120111_0048_user
  jdocs-ex: 12.1I20120111_0048_user
  jroute-ex: 12.1I20120111_0048_user
  jswitch-ex: 12.1I20120111_0048_user
  jweb-ex: 12.1I20120111_0048_user
Information for snapshot on   external (/dev/da1s2a) (primary)
Creation date: Mar 19 03:38:25 2012
JUNOS version on snapshot:
  jbase  : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
```

**Meaning**   The output shows the date and time when the snapshot was created and the packages that are part of the snapshot. Check to see that the date and time match the time when you created the snapshot.
You can compare the output of this command to the output of the `show system software` command to ensure that the snapshot contains the same packages as the software currently running the switch.

**Related Documentation**
- Creating a Snapshot and Using It to Boot an EX Series Switch on page 591

**Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch**

Before or after upgrading or downgrading Junos OS, you might need to verify the Junos OS version. You might also need to verify the boot loader software version if you are upgrading to or downgrading from a release that supports resilient dual-root partitions (Junos OS Release 10.4R3 and later).

This topic includes:
- Verifying the Number of Partitions and File System Mountings on page 598
- Verifying the Loader Software Version on page 599
- Verifying Which Root Partition Is Active on page 600
- Verifying the Junos OS Version in Each Root Partition on page 600

**Verifying the Number of Partitions and File System Mountings**

**Purpose**
Between Junos OS Release 10.4R2 and Release 10.4R3, upgrades were made to further increase resiliency of root partitions, which required reformating the disk from three partitions to four partitions. If your switch is running Release 10.4R2 or earlier, it has three partitions, and if it is running Release 10.4R3 or later, it has four partitions.

**Action**
Verify how many partitions the disk has, as well as where each file system is mounted, by using the following command:

```
user@switch> show system storage
fpc0:
-----------------------------------------------------------------------
Filesystem  Size  Used  Avail  Capacity Mounted on
/dev/da0s1a 184M  124M    45M     73%    /
devfs       1.0K  1.0K    0B      100%  /dev
/dev/md0     37M   37M    0B      100%  /packages/mnt/jbase
/dev/md1     18M   18M    0B      100%  /packages/mnt/jcrypto-ex-10.4I20110121_0509_hbRPSRLI15184421081
/packages/mnt/jdocs-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md2    6.1M  6.1M    0B      100%  /packages/mnt/jkernel-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md3   154M  154M    0B      100%  /packages/mnt/jswitch-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md4   23M   23M    0B      100%  /packages/mnt/jweb-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md5   46M   46M    0B      100%  /packages/mnt/jpfe-ex42x-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md6   28M   28M    0B      100%  /packages/mnt/jroute-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md7   22M   22M    0B      100%  /packages/mnt/jswitch-ex-10.4I20110121_0509_hbRPSRLI15184421081
/dev/md8   126M  10.0K 116M       0%  /tmp
/dev/da0s3e 123M  632K  112M     1%  /var
```
Meaning  The presence of the partition name containing s4d indicates that there is a fourth slice. If this were a three-slice partition scheme, in place of s1a, s2f, s2a, s2f, s3d, and s3e, you would see s1a, s1f, s2a, s2f, s3d, and s3e and you would not see s4d.

Verifying the Loader Software Version

Purpose  For the special case of upgrading from Junos OS Release 10.4R2 or earlier to Release 10.4R3 or later, you must upgrade the loader software.

Action  For EX Series switches except EX8200 switches:

user@switch> show chassis firmware
<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>uboot</td>
<td>U-Boot 1.1.6 (Jan 3 2011 - 16:14:58) 1.0.0</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.4</td>
</tr>
</tbody>
</table>

For EX8200 switches:

user@switch> show chassis firmware
<table>
<thead>
<tr>
<th>Part</th>
<th>Type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>uboot</td>
<td>U-Boot 1.1.6 (Jan 3 2011 - 16:14:58) 3.5.0</td>
</tr>
<tr>
<td></td>
<td>loader</td>
<td>FreeBSD/PowerPC U-Boot bootstrap loader 2.4</td>
</tr>
</tbody>
</table>

Meaning  For EX Series switches other than EX8200 switches, with Junos OS Release 10.4R3 or later installed:

- If there is version information following the timestamp for U-Boot (1.0.0 in the preceding example), then the loader software does not require upgrading.
- If there is no version number following the timestamp for U-boot, then the loader software requires upgrading.

NOTE: If the software version is Release 10.4R2 or earlier, no version number is displayed following the timestamp for U-boot, regardless of the loader software version installed. If you do not know whether you have installed the new loader software, we recommend that you upgrade the loader software when you upgrade the software version.
For EX8200 switches, if the version number following the timestamp for U-Boot is earlier than 3.5.0, you must upgrade the loader software when you upgrade the software version.

**Verifying Which Root Partition Is Active**

**Purpose**
Switches running Release 10.4R3 or later have resilient dual-root partition functionality, which includes the ability to boot transparently from the inactive partition if the system fails to boot from the primary root partition.

You can verify which root partition is active using the following command:

```
user@switch> show system storage partitions
```

```
fpc0:
--------------------------------------------------------------------------
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)
```

**Meaning**
The `Currently booted from:` field shows which root partition is active.

**Verifying the Junos OS Version in Each Root Partition**

**Purpose**
Each switch contains two root partitions. We recommend that you copy the same Junos OS version in each partition when you upgrade. In Junos OS Release 10.4R2 and earlier, you might choose to have different Junos OS release versions in each partition. You might have different versions during a software upgrade and before you have finished verifying the new software installation. To enable a smooth reboot if corruption is found in the primary root file system, ensure that the identical Junos OS images are in each root partition. For Release 10.4R2 and earlier, you must manually reboot the switch from the backup root partition. However, for Release 10.4R3 and later, the switch reboots automatically from the backup root partition if it fails to reboot from the active root partition.

**Action**
Verify whether both root partitions contain the same image by using the following command:

```
user@switch> show system snapshot media internal
```

```
Information for snapshot on internal (/dev/da0s1a) (backup)
Creation date: Jan 11 03:02:59 2012
JUNOS version on snapshot:
  jbase  : ex-12.2120120305_2240_user
  jcrypto-ex: 12.2120120305_2240_user
  jdocs-ex: 12.2120120305_2240_user
```

Copyright © 2013, Juniper Networks, Inc.
The command shows which Junos OS version is installed on each media partition. Verify that the same version is installed on both partitions.

**Related Documentation**
- Troubleshooting Software Installation on page 657
- Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 660
- Understanding Resilient Dual-Root Partitions on Switches on page 575
- Resilient Dual-Root Partitions Frequently Asked Questions

### Monitoring Licenses

- License Key Components for the EX Series Switch on page 601
- Monitoring Licenses for the EX Series Switch on page 602

**License Key Components for the EX Series Switch**

When you purchase a license for a Junos OS feature that requires a separate license, you receive a license key.

A license key consists of two parts:

- **License ID**—Alphanumeric string that uniquely identifies the license key. When a license is generated, it is given a license ID.
- **License data**—Block of binary data that defines and stores all license key objects.

For example, in the following typical license key, the string Junos204558 is the license ID, and the trailing block of data is the license data:

Junos204558 aeqa qaemjhd amroqha ztfmbu qgqama uqceds ra32rz lsevki ftvjad o4jy5u fynzzj mgviyl kgioyf ardb5g sj7wnt rsfked wbj65a sg

The license data defines the device ID for which the license is valid and the version of the license.

**Related Documentation**
- Managing Licenses for the EX Series Switch (CLI Procedure) on page 592
- Managing Licenses for the EX Series Switch (J-Web Procedure) on page 593
Monitoring Licenses for the EX Series Switch

To enable and use some Junos OS features on the EX Series switch, you must purchase, install, and manage the appropriate software licenses. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy.

To monitor your installed licenses, perform the following tasks:

- Displaying Installed Licenses and License Usage Details on page 602
- Displaying Installed License Keys on page 603

### Displaying Installed Licenses and License Usage Details

**Purpose**
Verify that the expected license is installed and active on the switch and fully covers the switch configuration.

**Action**
From the CLI, enter the `show system license` command. (To display only the License usage list, enter the `show system license usage` command. To display only the Licenses installed output, enter `show system license installed`.)

```
user@switch> show system license
License usage:

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Licenses</th>
<th>Licenses</th>
<th>Licenses</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>isis</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>ospf3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>ripng</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>mpls</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>permanent</td>
</tr>
</tbody>
</table>
```

**Licenses installed:**

License identifier: JUNOS204558

License version: 2

Valid for device: BN0208380000

Features:

- ex-series - Licensed routing protocols in ex-series
  permanent
Meaning  The output shows the license or licenses (for Virtual Chassis deployments) installed on the switch and license usage. Verify the following information:

- If a feature that requires a license is configured (used), a license is installed on the switch. The Licenses needed column must show that no licenses are required.
- The appropriate number of licenses is installed. Each switch requires one license. For a Virtual Chassis deployment, two licenses are recommended for redundancy.
- The expected license is installed.

Displaying Installed License Keys

Purpose  Verify that the expected license keys are installed on the switch.

Action  From the CLI, enter the `show system license keys` command.

```
user@switch> show system license keys
JUNOS204558 abcd efghij klmnop qrstuv wzyzab cdefgh ijklmn opqrst
     klmnop qrstuv wzyzab cdefgh ijklmn opqrst
     uvwxyz 61abcd efgh21 31efgh yzabcd
```

Meaning  The output shows the license key or keys (for Virtual Chassis deployments) installed on the switch. Verify that each expected license key is present.

Related Documentation  
- Managing Licenses for the EX Series Switch (CLI Procedure) on page 592
- Managing Licenses for the EX Series Switch (J-Web Procedure) on page 593
- Understanding Software Licenses for EX Series Switches on page 581

Operational Commands
request system license add

Syntax  
request system license add (filename | terminal)

Release Information  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Add a license key.

Options  
filename—License key from a file or URL. Specify the filename or the URL where the key is located.

terminal—License key from the terminal.

Required Privilege Level  
maintenance

Related Documentation  
• Adding New Licenses (CLI Procedure)

List of Sample Output  
request system license add on page 604

Output Fields  
When you enter this command, you are provided feedback on the status of your request.

Sample Output  
request system license add

user@host> request system license add terminal
request system license delete

Syntax  
request system license delete ( license-identifier | license-identifier-list [ licenseid001 licenseid002 licenseid003 ] | all )

Release Information  
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Option license-identifier-list introduced in Junos OS Release 13.1.

Description  
Delete a license key. You can choose to delete one license at a time, all licenses at once, or a list of license identifiers enclosed in brackets.

Options  
license-identifier—Text string that uniquely identifies a license key.
license-identifier-list [ licenseid001 licenseid002 licenseid003 .... ]—Delete multiple license identifiers as a list enclosed in brackets.
all—Delete all licenses on the device.

Required Privilege  
Level maintenance

Related Documentation  
• Deleting a License (CLI Procedure)
**request system license save**

**Syntax**
```
request system license save (filename | terminal)
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Save installed license keys to a file or URL.

**Options**
- `filename`—License key from a file or URL. Specify the filename or the URL where the key is located.
- `terminal`—License key from the terminal.

**Required Privilege**
- `maintenance`

**Related Documentation**
- `Saving License Keys`

**List of Sample Output**
request system license save on page 606

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
```
request system license save

user@host> request system license save ftp://user@host/license.conf
```
request system reboot

Syntax  
request system reboot  
<at time>  
<both-routing-engines>  
<in minutes>  
<media (compact-flash | disk | removable-compact-flash | usb)>  
<message "text">  
<other-routing-engine>

Syntax (EX Series Switches)  
request system reboot  
<all-members>  
<at time>  
<both-routing-engines>  
<in minutes>  
<local>  
<media (external | internal)>  
<member member-id>  
<message "text">  
<other-routing-engine>  
<slice slice>

Syntax (TX Matrix Router)  
request system reboot  
<all-chassis | all-lcc | lcc number | scc>  
<at time>  
<both-routing-engines>  
<in minutes>  
<media (compact-flash | disk)>  
<message "text">  
<other-routing-engine>  
<slice slice>

Syntax (TX Matrix Plus Router)  
request system reboot  
<all-chassis | all-lcc | lcc number | sfc number>  
<at time>  
<both-routing-engines>  
<in minutes>  
<media (compact-flash | disk)>  
<message "text">  
<other-routing-engine>  
<partition (1 | 2 | alternate)>

Syntax (MX Series Router)  
request system reboot  
<all-members>  
<at time>  
<both-routing-engines>  
<in minutes>  
<local>  
<media (external | internal)>  
<member member-id>  
<message "text">  
<other-routing-engine>

Release Information  
Command introduced before Junos OS Release 7.4.
Option **other-routing-engine** introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Option **both-routing-engines** introduced in Junos OS Release 12.1.

**Description**
Reboot the software.

**Options**

- **none**—Reboot the software immediately.
- **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.
- **all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.
- **all-members**—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.
- **at time**—(Optional) Time at which to reboot the software, specified in one of the following ways:
  - **now**—Stop or reboot the software immediately. This is the default.
  - **+minutes**—Number of minutes from now to reboot the software.
  - **ymdhhmm**—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
  - **hh:mm**—Absolute time on the current day at which to stop the software, specified in 24-hour time.
- **both-routing-engines**—(Optional) Reboot both Routing Engines at the same time.
- **in minutes**—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at +minutes** option.
- **lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.
  Replace **number** with the following values depending on the LCC configuration:
  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
local—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the local Virtual Chassis member.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Boot medium for next boot. (The options removable-compact-flash and usb pertain to the J Series routers only.)

media (external | internal)—(EX Series switches and MX Series routers only) (Optional) Reboot the boot media:

- external—Reboot the external mass storage device.
- internal—Reboot the internal flash device.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

message "text"—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition—(TX Matrix Plus routers only) (Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

- 1—Reboot from partition 1.
- 2—Reboot from partition 2.
- alternate—Reboot from the alternate partition.

scc—(TX Matrix routers only) (Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

sfc number—(TX Matrix Plus routers only) (Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace number with 0.

slice slice—(EX Series switches only) (Optional) Reboot a partition on the boot media. This option has the following suboptions:

- 1—Power off partition 1.
- 2—Power off partition 2.
- alternate—Reboot from the alternate partition.
Additional Information  Reboot requests are recorded in the system log files, which you can view with the `show log` command (see `show log`). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the `show system processes` command (see `show system processes`).

On a TX Matrix or TX Matrix Plus router, if you issue the `request system reboot` command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.

**NOTE:** Before issuing the `request system reboot` command on a TX Matrix Plus router with no options or the all-chassis, all-lcc, lcc `number`, or `sfc` options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the `request system reboot` command.

**NOTE:** To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

Required Privilege Level  maintenance

Related Documentation  • clear system reboot on page 163  
• request system halt on page 180  
• request system reboot  
• Rebooting and Halting a QFX Series Product  
• Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output  request system reboot on page 611  
request system reboot (at 2300) on page 611  
request system reboot (in 2 Hours) on page 611  
request system reboot (Immediately) on page 611  
request system reboot (at 1:20 AM) on page 611

Output Fields  When you enter this command, you are provided feedback on the status of your request.
Sample Output
request system reboot

user@host> request system reboot
Reboot the system? [yes,no] (no)

request system reboot (at 2300)

user@host> request system reboot at 2300 message? Maintenance time? Yes
Reboot the system? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00

request system reboot (Immediately)

user@host> request system reboot at now

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
request system reboot

Syntax

```
request system reboot
<all-members | local | member member-id>
<at time>
<in minutes>
<media (external | internal)>
<message "text">
<slice (1 | 2 | alternate)>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Option `partition` changed to `slice` in Junos OS Release 10.0 for EX Series switches.

Description

Reboot the Junos OS.

Reboot requests are recorded in the system log files, which you can view with the `show log` command. You can view the process names with the `show system processes` command.

Options

```
none—Reboots the software immediately.
```

```
all-members | local | member member-id—(EX4200 switch only) (Optional) Specify which member of the Virtual Chassis to reboot:
```

```
• all-members—Reboots each switch that is a member of the Virtual Chassis.
```

```
• local—Reboots the local switch, meaning the switch you are logged into, only.
```

```
• member member-id—Reboots the specified member switch of the Virtual Chassis.
```

```
at time—(Optional) Time at which to reboot the software, specified in one of the following ways:
```

```
• +minutes—Number of minutes from now to reboot the software.
```

```
• hh:mm—Absolute time on the current day at which to reboot the software, specified in 24-hour time.
```

```
• now—Stop or reboot the software immediately. This is the default.
```

```
• yyyydddhhmm—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
```

```
in minutes—(Optional) Number of minutes from now to reboot the software. This option is an alias for the at +minutes option.
```

```
media (external | internal)—(Optional) Boot medium for the next boot. The external option reboots the switch using a software package stored on an external boot source, such as a USB flash drive. The internal option reboots the switch using a software package stored in an internal memory source.
```

```
message "text"—(Optional) Message to display to all system users before rebooting the software.
```
slice (1 | 2 | alternate)—(Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:
- 1—Reboot from partition 1.
- 2—Reboot from partition 2.
- alternate—Reboot from the alternate partition, which is the partition that did not boot the switch at the last bootup.

**Required Privilege Level**
- maintenance

**Related Documentation**
- clear system reboot on page 163

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
```
request system reboot
user@host> request system reboot
Reboot the system ? [yes,no] (no)

request system reboot (at 2300)
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes

shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00

request system reboot (in 2 Hours)
The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00

request system reboot (Immediately)
user@host> request system reboot at now

request system reboot (at 1:20 AM)
To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
request system snapshot

Syntax  
request system snapshot
<partition>

Syntax (ACX Series Routers)  
request system snapshot
<media type>
<partition>

Syntax (EX Series Switches)  
request system snapshot
<all-members | local | member member-id>
<media type>
<partition>
<re0 | re1 | routing-engine routing-engine-id>
slice alternate

Syntax (J Series Routers)  
request system snapshot
<as-primary>
<config-size size>
<data-size size>
<factory>
<media type>
<partition>
[root-size size]
<swap-size size>

Syntax (MX Series Routers)  
request system snapshot
<all-members>
<config-partition>
<local>
<member member-id>
<media usb-port-number>
<partition>
[root-partition]

Syntax (TX Matrix Routers)  
request system snapshot
<all-chassis | all-lcc | lcc number | scc>
<config-partition>
<partition>
[root-partition]

Syntax (TX Matrix Plus Routers)  
request system snapshot
<all-chassis | all-lcc | lcc number | sfc number>
<config-partition>
<partition>
[root-partition]

Release Information  
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 12.2 for ACX Series switches.
Options <config-partition> and <root-partition> introduced in Junos OS Release 13.1 for M, MX, T, TX Series switches.
Option media **usb-port-number** introduced in Junos OS Release 13.2 for MX104 routers.

**Description**
- On the router, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, the root file system (/) is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.
- On the switch, take a snapshot of the files currently used to run the switch—the complete contents of the root (/), /altroot, /config, /var, and /var-tmp directories, which include the running Junos OS, the active configuration, and log files.

**CAUTION:** After you run the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

**Options**
The specific options available depend upon the router or switch:

- **none**—Back up the currently running software as follows:
  - On the router, back up the currently running and active file system partitions to standby partitions that are not running. Specifically, the root file system (/) is backed up to /altroot, and /config is backed up to /altconfig. The root and /config file systems are on the router's flash drive, and the /altroot and /altconfig file systems are on the router's hard drive.
  - On the switch, take a snapshot of the files currently used to run the switch and copy them to the media that the switch did not boot from. If the switch is booted from internal media, the snapshot is copied to external (USB) media. If the switch is booted from external (USB) media, the snapshot is copied to internal media.
    - If the snapshot destination is external media but a USB flash drive is not connected, an error message is displayed.
    - If the automatic snapshot procedure is already in progress, the command returns the following error: **Snapshot already in progress. Cannot start manual snapshot.**
    For additional information about the automatic snapshot feature, see "Understanding Resilient Dual-Root Partitions on Switches" on page 575.

- **all-chassis | all-lcc | lcc number**—(TX Matrix and TX Matrix Plus router only) (Optional)
  - **all-chassis**—On a TX Matrix router, archive data and executable areas for all Routing Engines in the chassis. On a TX Matrix Plus router, archive data and executable areas for all Routing Engines in the chassis.
  - **all-lcc**—On a TX Matrix router, archive data and executable areas for all T640 routers (or line-card chassis) connected to a TX Matrix router. On a TX Matrix Plus router, archive data and executable areas for all routers (or line-card chassis) connected to a TX Matrix Plus router.
- **lcc number**—On a TX Matrix router, archive data and executable areas for a specific T640 router (or line-card chassis) that is connected to a TX Matrix router. On a TX Matrix Plus router, archive data and executable areas for a specific router (line-card chassis) that is connected to a TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T6600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T6600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**all-members | local | member member-id**—(EX Series switch Virtual Chassis and MX Series routers only) (Optional) Specify where to place the snapshot (archive data and executable areas) in a Virtual Chassis:

- **all-members**—Create a snapshot (archive data and executable areas) for all members of the Virtual Chassis.
- **local**—Create a snapshot (archive data and executable areas) on the member of the Virtual Chassis that you are currently logged into.
- **member member-id**—Create a snapshot (archive data and executable areas) for the specified member of the Virtual Chassis.

**as-primary**—(J Series routers only) (Optional) Create a snapshot that can be used to replace the medium in the primary compact flash drive. This option can be used on the removable compact flash only. The option copies the default files that were loaded on the primary compact flash drive when it was shipped from the factory, plus the rescue configuration if one has been set. This option is useful if you have multiple routers and want to use the same software and configuration on each router. After a boot device is created as a primary compact flash drive, it can operate in only a primary compact flash drive slot. This option causes the boot medium to be partitioned.

**config-partition**—(M, MX, T, TX Series routers only) Create a snapshot of the configuration partition only and store it onto the default /altconfig on the hard disk device or an /altconfig on a USB device.

**config-size size**—(J Series routers only) (Optional) Specify the size of the config partition, in megabytes. The default value is 10 percent of physical memory on the boot partition. The config partition is mounted on /config, and the configuration files are stored in this partition. This option causes the boot medium to be partitioned.

**data-size size**—(J Series routers only) (Optional) Specify the size of the data partition, in megabytes. The default value is 0 MB. The data partition is mounted on /data. This
space is not used by the router, and can be used for extra storage. This option causes
the boot medium to be partitioned.

**factory**—(J Series routers only) (Optional) Copy only default files that were loaded on
the primary compact flash drive when it was shipped from the factory, plus the rescue
configuration if one has been set. After the boot medium is created with the factory
option, it can operate in only the primary compact flash drive.

**media type**—(J Series routers and EX Series switches only) (Optional) Specify the boot
device the software is copied to:

- **compact-flash**—Copy software to the primary compact flash drive.
- **external**—(Switches only) Copy software to an external mass storage device, such
  as a USB flash drive. If a USB drive is not connected, the switch displays an error
  message.
- **internal**—(Switches only) Copy software to an internal flash drive.
- **removable-compact-flash**—Copy software to the removable compact flash drive.
- **usb**—(ACX Series, M320, T640, MX960, and J Series routers only) Copy software
to the device connected to the USB port.
- **usb0**—(MX104 routers only) Copy software to the device connected to the USB0
  port.
- **usb1**—(MX104 routers only) Copy software to the device connected to the USB1
  port.

**partition**—(Optional) Repartition the flash drive before a snapshot occurs. If the partition
(table on the flash drive is corrupted, the request system snapshot command fails
and reports errors. The partition option is only supported for restoring the software
image from the hard drive to the flash drive.

(Routers only) You cannot issue the request system snapshot command when you
enable flash disk mirroring. We recommend that you disable flash disk mirroring
when you upgrade or downgrade the software. For more information, see the Junos
OS Administration Library for Routing Devices.

(EX Series switches only) If the snapshot destination is the media that the switch
did not boot from, you must use the **partition** option.

**re0 | re1 | routing-engine routing-engine-id**—(EX6200 and EX8200 switches only) Specify
where to place the snapshot in a redundant Routing Engine configuration.

- **re0**—Create a snapshot on Routing Engine 0.
- **re1**—Create a snapshot on Routing Engine 1.
- **routing-engine routing-engine-id**—Create a snapshot on the specified Routing
  Engine.

**root-partition**—(M, MX, T, TX Series routers only) Create a snapshot of the root partition
only and store it onto the default /altroot on the hard disk device or an /altroot on a
USB device.
root-size size—(J Series routers only) (Optional) Specify the size of the root partition, in megabytes. The default value is one-third of the physical memory minus the config, data, and swap partitions. The root partition is mounted on / and does not include configuration files. This option causes the boot medium to be partitioned.

slice alternate—(EX Series switches only) (Optional) Take a snapshot of the active root partition and copy it to the alternate slice on the boot media.

scc—(TX Matrix router only) (Optional) Archive data and executable areas for a TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus router only) (Optional) Archive data and executable areas for a TX Matrix Plus router (or switch-fabric chassis). Replace number with 0.

swap-size size—(J Series router only) (Optional) Specify the size of the swap partition, in megabytes. The default value is one-third of the physical memory on a boot medium larger than 128 MB, or 0 MB on a smaller boot device. The swap partition is used for swap files and software failure memory snapshots. Software failure memory snapshots are saved to the boot medium only if it is specified as the dump device in the system dump-device configuration hierarchy. This option causes the boot medium to be partitioned.

Additional Information

• (Routers only) Before upgrading the software on the router, when you have a known stable system, issue the request system snapshot command to back up the software, including the configuration, to the /altroot and /altconfig file systems. After you have upgraded the software on the router and are satisfied that the new packages are successfully installed and running, issue the request system snapshot command again to back up the new software to the /altroot and /altconfig file systems.

• (Routers only) You cannot issue the request system snapshot command when you enable flash disk mirroring. We recommend that you disable flash disk mirroring when you upgrade or downgrade the software. For more information, see the Junos OS Administration Library for Routing Devices.

• (TX Matrix and TX Matrix Plus router only) On a routing matrix, if you issue the request system snapshot command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are backed up. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are backed up.

Required Privilege Level

maintenance

Related Documentation

• show system snapshot on page 652

• show system auto-snapshot on page 640

List of Sample Output

request system snapshot (Routers) on page 619
request system snapshot (EX Series Switches) on page 619
request system snapshot (When the Partition Flag Is On) on page 619
request system snapshot (MX104 routers when media device is missing) on page 619
Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system snapshot (Routers)

user@host> request system snapshot
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)
umount: /altconfig: not currently mounted
Copying /config to /altconfig.. (this may take a few minutes)
The following filesystems were archived: / /config

request system snapshot (EX Series Switches)

user@switch> request system snapshot partition
Clearing current label...
Partitioning external media (/dev/da1) ...
Partitions on snapshot:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Mountpoint</th>
<th>Size</th>
<th>Snapshot argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>/altroot</td>
<td>179M</td>
<td>none</td>
</tr>
<tr>
<td>s2a</td>
<td>/</td>
<td>180M</td>
<td>none</td>
</tr>
<tr>
<td>s3d</td>
<td>/var/tmp</td>
<td>361M</td>
<td>none</td>
</tr>
<tr>
<td>s3e</td>
<td>/var</td>
<td>121M</td>
<td>none</td>
</tr>
<tr>
<td>s4d</td>
<td>/config</td>
<td>60M</td>
<td>none</td>
</tr>
</tbody>
</table>

Copying '/dev/da0s1a' to '/dev/da1s1a' .. (this may take a few minutes)
Copying '/dev/da0s2a' to '/dev/da1s2a' .. (this may take a few minutes)
Copying '/dev/da0s3d' to '/dev/da1s3d' .. (this may take a few minutes)
Copying '/dev/da0s3e' to '/dev/da1s3e' .. (this may take a few minutes)
Copying '/dev/da0s4d' to '/dev/da1s4d' .. (this may take a few minutes)
The following filesystems were archived: /altroot / /var/tmp /var /config

request system snapshot (When the Partition Flag Is On)

user@host> request system snapshot partition
Performing preliminary partition checks ...
Partitioning ad0 ...
umount: /altroot: not currently mounted
Copying / to /altroot.. (this may take a few minutes)
The following filesystems were archived: /config

request system snapshot (MX104 routers when media device is missing)

user@host> request system snapshot media usb0
error: usb0 media missing or invalid

request system snapshot (When Mirroring Is Enabled)

user@host> request system snapshot
Snapshot is not possible since mirror-flash-on-disk is configured.

request system snapshot all-lcc (Routing Matrix)

user@host> request system snapshot all-lcc
lcc0-re0:
-------------------------------------------------------------------------
Copying '/' to '/altroot' .. (this may take a few minutes)
Copying '/config' to '/altconfig' .. (this may take a few minutes)
The following filesystems were archived: / /config

lcc2-re0:
-------------------------------------------------------------------------
Copying '/' to '/altroot' .. (this may take a few minutes)
Copying '/config' to '/altconfig' .. (this may take a few minutes)
The following filesystems were archived: / /config

request system snapshot all-members (Virtual Chassis)

user@switch>  request system snapshot all-members media internal
fpc0:
-------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc1:
-------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc2:
-------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc3:
-------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc4:
-------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /

fpc5:
-------------------------------------------------------------------------
Copying '/dev/da0s2a' to '/dev/da0s1a' .. (this may take a few minutes)
The following filesystems were archived: /
request system software add

Syntax
request system software add package-name
   <best-effort-load>
   <delay-restart>
   <force>
   <no-copy>
   <no-validate>
   <re0 | re1>
   <reboot>
   <set [package-name package-name]>
   <unlink>
   <upgrade-with-config>
   <upgrade-with-config-format format>
   <validate>

Syntax (EX Series Switches)
request system software add package-name
   <best-effort-load>
   <delay-restart>
   <force>
   <no-copy>
   <no-validate>
   <re0 | re1>
   <reboot>
   <set [package-name package-name]>
   <upgrade-with-config>
   <upgrade-with-config-format format>
   <validate>

Syntax (TX Matrix Router)
request system software add package-name
   <best-effort-load>
   <delay-restart>
   <force>
   <lcc number | scc>
   <no-copy>
   <no-validate>
   <re0 | re1>
   <reboot>
   <set [package-name package-name]>
   <unlink>
   <upgrade-with-config>
   <upgrade-with-config-format format>
   <validate>

Syntax (TX Matrix Plus Router)
request system software add package-name
   <best-effort-load>
   <delay-restart>
   <force>
   <lcc number | sfc number>
   <no-copy>
   <no-validate>
   <re0 | re1>
   <reboot>
   <set [package-name package-name]>

Copyright © 2013, Juniper Networks, Inc.
<unlink>
<upgrade-with-config>
<upgrade-with-config-format format>
<validate>

**Syntax (MX Series Router)**

```
request system software add package-name
<best-effort-load>
<delay-restart>
<force>
<member member-id>
<no-copy>
<no-validate>
<re0 | re1>
<reboot>
<set [package-name package-name]>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format format>
<validate>
```

**Syntax (QFX Series)**

```
request system software add package-name
<best-effort-load>
<component all>
<delay-restart>
<force>
<no-copy>
<no-validate>
<partition>
<reboot>
<unlink>
<upgrade-with-config>
<upgrade-with-config-format format>
<validate>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

- **best-effort-load** and **unlink** options added in Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- **sfc** option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- **set [package-name package-name]** option added in Junos OS Release 11.1 for EX Series switches.
- **set [package-name package-name]** option added in Junos OS Release 12.2 for M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways.

---

**NOTE:** On EX Series switches, the **set [package-name package-name]** option allows you to install only two software packages on a mixed EX4200 and EX4500 Virtual Chassis, whereas, on M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways, the **set [package-name package-name]** option allows you to install multiple software packages and software add-on packages at the same time.

**Description**

NOTE: We recommend that you always download the software image to /var/tmp only. On EX Series and QFX Series switches, you must use the /var/tmp directory. Other directories are not supported.

Install a software package or bundle on the router or switch.

**Options**

`package-name`—Location from which the software package or bundle is to be installed. For example:

- `/var/tmp/package-name`—For a software package or bundle that is being installed from a local directory on the router or switch.

- `protocol://hostname/pathname/package-name`—For a software package or bundle that is to be downloaded and installed from a remote location. Replace `protocol` with one of the following:
  - `ftp`—File Transfer Protocol. Use `ftp://hostname/pathname/package-name`. To specify authentication credentials, use `ftp://<username>:<password>@hostname/pathname/package-name`. To have the system prompt you for the password, specify `prompt` in place of the password. If a password is required and you do not specify the password or `prompt`, an error message is displayed.
  - `http`—Hypertext Transfer Protocol. Use `http://hostname/pathname/package-name`. To specify authentication credentials, use `http://<username>:<password>@hostname/pathname/package-name`. If a password is required and you omit it, you are prompted for it.
NOTE:

- The *pathname* in the protocol is the relative path to the user's home directory on the remote system and not the root directory.

- Do not use the *scp* protocol in the request system software add command to download and install a software package or bundle from a remote location. The previous statement does not apply to the QFabric switch. The software upgrade is handled by the MGD process which does not support scp.

Use the file `copy` command to copy the software package or bundle from the remote location to the `/var/tmp` directory on the hard disk:
```
file copy scp://source/package-name /var/tmp
```
Then install the software package or bundle using the request system software add command:
```
request system software add /var/tmp/package-name
```

- On a J Series Services Router, when you install the software from a remote location, the package is removed at the earliest opportunity in order to make room for the installation to be completed. If you copy the software to a local directory on the router and then install the new package, use the `unlink` option to achieve the same effect and allow the installation to be completed.

---

**best-effort-load**—(Optional) Activate a partial load and treat parsing errors as warnings instead of errors.

**component all**—(QFabric systems only) (Optional) Install software package on all of the QFabric components.

**delay-restart**—(Optional) Install a software package or bundle, but do not restart software processes.

**force**—(Optional) Force the addition of the software package or bundle (ignore warnings).

**lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) In a routing matrix based on the TX Matrix router, install a software package or bundle on a T640 router that is connected to the TX Matrix router. In a routing matrix based on the TX Matrix Plus router, install a software package or bundle on a router that is connected to the TX Matrix Plus router.

Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
• 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

• 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

member member-id—(MX Series routers only) (Optional) Install a software package on the specified Virtual Chassis member. Replace member-id with a value of 0 or 1.

partition—(QFX3500 switches only) (Optional) Format and repartition the media before installation.

scc—(TX Matrix routers only) (Optional) Install a software package or bundle on a Routing Engine on a TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus routers only) (Optional) Install a software package or bundle on a Routing Engine on a TX Matrix Plus router. Replace number with 0.

no-copy—(Optional) Install a software package or bundle, but do not save copies of the package or bundle files.

no-validate—(Optional) When loading a software package or bundle with a different release, suppress the default behavior of the validate option.

re0 | re1—(Optional) On routers or switches that support dual or redundant Routing Engines, load a software package or bundle on the Routing Engine in slot 0 (re0) or the Routing Engine in slot 1 (re1).

reboot—(Optional) After adding the software package or bundle, reboot the system. On a QFabric switch, the software installation is not complete until you reboot the component for which you have installed the software.

set [package-name package-name]—(Mixed EX4200 and EX4500 Virtual Chassis only) (Optional) Install two software packages—a package for an EX4200 switch and the same release of the package for an EX4500 switch—to upgrade all member switches in a mixed EX4200 and EX4500 Virtual Chassis.

set [package-name package-name]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages and software add-on packages at the same time.

unlink—(Optional) On J Series Services Routers, this option ensures that the software package is removed at the earliest opportunity in order to make room for the installation to be completed. On M Series, T Series, and MX Series routers, use the unlink option to remove the software package from this directory after a successful upgrade is completed.

upgrade-with-config—(Optional) Install one or more configuration files.

upgrade-with-config-format format—(Optional) Specify the configuration file format, text or xml. The default format is text.
The upgrade-with-config and upgrade-with-config-format options are only available locally on the router or switch. In a routing matrix, the configuration is applied only to the local router and is not propagated to other routers.

The options are validated during the validation process and applied to the router or switch during the upgrade process. If the upgrade process is successful, the options are removed from the configuration. If the upgrade process fails, the configuration file is renamed with the .failed suffix.

validate—(Optional) Validate the software package or bundle against the current configuration as a prerequisite to adding the software package or bundle. This is the default behavior when the software package or bundle being added is a different release.

The validate option only works on systems that do not have graceful-switchover (GRES) enabled. To use the validate option on a system with GRES, either disable GRES for the duration of the installation, or install using the command request system software in-service-upgrade, which requires nonstop active routing (NSR) to be enabled when using GRES.

Additional Information

Before upgrading the software on the router or switch, when you have a known stable system, issue the request system snapshot command to back up the software, including the configuration, to the /altroot and /altconfig file systems. After you have upgraded the software on the router or switch and are satisfied that the new package or bundle is successfully installed and running, issue the request system snapshot command again to back up the new software to the /altroot and /altconfig file systems.

The request system snapshot command is currently not supported on the QFabric system. Also, you cannot add or install multiple packages on a QFabric system.

After you run the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.

If you are upgrading more than one package at the same time, delete the operating system package, jkernel, last. Add the operating system package, jkernel, first and the routing software package, jroute, last. If you are upgrading all packages at once, delete and add them in the following order:
By default, when you issue the `request system software add package-name` command on a TX Matrix master Routing Engine, all the T640 master Routing Engines that are connected to it are upgraded to the same version of software. If you issue the same command on the TX Matrix backup Routing Engine, all the T640 backup Routing Engines that are connected to it are upgraded to the same version of software.

Likewise, when you issue the `request system software add package-name` command on a TX Matrix Plus master Routing Engine, all the T1600 or T4000 master Routing Engines that are connected to it are upgraded to the same version of software. If you issue the same command on the TX Matrix Plus backup Routing Engine, all the T1600 or T4000 backup Routing Engines that are connected to it are upgraded to the same version of software.

**Required Privilege Level**
- maintenance

**Related Documentation**
- request system software delete on page 629
- request system software rollback on page 633
- request system storage cleanup on page 203
- Upgrading Software on QFX3500 and QFX3600 Standalone Switches
- Upgrading Software on a QFabric System
- Routing Matrix with a TX Matrix Plus Router Solutions Page

**List of Sample Output**
- request system software add validate on page 627
- request system software add (Mixed EX4200 and EX4500 Virtual Chassis) on page 628
- request system software add component all (QFabric Systems) on page 628

**Output Fields**
- When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
request system software add validate

```
user@host> request system software add validate /var/tmp/jinstall-7.2R1.7-domestic-signed.tgz
Checking compatibility with configuration
Initializing...
Using jbase-7.1R2.2
Using /var/tmp/jinstall-7.2R1.7-domestic-signed.tgz
Verified jinstall-7.2R1.7-domestic.tgz signed by PackageProduction_7_2_0
Using /var/validate/tmp/jinstall-signed/jinstall-7.2R1.7-domestic.tgz
Using /var/validate/tmp/jinstall/jbundle-7.2R1.7-domestic.tgz
Checking jbundle requirements on /
Using /var/validate/tmp/jbundle/jbase-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jkernel-7.2R1.7.tgz
```
Using /var/validate/tmp/jbundle/jcrypto-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jpfe-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jdocs-7.2R1.7.tgz
Using /var/validate/tmp/jbundle/jroute-7.2R1.7.tgz
Validating against /config/juniper.conf.gz
mgd: commit complete
Validation succeeded
Validating against /config/rescue.conf.gz
mgd: commit complete
Validation succeeded
Installing package '/var/tmp/jinstall-7.2R1.7-domestic-signed.tgz' ...
Verified jinstall-7.2R1.7-domestic.tgz signed by PackageProduction_7_2_0
Adding jinstall...

WARNING:  This package will load JUNOS 7.2R1.7 software.
WARNING:  It will save JUNOS configuration files, and SSH keys
WARNING:  (if configured), but erase all other files and information
WARNING:  stored on this machine.  It will attempt to preserve dumps
WARNING:  and log files, but this can not be guaranteed.  This is the
WARNING:  pre-installation stage and all the software is loaded when
WARNING:  you reboot the system.

Saving the config files ...
Installing the bootstrap installer ...

WARNING:  A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:  'request system reboot' command when software installation is
WARNING:  complete. To abort the installation, do not reboot your system,
WARNING:  instead use the 'request system software delete jinstall'
WARNING:  command as soon as this operation completes.

Saving package file in /var/sw/pkg/jinstall-7.2R1.7-domestic-signed.tgz ...
Saving state for rollback ...

Sample Output
request system software add (Mixed EX4200 and EX4500 Virtual Chassis)

user@switch> request system software add set
[/var/tmp/jinstall-ex-4200-11.1R1.1-domestic-signed.tgz
/var/tmp/jinstall-ex-4500-11.1R1.1-domestic-signed.tgz]
...

request system software add component all (QFabric Systems)

user@switch> request system software add/pbdata/packages/jinstall-qfabric-12.2X50-D1.3.rpm
component all
...

**request system software delete**

**Syntax**
```plaintext
request system software delete software-package
<force>
<reboot>
<set [package-name package-name]>
```

**Syntax (TX Matrix Router)**
```plaintext
request system software delete software-package
<force>
<lcc number | scc>
<reboot>
<set [package-name package-name]>
```

**Syntax (TX Matrix Plus Router)**
```plaintext
request system software delete software-package
<force>
<lcc number | sfc number>
<reboot>
<set [package-name package-name]>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Option `sfc` introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- Option `reboot` introduced in Junos OS Release 12.3.

**Description**
Remove a software package or bundle from the router or switch.

---

**CAUTION:** Before removing a software package or bundle, make sure that you have already placed the new software package or bundle that you intend to load onto the router or switch.

**Options**
- **software-package**—Software package or bundle name. You can delete any or all of the following software bundles or packages:
  - `jbase`—(Optional) Junos base software suite
  - `jcrypto`—(Optional, in domestic version only) Junos security software
  - `jdocs`—(Optional) Junos online documentation file
  - `jkernel`—(Optional) Junos kernel software suite
  - `jpfe`—(Optional) Junos Packet Forwarding Engine support
  - `jroute`—(Optional) Junos routing software suite
  - `junos`—(Optional) Junos base software
NOTE: On EX Series switches, some of the package names are different than those listed. To see the list of packages that you can delete on an EX Series switch, enter the command show system software.

force—(Optional) Ignore warnings and force removal of the software.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, remove an extension or upgrade package from a specific T640 router (line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, remove an extension or upgrade package from a specific router that is connected to the TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

reboot—As of Junos OS 12.3 and greater, automatically reboot upon completing the request system software delete command.

scc—(TX Matrix routers only) (Optional) Remove an extension or upgrade package from the TX Matrix router (or switch-card chassis).

set [package-name package-name]—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages or software add-on packages at the same time.

sfc number—(TX Matrix Plus routers only) (Optional) Remove an extension or upgrade package from the TX Matrix Plus router. Replace number with 0.

Additional Information

Before upgrading the software on the router or switch, when you have a known stable system, issue the request system snapshot command to back up the software, including the configuration, to the /altroot and /altconfig file systems (on routers) or the /, /altroot, /config, /var, and /var/tmp file systems (on switches). After you have upgraded the software on the router or switch and are satisfied that the new packages are successfully installed and running, issue the request system snapshot command again to back up the new software to the /altroot and /altconfig file systems (on routers) or the /, /altroot, /config, /var, and /var/tmp file systems (on switches). After you run the request system snapshot command, you cannot return to the previous version of the software, because the running and backup copies of the software are identical.
Required Privilege Level

- maintenance

Related Documentation

- request system software add on page 621
- request system software rollback on page 633
- request system software validate on page 637
- Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output

- request system software delete jdocs on page 631

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system software delete jdocs

The following example displays the system software packages before and after the jdocs package is deleted through the request system software delete command:

user@host> show system software
Information for jbase:

Comment:
JUNOS Base OS Software Suite [7.2R1.7]

Information for jcrypto:

Comment:
JUNOS Crypto Software Suite [7.2R1.7]

Information for jdocs:

Comment:
JUNOS Online Documentation [7.2R1.7]

Information for jkernel:

Comment:
JUNOS Kernel Software Suite [7.2R1.7]

...

user@host> request system software delete jdocs
Removing package 'jdocs' ...

user@host> show system software
Information for jbase:

Comment:
JUNOS Base OS Software Suite [7.2R1.7]
Information for jcrypto:

Comment:
JUNOS Crypto Software Suite [7.2R1.7]

Information for jkernel:

Comment:
JUNOS Kernel Software Suite [7.2R1.7]

...
### request system software rollback

<table>
<thead>
<tr>
<th>Syntax</th>
<th>request system software rollback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax (EX Series Switches)</td>
<td>request system software rollback</td>
</tr>
<tr>
<td></td>
<td>&lt;all-members&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;local&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;member member-id&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;reboot&gt;</td>
</tr>
<tr>
<td>Syntax (TX Matrix Router)</td>
<td>request system software rollback</td>
</tr>
<tr>
<td></td>
<td>&lt;lcc number</td>
</tr>
<tr>
<td></td>
<td>&lt;reboot&gt;</td>
</tr>
<tr>
<td>Syntax (TX Matrix Plus Router)</td>
<td>request system software rollback</td>
</tr>
<tr>
<td></td>
<td>&lt;lcc number</td>
</tr>
<tr>
<td></td>
<td>&lt;reboot&gt;</td>
</tr>
<tr>
<td>Syntax (MX Series Router)</td>
<td>request system software rollback</td>
</tr>
<tr>
<td></td>
<td>&lt;all-members&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;local&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;member member-id&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;reboot&gt;</td>
</tr>
</tbody>
</table>

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command behavior changed in Junos OS Release 12.1.
Option reboot introduced in Junos OS Release 12.3.

**Description**

For all versions of Junos OS up to and including Junos OS 11.4, revert to the software that was loaded at the last successful `request system software add` command.

As of Junos OS 12.1 and greater, revert to the last known good state before the most recent `request system software (add | delete)` command. For example, using rollback in Junos OS 12.1 after using `request system software add` restores the system to a known good state prior to using the `add` command. Similarly, using rollback in Junos OS 12.1 after using `request system software delete` restores the system to a known good state prior to using the `delete` command.

A software rollback fails if any required package (or a jbundle package containing the required package) cannot be found in `/var/sw/pkg`.

**Additional Information**

- On M Series and T Series routers, if `request system software add <jinstall> reboot` was used for the previous installation, then `request system software rollback` has no effect. In this case, use `jinstall` to reinstall the required package.
On M Series and T Series routers, if `request system software add <sdk1>` was used for the previous installation, then `request system software rollback` removes the last installed SDK package (`sdk1` in this example).

On SRX Series devices with dual root systems, when `request system software rollback` is run, the system switches to the alternate root. Each root can have a different version of Junos OS. Rollback takes each root back to the previously installed image.

**Options**

- **all-members**—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on all members of the Virtual Chassis configuration.

- **lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, attempt to roll back to the previous set of packages on a T640 router connected to the TX Matrix router. On a TX Matrix Plus router, attempt to roll back to the previous set of packages on a connected router connected to the TX Matrix Plus router.
  
  Replace `number` with the following values depending on the LCC configuration:

  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

- **local**—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on the local Virtual Chassis member.

- **member member-id**—(EX4200 switches and MX Series routers only) (Optional) Attempt to roll back to the previous set of packages on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace `member-id` with a value from 0 through 9. For an MX Series Virtual Chassis, replace `member-id` with a value of 0 or 1.

- **none**—For all versions of Junos OS up to and including Junos OS 11.4, revert to the set of software as of the last successful `request system software add`. As of Junos OS 12.1 and greater, revert to the last known good state before the most recent `request system software (add | delete)` command.

- **reboot**—As of Junos OS 12.3 and greater, automatically reboot upon completing the `request system software rollback` command.

- **scc**—(TX Matrix routers only) (Optional) Attempt to roll back to the previous set of packages on the TX Matrix router (or switch-card chassis).
**sfc number**—(TX Matrix Plus routers only) (Optional) Attempt to roll back to the previous set of packages on the TX Matrix Plus router. Replace *number* with 0.

**Required Privilege Level**

maintenance

**Related Documentation**

- request system software abort
- request system software add on page 621
- request system software delete on page 629
- request system software validate on page 637
- request system configuration rescue delete on page 547
- request system configuration rescue save on page 548
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

**List of Sample Output**

request system software rollback on page 636

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.
Sample Output
request system software rollback

user@host> request system software rollback
Verified SHA1 checksum of ./jbase-7.2R1.7.tgz
Verified SHA1 checksum of ./jdocs-7.2R1.7.tgz
Verified SHA1 checksum of ./jroute-7.2R1.7.tgz
Installing package './jbase-7.2R1.7.tgz' ...
Available space: 35495 require: 7335
Installing package './jdocs-7.2R1.7.tgz' ...
Available space: 35339 require: 3497
Installing package './jroute-7.2R1.7.tgz' ...
Available space: 35238 require: 6976
NOTICE: uncommitted changes have been saved in
/var/db/config/juniper.conf.pre-install
Reloading /config/juniper.conf.gz ...
Activating /config/juniper.conf.gz ...
mgd: commit complete
Restarting mgd ...
Restarting aprobed ...
Restarting apsd ...
Restarting cospd ...
Restarting fsad ...
Restarting fud ...
Restarting gcdrd ...
Restarting ilmid ...
Restarting irsd ...
Restarting l2tpd ...
Restarting mib2d ...
Restarting nasd ...
Restarting pppoed ...
Restarting rdd ...
Restarting rmopd ...
Restarting rsdp ...
Restarting sampled ...
Restarting serviced ...
Restarting snmpd ...
Restarting spd ...
Restarting vrrpd ...

WARNING: cli has been replaced by an updated version:
CLI release 7.2R1.7 built by builder on 2005-04-22 02:03:44 UTC
Restart cli using the new version? [yes,no] (yes) yes

Restarting cli ...
user@host
**request system software validate**

**Syntax**

```plaintext
request system software validate package-name
<set [package-name package-name]>
<upgrade-with-config>
<upgrade-with-config-format format>
```

**Syntax (TX Matrix Router)**

```plaintext
request system software validate package-name
<lcc number | scc>
<set [package-name package-name]>
<upgrade-with-config>
<upgrade-with-config-format format>
```

**Syntax (TX Matrix Plus Router)**

```plaintext
request system software validate package-name
<lcc number | sfc number>
<set [package-name package-name]>
<upgrade-with-config>
<upgrade-with-config-format format>
```

**Syntax (MX Series Router)**

```plaintext
request system software validate package-name
<member member-id>
<set [package-name package-name]>
<upgrade-with-config>
<upgrade-with-config-format format>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

- `sfc` option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Validate candidate software against the current configuration of the router.

**Options**

- **lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, validate the software bundle or package on a specific T640 router (or line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, validate the software bundle or package for a specific router that is connected to the TX Matrix Plus router.

  Replace `number` with the following values depending on the LCC configuration:

  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
• 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

• 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**member member-id**—(MX Series routers only) (Optional) Validate the software bundle or package on the specified member of the Virtual Chassis configuration. For an MX Series Virtual Chassis, replace `member-id` with a value of 0 or 1.

**package-name**—Name of the software bundle or package to test.

**scc**—(TX Matrix routers only) (Optional) Validate the software bundle or package for the TX Matrix router (or switch-card chassis).

**set [package-name package-name]**—(M Series, MX Series, T Series routers, and Branch SRX Series Services Gateways only) (Optional) Install multiple software packages or software add-on packages at the same time.

**sfc number**—(TX Matrix Plus routers only) (Optional) Validate the software bundle or package for the TX Matrix Plus router.

**upgrade-with-config**—(Optional) Install one or more configuration files.

**upgrade-with-config-format format**—(Optional) Specify the configuration file format, text or xml. The default format is text.

---

**NOTE:** The `upgrade-with-config` and `upgrade-with-config-format` options are only available locally on the router or switch. In a routing matrix, the configuration is applied only to the local router and is not propagated to other routers.

The options are validated during the validation process and applied to the router or switch during the upgrade process. If the upgrade process is successful, the options are removed from the configuration. If the upgrade process fails, the configuration file is renamed with the `.failed` suffix.

**Additional Information**

By default, when you issue the `request system software validate` command on a TX Matrix master Routing Engine, all the T640 master Routing Engines that are connected to it are validated. If you issue the same command on the TX Matrix backup Routing Engine, all the T640 backup Routing Engines that are connected to it are upgraded to the same version of software.

Likewise, if you issue the `request system software validate` command on a TX Matrix Plus master Routing Engine, all the T1600 or T4000 master Routing Engines that are connected to it are validated. If you issue the same command on a TX Matrix Plus backup Routing Engine, all the T1600 or T4000 backup Routing Engines that are connected to it are upgraded to the same version of software.
<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>maintenance</th>
</tr>
</thead>
</table>

**Related Documentation**

- `request system software abort`
- `request system software add` on page 621
- `request system software delete` on page 629
- `request system software rollback` on page 633
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

**List of Sample Output**

- `request system software validate (Successful Case)` on page 639
- `request system software validate (Failure Case)` on page 639

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

**request system software validate (Successful Case)**

```
user@host> request system software validate /var/sw/pkg/jbundle-5.3I20020124_0520_sjg.tgz
Checking compatibility with configuration
Initializing...
Using /packages/jbase-5.3I20020122_1901_sjg
Using /var/sw/pkg/jbundle-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jbase-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jkernel-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jcrypto-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jpfe-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jdocs-5.3I20020124_0520_sjg.tgz
Using /var/chroot/var/tmp/jbundle/jroute-5.3I20020124_0520_sjg.tgz
Validating against /config/juniper.conf.gz
mgd: commit complete
```

**WARNING:** cli has been replaced by an updated version:

CLI release 5.3I0 built by sjg on 2002-01-24 05:23:53 UTC

Restart cli using the new version? [yes,no] (yes)

**request system software validate (Failure Case)**

```
user@host> request system software validate 6.3/
Pushing bundle to lcc0-re0
error: Failed to transfer package to lcc0-re0
```

```
user@host> request system software validate test
Pushing bundle to lcc0-re0
Pushing bundle to lcc2-re0
lcc0-re0:
gzip: stdin: not in gzip format
tar: child returned status 1
ERROR: Not a valid package: /var/tmp/test
```
show system auto-snapshot

Syntax

```
show system auto-snapshot
```

Release Information

Command introduced in Junos OS Release 12.3 for EX Series switches.

Description

Display automatic snapshot status information. When the automatic snapshot feature is enabled and the system reboots from the alternate root partition, the switch automatically takes a snapshot of the root file system in the alternate root partition and copies it onto the primary root partition. This automatic snapshot procedure takes place whenever the system reboots from the alternate partition, regardless of whether the reboot from the alternate partition is due to a command or due to a corruption of the primary partition.

When the automatic snapshot procedure is in progress, you cannot run the manual snapshot command, `request system snapshot`.

Options

This command has no options.

Required Privilege

Level view

Related Documentation

- Understanding Resilient Dual-Root Partitions on Switches on page 575

List of Sample Output

show system auto-snapshot on page 641

Output Fields

Table 106 on page 640 describes the output fields for the `show system auto-snapshot` command. Output fields are listed in the approximate order in which they appear.

### Table 106: show system auto-snapshot status Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| **Auto-snapshot configuration** | Status of the configuration:  
- Enabled—If the system reboots from the alternate partition, the automatic snapshot feature automatically takes a snapshot of the alternate partition and copies it onto the primary partition.  
- Disabled—The system does not automatically take a snapshot of the alternate partition. You must use the manual snapshot command, `request system snapshot`, to take a snapshot of one partition and copy it onto the other. |
| **Auto-snapshot state** | Status of the automatic snapshot procedure:  
- Completed—The automatic snapshot procedure has completed copying the alternate partition to the primary partition and the alarm has been cleared.  
- Disabled—The automatic snapshot procedure is inactive.  
- In progress—The automatic snapshot procedure is in progress. It takes about 10 to 15 minutes to complete, depending upon disk size. |
**Sample Output**

```plaintext
show system auto-snapshot

user@switch> show system auto-snapshot
Auto-snapshot Configuration: Enabled
Auto-snapshot State: Disabled
```
show system boot-messages

Syntax

show system boot-messages

Syntax (EX Series Switches)

show system boot-messages
<all-members>
<local>
<member member-id>

Syntax (TX Matrix Router)

show system boot-messages
<all-chassis | all-lcc | lcc number | scc>

Syntax (TX Matrix Plus Router)

show system boot-messages
<all-chassis | all-lcc | lcc number | sfc number>

Syntax (MX Series Router)

show system boot-messages
<all-members>
<local>
<member member-id>

Syntax (QFX Series)

show system boot-messages
infrastructure name | interconnect-device name | node-group name

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display initial messages generated by the system kernel upon startup. These messages are the contents of /var/run/dmesg.boot.

Options

none—Display all boot time messages.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display boot time messages for all of the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display boot time messages for all T640 routers connected to a TX Matrix router. On a TX Matrix Plus router, display boot time messages for all connected T1600 or T4000 LCCs.

all-members—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on all members of the Virtual Chassis configuration.

infrastructure name—(QFabric systems only) (Optional) Display boot time messages on the fabric control Routing Engine or fabric manager Routing engines.

interconnect-device name—(QFabric systems only) (Optional) Display boot time messages on the Interconnect device.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display boot time messages for a specific T640 router connected to
a TX Matrix router. On a TX Matrix Plus router, display boot time messages for a specific router connected to a TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on the local Virtual Chassis member.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Display boot time messages on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

node-group name—(QFabric systems only) (Optional) Display boot time messages on the Node group.

scc—(TX Matrix routers only) (Optional) Display boot time messages for the TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus routers only) (Optional) Display boot time messages for the TX Matrix Plus router. Replace number with 0.

Additional Information

By default, when you issue the show system boot-messages command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

Required Privilege Level

text

Related Documentation

- Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output

- show system boot-messages (TX Matrix Router) on page 644
- show system boot-messages lcc (TX Matrix Router) on page 645
- show system boot-messages (TX Matrix Plus Router) on page 646
- show system boot-messages (QFX3500 Switch) on page 646
Sample Output
show system boot-messages (TX Matrix Router)

user@host> show system boot-messages
Copyright (c) 1992–1998 FreeBSD Inc.
Copyright (c) 1996–2000 Juniper Networks, Inc.
All rights reserved.
The Regents of the University of California. All rights reserved.

JUNOS 4.1-20000216-Zf8469 #0: 2000-02-16 12:57:28 UTC
tlim@single.juniper.net:/p/build/20000216-0905/4.1/release_kernel/sys/compile/GENERIC
CPU: Pentium Pro (332.55-MHz 686-class CPU)
        Origin = "GenuineIntel"  Id = 0x66a  Stepping=10
        Features=0x183f9ff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,SEP,MTRR,PGE,MCA,CMOV,<b
16>,<b17>,MMX,<b24>>
Teknor CPU Card Recognized
real memory = 805306368 (786432K bytes)
avail memory = 786280448 (767852K bytes)
Probing for devices on PCI bus 0:
  chip0 <generic PCI bridge (vendor=8086 device=7192 subclass=0)> rev 3 class 6000
  0 on pci0:0:0
  chip1 <Intel 82371AB PCI-ISA bridge> rev 1 class 60100 on pci0:7:0
  chip2 <Intel 82371AB IDE interface> rev 1 class 10180 on pci0:7:1
  chip3 <Intel 82371AB USB interface> rev 1 class c0300 int d irq 11 on pci0:7:2
  smb0 <Intel 82371AB SMB controller> rev 1 class 68000 on pci0:7:3
  pcic0 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int a irq 15 on pci0:13
    :0
    TI1131 PCI Config Reg: [pci only][FUNC0 pci int]
    pcic1 <TI PCI-1131 PCI-CardBus Bridge> rev 1 class 60700 int b irq 12 on pci0:13
    :1
    TI1131 PCI Config Reg: [pci only][FUNC1 pci int]
  fxp0 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 12 on
    pci0:16:0
  chip4 <generic PCI bridge (vendor=1011 device=0022 subclass=4)> rev 4 class 6040
  0 on pci0:17:0
  fxp1 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on
    pci0:19:0
Probing for devices on PCI bus 1:
  mcs0 <Miscellaneous Control Subsystem> rev 12 class ff0000 int a irq 12 on pci1:
    13:0
  fxp2 <Intel EtherExpress Pro 10/100B Ethernet> rev 8 class 20000 int a irq 10 on
    pci1:14:0
Probing for devices on the ISA bus:
  sc0 at 0x60-0x6f irq 1 on motherboard
  sc0: EGA color <16 virtual consoles, flags=0x0>
ed0 not found at 0x300
  ed1 not found at 0x280
  ed2 not found at 0x340
  psm0 not found at 0x60
  sio0 at 0x3f8-0x3ff irq 4 flags 0x20010 on isa
  sio0: type 16550A, console
  sio1 at 0x3e8-0x3ef irq 5 flags 0x20000 on isa
  sio1: type 16550A
  sio2 at 0x2f8-0x2ff irq 3 flags 0x20000 on isa
  sio2: type 16550A
show system boot-messages lcc (TX Matrix Router)

user@host> show system boot-messages lcc2
lcc2-re0:

Copyright (c) 1996-2001, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2001 The FreeBSD Project.
The Regents of the University of California. All rights reserved.
JUNOS 7.0-20040912.0 #0: 2004-09-12 09:16:32 UTC

builder@benten.juniper.net:/build/benten-b/7.0/20040912.0/obj-i386/sys/compile/JUNIPER
Timecounter "i8254" frequency 1193182 Hz
Timecounter "TSC" frequency 601368936 Hz
CPU: Pentium III/Pentium III Xeon/Celeron (601.37-MHz 686-class CPU)

Features=0x387f9ff<FPU,VME,DE,PSE,MCE,CX8,SEP,MTRR,PE,8086,MMX,FXSR,SSE>
real memory = 2147467264 (2097136K bytes)

Copyright © 2013, Juniper Networks, Inc.

Chapter 20: Administration
show system boot-messages (TX Matrix Plus Router)

user@host> show system boot-messages
sfc0-re0:
-----------------------------------------------
Copyright (c) 1996-2009, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
The Regents of the University of California. All rights reserved.
JUNOS 9.6B3.3 #0: 2009-06-17 19:52:08 UTC

build@lanath.juniper.net:/volume/build/junos/9.6/release/9.6B3.3/obj-i386/bsd/sys/compile/JUNIPER
MTable: Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Xeon(R) CPU           L5238  @ 2.66GHz (2660.01-MHz 686-class CPU) Origin =
"GenuineIntel"  Id = 0x1067a  Stepping = 10  Features=0xbfebfbff
...
lcc1-re0:
-----------------------------------------------
Copyright (c) 1996-2009, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
The Regents of the University of California. All rights reserved.
JUNOS 9.6-20090617.0 #0: 2009-06-17 04:15:14 UTC

build@lanath.juniper.net:/volume/build/junos/9.6/production/20090617.0/obj-i386/bsd/sys/compile/JUNIPER
Timecounter "i8254" frequency 1193182 Hz quality 0
CPU: Intel(R) Xeon(R) CPU                  @ 1.86GHz (1862.01-MHz 686-class CPU)
Origin = "GenuineIntel"  Id = 0x1067a  Stepping = 10  Features=0xbfebfbff
...

show system boot-messages (QFX3500 Switch)

user@switch> show system boot-messages
getmemsize: msgbufp[size=32768] = 0x81d07fe4

System physical memory distribution:
-----------------------------------------------
Total physical memory: 4160749568 (3968 MB)
Physical memory used: 3472883712 (3280 MB)
Physical memory allocated to kernel: 2130706432 (2032 MB)
Physical memory allocated to user BTLB: 1342177280 (1280 MB)

Copyright (c) 1996-2010, Juniper Networks, Inc.
All rights reserved.
Copyright (c) 1992-2006 The FreeBSD Project.
The Regents of the University of California. All rights reserved.
JUNOS 11.1L #0: 2010-09-17 19:18:07 UTC

ssiano@svl-junos-pool125.juniper.net:/c/ssiano/DEV_QFX_SI_BRANCH/03/20100917.399988/
obj-xlr/bsd/sys/compile/JUNIPER-DCTOR
WARNING: debug.mpsafenet forced to 0 as ipsec requires Giant
JUNOS 11.1I #0: 2010-09-17 19:18:07 UTC

ssiano@svl-junos-pool125.juniper.net:/c/ssiano/DEV_QFX_SI_BRANCH/03/20100917.399988/
obj-xlr/bsd/sys/compile/JUNIPER-DCTOR
real memory = 3472883712 (3312MB)
avail memory = 1708171264 (1629MB)
cpuid: 0, btlb_cpumap:0xffffffff
FreeBSD/SMP: Multiprocessor System Detected: 12 CPUs
ETHERNET SOCKET BRIDGE initialising
Initializing QFX platform properties..
cpu0 on motherboard
  : RMI's XLR CPU Rev. 0.3 with no FPU implemented
  L1 Cache: I size 32kb(32 line), D size 32kb(32 line), eight way.
  L2 Cache: Size 1024kb, eight way
pic_lbus0: <XLR Local Bus>
  on motherboard
Enter qfx control ethernet probe addr:0xc5eeec00
  gmac4: <XLR GMAC GE Ethernet> on pic_lbus0
me0: Ethernet address 00:1d:b5:f7:68:40
  Enter qfx control ethernet probe addr:0xc5eeeb40
  gmac5: <XLR GMAC GE Ethernet> on pic_lbus0
me1: Ethernet address 00:1d:b5:f7:68:41
  Enter qfx control ethernet probe addr:0xc5eeea80
  gmac6: <XLR GMAC GE Ethernet> on pic_lbus0
sio0 on pic_lbus0
  Entering sioattach
  sio0: type 16550A, console
  xls_setup_intr: skip irq 3, xlr regs are set up somewhere else.
  gblmem0 on pic_lbus0
ehci0: <RMI XLS USB 2.0 controller> on pic_lbus0
ehci_bus_attach: allocated resource.  tag=1, base=bef24000
ehcihw: endian hardware swapping NOT enabled.
usb0: EHCI version 1.0
usb0 on ehci0
usb0: USB revision 2.0
uhub0: vendor 0x0000 EHCI root hub, class 9/0, rev 2.00/1.00, addr 1
  2 ports with 2 removable, self powered
umass0: USB USBFlashDrive, rev 2.00/11.00, addr 2
pci0: PCIe link 0 up
pci0: PCIe link 2 up
pci0: PCIe link 3 up
pci0: <XLS PCI Host Controller> on pic_lbus0
pci0: <PCI bus on pci0
pci1: <PCI-PCI bridge> at device 0.0 on pci0
pci1: <PCI bus on pci1
pci1: <network, ethernet> at device 0.0 (no driver attached)
pci2: <PCI-PCI bridge> at device 1.0 on pci0
pci2: <PCI bus on pci2
pci2: <network, ethernet> at device 0.0 (no driver attached)
pci3: <PCI-PCI bridge> at device 2.0 on pci0
pci3: <PCI bus on pci3
pci3: <network, ethernet> at device 0.0 (no driver attached)
cfi device address space at 0xbc000000
cfi0: <AMD/Fujitsu - 8MB> on pic_lbus0
cfi device address space at 0xbc000000
i2c0: <I2C bus controller> on pic_lbus0
i2c1: <I2C bus controller> on pic_lbus0
qfx_fmn0 on pic_lbus0
pool offset 1503776768
xlr_bus0: <XLR Local Bus Controller> on motherboard
qfx_bcpld_probe[124]
qfx_bcpld_probe[138]: dev_type=0x0
qfx_bcpld_probe[124]
qfx_bcpld0: QFX BCPLD probe success
qfx_bcpld0qfx_bcpld_attach[174]
qfx_bcpld_attach[207] : bus_space_tag=0x0, bus_space_handle=0xbd900000
qfx_bcpld_probe[124]
qfx_bcpld1: QFX BCPLD probe success
qfx_bcpld1qfx_bcpld_attach[174]
tor_bcpld_slave_attach[1245] : bus_space_tag=0x0, bus_space_handle=0xbda00000
Initializing product: 96 ..
bmeb: bmeb_lib_init done 0xc60a5000, addr 0x809c99a0
bme0:Virtual BME driver initializing
Timecounter "mips" frequency 1200000000 Hz quality 0
Timecounter "xlr_pic_timer" frequency 66666666 Hz quality 1
Timecounters tick every 1.000 msec
Loading the NETPFE fc module
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #7 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #11 Launched!
SMP: AP CPU #10 Launched!
SMP: AP CPU #9 Launched!
SMP: AP CPU #8 Launched!
da0 at umass-sim0 bus 0 target 0 lun 0
da0: <USB USBFlashDrive 1100> Removable Direct Access SCSI-0 device
da0: 40.000MB/s transfers
da0: 3920MB (8028160 512 byte sectors: 255H 63S/T 499C)
Trying to mount root from ufs:/dev/da0s1a
show system license

**Syntax**

```
show system license
<installed | keys | usage>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display licenses and information about how they are used.

**Options**

- `none`—Display all license information.
- `installed`—(Optional) Display installed licenses only.
- `keys`—(Optional) Display a list of license keys. Use this information to verify that each expected license key is present.
- `usage`—(Optional) Display the state of licensed features.

**Required Privilege**

- Level: maintenance

**List of Sample Output**

- `show system license on page 650`
- `show system license installed on page 650`
- `show system license keys on page 651`
- `show system license usage on page 651`
- `show system license (QFX Series) on page 651`

**Output Fields**

Table 107 on page 649 lists the output fields for the `show system license` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Feature name</strong></td>
<td>Name assigned to the configured feature. You use this information to verify that all the features for which you installed licenses are present.</td>
</tr>
<tr>
<td><strong>Licenses used</strong></td>
<td>Number of licenses used by a router or switch. You use this information to verify that the number of licenses used matches the number configured. If a licensed feature is configured, the feature is considered used.</td>
</tr>
</tbody>
</table>

**NOTE:** In Junos OS Release 10.1 and later, the **Licenses used** column displays the actual usage count based on the number of active sessions or connections as reported by the corresponding feature daemons. This is applicable for scalable license-based features such as Subscriber Access (`scale-subscriber`), L2TP (`scale-l2tp`), Mobile IP (`scale-mobile-ip`), and so on.
Table 107: show system license Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licenses installed</td>
<td>Information about the installed license key:</td>
</tr>
<tr>
<td></td>
<td>• <strong>License identifier</strong>—Identifier associated with a license key.</td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>—State of the license key: <strong>valid</strong> or <strong>invalid</strong>. A <strong>invalid</strong> state indicates that the key was entered incorrectly or is not valid for the specific device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>License version</strong>—Version of a license. The version indicates how the license is validated, the type of signature, and the signer of the license key.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Valid for device</strong>—Device that can use a license key.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Group defined</strong>—Group membership of a device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Features</strong>—Feature associated with a license, such as data link switching (DLSw).</td>
</tr>
<tr>
<td>Licenses needed</td>
<td>Number of licenses required for features being used but not yet properly licensed.</td>
</tr>
<tr>
<td>Expiry</td>
<td>Amount of time left within the grace period before a license is required for a feature being used.</td>
</tr>
</tbody>
</table>

Sample Output
show system license

user@host> show system license

License usage:

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Licenses used</th>
<th>Licenses installed</th>
<th>Licenses needed</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscriber-accounting</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-authentication</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-address-assignment</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-vlan</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-ip</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>scale-subscriber</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>scale-l2tp</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>scale-mobile-ip</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
</tbody>
</table>

Licenses installed:
License identifier: XXXXXXXXXX
License version: 2
Features:

- subscriber-accounting - Per Subscriber Radius Accounting
  permanent
- subscriber-authentication - Per Subscriber Radius Authentication
  permanent
- subscriber-address-assignment - Radius/SRC Address Pool Assignment
  permanent
- subscriber-vlan - Dynamic Auto-sensed Vlan
  permanent
- subscriber-ip - Dynamic and Static IP
  permanent

show system license installed

user@host> show system license installed
License identifier: XXXXXXXXXX
License version: 2
Features:
subscriber-accounting - Per Subscriber Radius Accounting
permanent
subscriber-authentication - Per Subscriber Radius Authentication
permanent
subscriber-address-assignment - Radius/SRC Address Pool Assignment
permanent
subscriber-vlan - Dynamic Auto-sensed Vlan
permanent
subscriber-ip - Dynamic and Static IP
permanent

show system license keys

user@host> show system license keys
XXXXXXXXX xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxx xxxxxx xxxxxx xxxxxx xxxxxx
xxxxxx xxxxxx xxxxxx

show system license usage

user@host> show system license usage
License usage:

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Licenses used</th>
<th>Licenses installed</th>
<th>Licenses needed</th>
<th>Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>subscriber-accounting</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-authentication</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-address-assignment</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-vlan</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>subscriber-ip</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>scale-subscriber</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>scale-l2tp</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>permanent</td>
</tr>
<tr>
<td>scale-mobile-ip</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>permanent</td>
</tr>
</tbody>
</table>

show system license (QFX Series)

user@switch> show system license
License usage:

<table>
<thead>
<tr>
<th>Feature name</th>
<th>Licenses used</th>
<th>Licenses installed</th>
<th>Licenses needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>qfx-edge-fab</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Licenses installed:
License identifier: JUNOS417988
License version: 1
Features:
qfx-edge-fab - QFX3000 Series QF/Node feature license
permanent
show system snapshot

**Syntax**

```
show system snapshot
```

**Syntax (EX Series Switches)**

```
show system snapshot
<all-members|local|member member-id>
<media (external | internal)>
```

**Release Information**

Command introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 10.0 for EX Series switches.

**Description**

Display information about the backup software:

- On the routers, display information about the backup software, which is located in the `/altroot`, and `/altconfig` file systems or on the alternate media.

- On the switches, display information about the backup of the root file system (/) and directories `/altroot`, `/config`, `/var`, and `/var/tmp`, which are located either on an external USB flash drive or in internal flash memory.

**NOTE:** To back up software, use the `request system snapshot` command.

**Options**

- `none`—Display information about the backup software.

- `all-members | local | member member-id`—(EX Series switch Virtual Chassis only) (Optional) Display the snapshot in a Virtual Chassis:
  - `all-members`—Display the snapshot for all members of the Virtual Chassis.
  - `local`—Display the snapshot on the member of the Virtual Chassis that you are currently logged into.
  - `member member-id`—Display the snapshot for the specified member of the Virtual Chassis.

- `media (external | internal)`—(EX Series switch only) (Optional) Display the destination media location for the snapshot. The `external` option specifies the snapshot on an external mass storage device, such as a USB flash drive. The `internal` option specifies the snapshot on an internal memory source, such as internal flash memory. If no additional options are specified, the command displays the snapshot stored in both slices.

**Required Privilege Level**

- `view`

**Related Documentation**

- `request system snapshot on page 614`

**List of Sample Output**

- `show system snapshot (Router) on page 653`
Output Fields  
Table 108 on page 653 lists the output fields for the `show system snapshot` command. Output fields are listed in the approximate order in which they appear.

Table 108: show system snapshot Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation date</td>
<td>Date and time of the last snapshot.</td>
</tr>
<tr>
<td>JUNOS version on snapshot</td>
<td>Junos OS release number of individual software packages.</td>
</tr>
</tbody>
</table>

Sample Output

show system snapshot (Router)

```
user@host> show system snapshot
Information for snapshot on hard-disk
Creation date: Oct 5 13:53:29 2005
JUNOS version on snapshot:
  jbase : 7.3R2.5
  jcrypto: 7.3R2.5
  jdocs : 7.3R2.5
  jkernel: 7.3R2.5
  jpfe   : M40-7.3R2.5
  jroute : 7.3R2.5
```

show system snapshot media external (Switch)

```
user@switch> show system snapshot media external
Information for snapshot on external (/dev/da1s1a) (backup)
Creation date: Mar 19 03:37:18 2012
JUNOS version on snapshot:
  jbase : ex-12.1I20120111_0048_user
  jcrypto-ex: 12.1I20120111_0048_user
  jdocs-ex: 12.1I20120111_0048_user
  jkernel-ex: 12.1I20120111_0048_user
  jroute-ex: 12.1I20120111_0048_user
  jswitch-ex: 12.1I20120111_0048_user
  jweb-ex: 12.1I20120111_0048_user
Information for snapshot on external (/dev/da1s2a) (primary)
Creation date: Mar 19 03:38:25 2012
JUNOS version on snapshot:
  jbase : ex-12.2I20120305_2240_user
  jcrypto-ex: 12.2I20120305_2240_user
  jdocs-ex: 12.2I20120305_2240_user
  jkernel-ex: 12.2I20120305_2240_user
  jroute-ex: 12.2I20120305_2240_user
  jswitch-ex: 12.2I20120305_2240_user
  jweb-ex: 12.2I20120305_2240_user
```

show system snapshot media internal (Switch)

```
user@switch> show system snapshot media internal
Information for snapshot on internal (/dev/da0s1a) (backup)
Creation date: Mar 14 05:01:02 2011
JUNOS version on snapshot:
  jbase : 11.1R1.9
```
Information for snapshot on internal (/dev/da0s2a) (primary)
Creation date: Mar 30 08:46:27 2011
JUNOS version on snapshot:
  jbase : 11.2-20110330.0
  jcrypto-ex: 11.2-20110330.0
  jdocs-ex: 11.2-20110330.0
  jkernel-ex: 11.2-20110330.0
  jroute-ex: 11.2-20110330.0
  jswitch-ex: 11.2-20110330.0
  jweb-ex: 11.2-20110330.0
  jpfe-ex2x: 11.2-20110330.0
show system storage partitions (EX Series Switches Only)

Syntax

```
show system storage partitions
<all-members>
<local>
<member member-id>
```

Release Information

Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Display information about the disk partitions on EX Series switches.

Options

- `none`—Display partition information.
- `all-members`—(Virtual Chassis systems only) (Optional) Display partition information for all members of the Virtual Chassis.
- `local`—(Virtual Chassis systems only) (Optional) Display partition information for the local Virtual Chassis member.
- `member member-id`—(Virtual Chassis systems only) (Optional) Display partition information for the specified member of the Virtual Chassis configuration.

Required Privilege

view

Related Documentation

- Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 598

List of Sample Output

show system storage partitions on page 656

Output Fields

Table 109 on page 655 describes the output fields for the `show system storage partitions` command. Output fields are listed in the approximate order in which they appear.

Table 109: show system storage partitions Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Media</td>
<td>Media (internal or external) from which the switch was booted.</td>
</tr>
<tr>
<td>Active Partition</td>
<td>Name of the active root partition.</td>
</tr>
<tr>
<td>Backup Partition</td>
<td>Name of the backup (alternate) root partition.</td>
</tr>
<tr>
<td>Currently booted from</td>
<td>Partition from which the switch was last booted.</td>
</tr>
<tr>
<td>Partitions information</td>
<td>Information about partitions on the boot media:</td>
</tr>
<tr>
<td></td>
<td>• Partition—Partition identifier.</td>
</tr>
<tr>
<td></td>
<td>• Size—Size of partition.</td>
</tr>
<tr>
<td></td>
<td>• Mountpoint—Directory on which the partition is mounted.</td>
</tr>
</tbody>
</table>
Sample Output

show system storage partitions

user@switch> show system storage partitions
fpc0:
--------------------------------------------------------------------------
Boot Media: internal (da0)
Active Partition: da0s1a
Backup Partition: da0s2a
Currently booted from: active (da0s1a)

Partitions information:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size</th>
<th>Mountpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>184M</td>
<td>/</td>
</tr>
<tr>
<td>s2a</td>
<td>184M</td>
<td>altroot</td>
</tr>
<tr>
<td>s3d</td>
<td>369M</td>
<td>/var/tmp</td>
</tr>
<tr>
<td>s3e</td>
<td>123M</td>
<td>/var</td>
</tr>
<tr>
<td>s4d</td>
<td>62M</td>
<td>/config</td>
</tr>
<tr>
<td>s4e</td>
<td></td>
<td>unused (backup config)</td>
</tr>
</tbody>
</table>
CHAPTER 21

Troubleshooting Procedures

- Troubleshooting Software Installation on page 657
- Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 660
- Resilient Dual-Root Partitions Frequently Asked Questions on page 661

Troubleshooting Software Installation

This topic describes troubleshooting issues with software installations on EX Series switches.

- Recovering from a Failed Software Upgrade on an EX Series Switch on page 657
- Rebooting from the Inactive Partition on page 658
- Freeing Disk Space for Software Installation on page 659
- Installation from the Boot Loader Generates 'cannot open package' Error on page 659

Recovering from a Failed Software Upgrade on an EX Series Switch

Problem  If Junos OS loads but the CLI is not working, or if the switch has no software installed, use this recovery installation procedure to install Junos OS.

Solution  If there is already a Junos OS image on the system, you can either install the new Junos OS package in a separate partition and have both Junos OS images remain on the system, or you can wipe the disk clean before the new installation proceeds.

If there is no Junos OS image on the system, follow the instructions in "Booting an EX Series Switch Using a Software Package Stored on a USB Flash Drive" on page 590 to get an image on the system and boot the switch.

To perform a recovery installation:

1. Power on the switch. The loader script starts.

   After the message Loading /boot/defaults/loader.conf displays, you are prompted with:

   Hit [Enter] to boot immediately, or space bar for command prompt.

2. Press the space bar to enter the manual loader. The loader> prompt displays.

3. Enter the following command:
loader> install [– --format] [– --external] source

where:

- **format**—Use this option to wipe the installation media before installing the software package. If you do not include this option, the system installs the new Junos OS package in a different partition from the partition used by the most recently installed Junos OS package.

- **external**—Use this option to install the software package on an external medium.

- **source**—Represents the name and location of the Junos OS package either on a server on the network or as a file on the USB flash drive:
  - Network address of the server and the path on the server; for example, `tftp://192.17.1.28/junos/jinstall-ex-4200-9.4R1.5-domestic-signed.tgz`
  - The Junos OS package on a USB device is commonly stored in the root drive as the only file; for example, `file:///jinstall-ex-4200-9.4R1.5-domestic-signed.tgz`

The boot process proceeds as normal and ends with a login prompt.

**Rebooting from the Inactive Partition**

**Problem**  EX Series switches shipped with Junos OS Release 10.4R2 or earlier have Junos OS loaded on the system disk in partition 1. The first time you upgrade, the new software package is installed in partition 2. When you finish the installation and reboot, partition 2 becomes the active partition. Similarly, subsequent software packages are installed in the inactive partition, which becomes the active partition when you reboot at the end of the installation process.

On switches shipped with Release 10.4R3 and later, the same Junos OS image is loaded in each of the two root partitions, and you should copy the new software image to the alternate partition each time you upgrade.

If you performed an upgrade and rebooted, the system resets the active partition. You can use this procedure to manually boot from the inactive partition.

**NOTE:** If you have completed the installation of the software image but have not yet rebooted, issue the request system software rollback command to return to the original software installation package.

**Solution**  Reboot from the inactive partition:

```
user@switch> request system reboot slice alternate
```
NOTE: If you cannot access the CLI, you can reboot from the inactive partition using the following procedure from the loader script prompt:

1. Unload and clear the interrupted boot from the active partition:
   
   ```
   loader> unload
   loader> unset vfs_root.mountfrom
   ```

2. Select the new (inactive) partition to boot from:
   
   ```
   loader> set currdev=diskx:y:
   ```
   
   where x is either 0 (internal) or 1 (external) and the y indicates the number of the inactive partition, either 1 or 2.
   
   You must include the colon (:) at the end of this command.

3. Boot Junos OS from the inactive partition:
   
   ```
   loader> boot
   ```

Freeing Disk Space for Software Installation

**Problem** The software installation process requires a certain amount of unused disk space. If there is not enough space, you might receive an error message such as:

```
fetch: /var/tmp/incoming-package.tgz: No space left on device
```

**Solution** Identify and delete unnecessary files by using the `request system storage cleanup` command.

Installation from the Boot Loader Generates 'cannot open package' Error

**Problem** When installing a Junos OS software image from the loader prompt, a “cannot open package error” is generated:

```
loader> install - -format
tftp://10.204.33.248/images/Flash_corr/official/jinstall-ex-4200-10.4I2011012-domestic-signed.tgz
Speed: 1000, full duplex
bootp: no reply
No response for RARP request
net_open: RARP failed
cannot open package (error 5)
```

**Solution** This might be due to the IP address, gateway IP address, netmask address, or server IP address not being properly set. You can set these values either from the shell or from the u-boot prompt.

To set these values from the shell:

```
% nvram setenv ipaddr 10.204.35.235
% nvram setenv netmask 255.255.240.0
% nvram setenv gatewayip 10.204.47.254
% nvram setenv serverip 10.204.33.248
```
To set these values from the u-boot prompt, log in to a console connection, reboot, and stop at the u-boot prompt (Ctrl+c):

```
=> setenv ipaddr 10.204.35.235
=> setenv gatewayip 10.204.47.254
=> setenv serverip 10.204.33.248
=> setenv netmask 255.255.240.0
=> saveenv
=> printenv Verify whether variables are set properly or not
=> boot
```

Related Documentation

- Installing Software on an EX Series Switch with a Single Routing Engine (CLI Procedure)
- Upgrading Software on an EX6200 or EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure)
- Installing Software on EX Series Switches (J-Web Procedure)
- Understanding Software Installation on EX Series Switches on page 571
- show system storage partitions (EX Series Switches Only) on page 655

Troubleshooting a Switch That Has Booted from the Backup Junos OS Image

**Problem**
The switch boots from the backup root file partition. It is possible that the primary copy of JUNOS OS failed to boot properly, which could indicate that it is corrupted. This event is flagged in two ways:

- Upon login through the console or management port, the following warning message is displayed:

```
WARNING: THIS DEVICE HAS BOOTED FROM THE BACKUP JUNOS IMAGE
```

It is possible that the primary copy of JUNOS failed to boot up properly, and so this device has booted from the backup copy.

Please re-install JUNOS to recover the primary copy in case it has been corrupted.

- The following alarm message is generated:

```
user@switch> show chassis alarms
1 alarms currently active
Alarm time     Class    Description
2011-02-17 05:48:49 PST Minor Host 0 Boot from backup root
```

If the switch is in a Virtual Chassis, the switch member number appears in the **Description** field, where the switch is called a host.

**Solution**
Install a new Junos OS image on the partition that had the corruption, or take a snapshot (use `request system snapshot`) of the currently active partition and use it to replace the image in the alternate partition:

If the switch is a standalone switch or a Virtual Chassis master switch, enter this command:

```
user@switch> request system snapshot slice alternate
```
If the switch is a Virtual Chassis member switch (not the master), enter this command on the Virtual Chassis:

```
user@switch> request systemsnapshotslicealternatemember member-id
```

where `member-id` is the Virtual Chassis member ID number.

---

### Resilient Dual-Root Partitions Frequently Asked Questions

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Resilient Dual-Root Partitions Frequently Asked Questions*. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

This FAQ addresses questions regarding resilient dual-root partitions on EX Series switches. The resilient dual-root partition feature was introduced on EX Series switches at Junos OS Release 10.4R3. It provides additional resiliency for EX Series switches.

This FAQ covers the following questions:

- What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Enabled? on page 661
- What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Not Enabled? on page 662
- How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System? on page 663

### What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Enabled?

If the automatic snapshot feature is enabled during a reboot, the system automatically takes a snapshot of Junos OS from the alternate root partition (Slice 2) and copies it onto the primary root partition (Slice 1). The system checks each file system partition for corruption. Table 110 on page 662 shows the action the system takes if corruption is detected and the corrective action that you can take.
Table 110: Actions If Corrupt Files Are Found and Automatic Snapshot is Enabled

<table>
<thead>
<tr>
<th>Slice 1</th>
<th>Slice 2</th>
<th>Slice 3</th>
<th>Slice 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>s2a</td>
<td>s3e</td>
<td>s3d</td>
</tr>
<tr>
<td>/</td>
<td>/</td>
<td>/var</td>
<td>/var/tmp</td>
</tr>
</tbody>
</table>

(root Junos OS) (root Junos OS)

If a root directory (/) is corrupted, the corrupted file system is not mounted. The switch automatically takes a snapshot of the Junos OS root file system and copies it onto the primary root partition. It boots from the alternate slice, but the next reboot happens from the primary slice.

Corrective action: No corrective action is required.

Corrective action: Restore the /var or /config files from the external backup.

What Happens to My Files If the System Detects a File System Corruption and Automatic Snapshot is Not Enabled?

During a reboot, the system checks each file system partition for corruption. Table 111 on page 662 shows the action the system takes if corruption is detected and the corrective action that you can take.

Table 111: Actions If Corrupt Files Are Found

<table>
<thead>
<tr>
<th>Slice 1</th>
<th>Slice 2</th>
<th>Slice 3</th>
<th>Slice 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>s1a</td>
<td>s2a</td>
<td>s3e</td>
<td>s3d</td>
</tr>
<tr>
<td>/</td>
<td>/</td>
<td>/var</td>
<td>/var/tmp</td>
</tr>
</tbody>
</table>

(root Junos OS) (root Junos OS)

If a root directory (/) is corrupted, the corrupted file system is not mounted and the switch boots from the alternate slice.

Corrective action: Issue a request system snapshot command from the good root directory to the corrupted slice.

Corrective action: Restore the /var or /config files from the external backup.
How Will I Be Informed If My Switch Boots from the Alternate Slice Because of Corruption in the Root File System?

If the switch detects corruption in the primary root file system, it boots from the alternate root partition. When this occurs, the type of notification depends on whether you have enabled the automatic snapshot feature or not:

• If the automatic snapshot feature is not enabled:
  • If you are logged in through the console port or the management port:
    WARNING: THIS DEVICE HAS BOOTTED FROM THE BACKUP JUNOS IMAGE

    It is possible that the primary copy of JUNOS failed to boot up properly, and so this device has booted from the backup copy.

    Please re-install JUNOS to recover the primary copy in case it has been corrupted.

    The following message is displayed when you issue `show chassis alarms`:

    user@switch: > show chassis alarms
    1 alarms currently active
    Alarm time               Class  Description
    2011-02-17 05:48:49 PST  Minor  Host 0 Boot from backup root

• If the automatic snapshot feature is enabled:
  • A banner message appears, indicating that an automatic snapshot operation is in progress. The banner message disappears when the snapshot operation is complete.
  • No alarm is issued to indicate that the switch has been rebooted from the alternate partition. However, the switch does log the event.

Related Documentation:
• Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 598
• Troubleshooting Software Installation on page 657
• Troubleshooting a Switch That Has Booted from the Backup Junos OS Image on page 660
• Verifying Junos OS and Boot Loader Software Versions on an EX Series Switch on page 598
PART 8

System Monitoring

- Overview on page 667
- Configuration on page 689
- Administration on page 705
CHAPTER 22

Overview

- Software Overview on page 667
- Alarms Overview on page 669
- Dashboard Overview on page 670
- Hardware/CLI Terminology Mapping Overview on page 686

Software Overview

- Understanding Software Infrastructure and Processes on page 667

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 667
- Junos OS Processes on page 668

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.

- Routing Engine—Provides three main functions:
- Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network.
- Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

### Junos OS Processes

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 61 on page 112 describes the primary Junos OS processes.

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis process</td>
<td>chassid</td>
<td>Detects hardware on the system that is used to configure network interfaces. Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered. Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</td>
</tr>
<tr>
<td>Ethernet switching process</td>
<td>eswd</td>
<td>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANS, and VLAN interfaces. Manages Ethernet switching interfaces, VLANS, and VLAN interfaces.</td>
</tr>
<tr>
<td>Forwarding process</td>
<td>pfem</td>
<td>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</td>
</tr>
<tr>
<td>Interface process</td>
<td>dcd</td>
<td>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</td>
</tr>
</tbody>
</table>
Table 112: Junos OS Processes (continued)

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management process</td>
<td>mgd</td>
<td>Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the switch. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</td>
</tr>
<tr>
<td>Routing protocol process</td>
<td>rpd</td>
<td>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- For more information about processes, see *Junos OS Network Operations Guide*
- For more information about basic system parameters, supported protocols, and software processes, see *Junos OS System Basics Configuration Guide*

**Alarms Overview**

- Understanding Alarm Types and Severity Levels on EX Series Switches on page 669

**Understanding Alarm Types and Severity Levels on EX Series Switches**

Before monitoring alarms on the switch, become familiar with the terms defined in Table 113 on page 669.

Table 113: Alarm Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm</td>
<td>Signal alerting you to conditions that might prevent normal operation. On a switch, the alarm signal is the yellow <strong>ALARM</strong> LED lit on the front of the chassis.</td>
</tr>
<tr>
<td>alarm condition</td>
<td>Failure event that triggers an alarm.</td>
</tr>
<tr>
<td>alarm severity</td>
<td>Seriousness of the alarm. The level of severity can be either major (red) or minor (yellow).</td>
</tr>
<tr>
<td>chassis alarm</td>
<td>Predefined alarm triggered by a physical condition on the switch such as a power supply failure, excessive component temperature, or media failure.</td>
</tr>
<tr>
<td>system alarm</td>
<td>Predefined alarm triggered by a missing rescue configuration or failure to install a license for a licensed software feature.</td>
</tr>
</tbody>
</table>

**Alarm Types**
The switch supports these alarms:

- **Chassis alarms** indicate a failure on the switch or one of its components. Chassis alarms are preset and cannot be modified.

- **System alarms** indicate a missing rescue configuration. System alarms are preset and cannot be modified, although you can configure them to appear automatically in the J-Web interface display or CLI display.

### Alarm Severity Levels

Alarms on Juniper Networks EX Series Ethernet Switches have two severity levels:

- **Major (red)**—Indicates a critical situation on the switch that has resulted from one of the following conditions. A red alarm condition requires immediate action.
  - One or more hardware components have failed.
  - One or more hardware components have exceeded temperature thresholds.
  - An alarm condition configured on an interface has triggered a critical warning.

- **Minor (yellow or amber)**—Indicates a noncritical condition on the switch that, if left unchecked, might cause an interruption in service or degradation in performance. A yellow alarm condition requires monitoring or maintenance.

A missing rescue configuration generates a yellow system alarm.

### Related Documentation

- Checking Active Alarms with the J-Web Interface on page 708
- Dashboard for EX Series Switches on page 670

### Dashboard Overview

- Dashboard for EX Series Switches on page 670

### Dashboard for EX Series Switches

When you log in to the J-Web user interface, the dashboard for the Juniper Networks EX Series Ethernet Switches appears. Use the dashboard to view system information.

The dashboard comprises four panels and a graphical chassis viewer. Click **Preferences** to choose which panels are to be displayed and set the refresh interval for chassis viewer information. Click **OK** to save your preference changes and return to the dashboard or click **Cancel** to return to the dashboard without saving changes.

**NOTE:** You can drag the various panels to different locations in the J-Web window.
NOTE: In a Virtual Chassis, the default values are shown on the Dashboard panel when no chassis image is clicked. The panel display changes based on the image clicked.

This topic describes:

- System Information Panel on page 671
- Health Status Panel on page 673
- Capacity Utilization Panel on page 675
- Alarms Panel on page 675
- File System Usage on page 675
- Chassis Viewer on page 675

### System Information Panel

Table 114: System Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System name</td>
<td>Indicates the local name of the EX Series switch. The local name of the EX Series switches changes when an individual image is clicked.</td>
</tr>
</tbody>
</table>
| Device model   | Indicates the model of the EX Series switch. In a Virtual Chassis configuration, to indicate the model of a switch, click the image of that switch.  

**NOTE:** In a Virtual Chassis setup for an EX6210, EX8208, or EX8216 switch, the Device model field displays details of the master Routing Engine. To view details of a member, select it.
Table 114: System Information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory details</td>
<td>Indicates the following:</td>
</tr>
<tr>
<td></td>
<td>• For EX3200 switches; and for EX2200, EX2200-C, EX3300, EX4200, EX4300, EX4500, and EX4550 switches that are not configured as Virtual Chassis, the value displayed in Inventory details field is always 1 FPC. FPC is a legacy term for a slot in a large Juniper Networks chassis; which simply refers to the standalone switch.</td>
</tr>
<tr>
<td></td>
<td>• For EX2200 and EX2200-C switches configured as a Virtual Chassis, the value displayed in the Inventory details field is 1–4 FPC, with the number corresponding to the number of member switches.</td>
</tr>
<tr>
<td></td>
<td>• For EX3300 switches configured as a Virtual Chassis, the value displayed in the Inventory details field is 1–6 FPC, with the number corresponding to the number of member switches.</td>
</tr>
<tr>
<td></td>
<td>• For EX4200, EX4300, EX4500, and EX4550 switches configured as a Virtual Chassis, the value displayed in the Inventory details field is 1–10 FPC, with the number corresponding to the number of member switches.</td>
</tr>
<tr>
<td></td>
<td>• For EX6210 switches, the values displayed in the Inventory details field are 1–2 CB and 1–9 FPC. CB, or Control Board, refers to the SRE module. FPC refers to line cards and the FPC within the CB.</td>
</tr>
<tr>
<td></td>
<td>• For an EX8208 switch, the values displayed in Inventory details field are 1–3 CB and 0–8 FPC. CB, or Control Board, refers to SRE and SF modules. FPC refers to line cards.</td>
</tr>
<tr>
<td></td>
<td>• For EX8216 switches, the values displayed in Inventory details field are 1–2 CB and 0–16 FPC. CB, or Control Board, refers to RE modules and FPC refers to line cards.</td>
</tr>
<tr>
<td></td>
<td>• For an XRE200 External Routing Engine in an EX8200 Virtual Chassis, the value displayed in Inventory details is 1 XRE. XRE refers to RE modules. For XRE200 External Routing Engines configured as a Virtual Chassis, the values displayed in Inventory details are 1–2 XRE and 0–4 LCC, where LCC refers to the EX8200 line card chassis.</td>
</tr>
<tr>
<td>Junos image</td>
<td>Indicates the version of the Junos OS image. In a Virtual Chassis configuration, the Junos OS image of the master switch is displayed by default. To display the Junos OS image of a specific switch, click the image of that switch.</td>
</tr>
<tr>
<td>Boot image</td>
<td>Indicates the version of the boot image that is used. In a Virtual Chassis configuration, the boot image of the master switch is displayed by default. To display the boot image of a specific switch, click the image of that switch.</td>
</tr>
<tr>
<td>Device uptime</td>
<td>Indicates the time since the last reboot. In a Virtual Chassis configuration, to display the uptime of the specific switch, click the image of that switch.</td>
</tr>
<tr>
<td>Last configured time</td>
<td>Indicates the time when the switch was last configured.</td>
</tr>
</tbody>
</table>
### Health Status Panel

#### Table 115: Health Status

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EX2200, EX2200-C, EX3200, EX3300, EX4200, and EX4300 Switches</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Memory util. | Indicates the memory used in the Routing Engine. In a Virtual Chassis configuration, the memory utilization value of the master Routing Engine is displayed.  
**NOTE:** In EX4300 Virtual Chassis, to display the Routing Engine memory utilization of the master or backup, click the respective images. |
| Flash | Indicates the usage and capacity of internal flash memory and any external USB flash drive.  
**NOTE:** In EX4300 Virtual Chassis, the flash memory utilization of the master switch is displayed by default. To display the flash memory utilization along with the internal and external flash memory utilization details for each switch or line card, mouse over individual switch or line card images. |
| Temp. | Indicates the chassis temperature status. Temperatures are listed in Celsius and the corresponding Fahrenheit values.  
**NOTE:** The **Temp** field is unavailable for a standalone EX2200-C switch.  
The **Temp** field is dynamically available for an EX2200 Virtual Chassis switch based on the model of the member clicked.  
**NOTE:** In an EX4300 Virtual Chassis, the temperature of the master Routing Engine is displayed by default. To display the temperature of the Routing Engine of any switch, click the image of that switch. |
| CPU load | Indicates the average CPU usage over 15 minutes. In a Virtual Chassis configuration, on loading the master or backup switch, the CPU load for that switch’s Routing Engine is displayed by default. To display the CPU load for a specific switch’s Routing Engine, click the image of that switch. |
| Fan status | Indicates the status of the fans in the fan tray. The possible values are **OK**, **Failed**, and **Absent**. In a Virtual Chassis configuration, the fan status of the master switch is displayed by default. To display the fan status for any switch, click the image of that switch.  
**NOTE:** The **Fan status** field is unavailable for a standalone EX2200-C switch.  
The **Fan status** field is dynamically available for an EX2200 Virtual Chassis switch based on the model of the member clicked. |
| **EX4500 and EX4550 Switches** |
| Memory util. | Indicates the memory used in the Routing Engine. In a Virtual Chassis configuration, the memory utilization value of the master Routing Engine is displayed. |
| Flash | Indicates the usage and capacity of internal flash memory and any external USB flash drive. |
| Temp. | Indicates the chassis temperature status. Temperatures in the dashboard are listed in Celsius and the corresponding Fahrenheit values.  
**NOTE:** The **Temp** field is unavailable for an EX4500 switch. |
| CPU load | Indicates the average CPU usage over 15 minutes. |
Table 115: Health Status (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan status</td>
<td>Indicates the status of the fans in the fan tray. The possible values are OK, Failed, and Absent. This field also indicates the direction of airflow of the fan tray. The possible values are Front to back and Back to front.</td>
</tr>
<tr>
<td>EX6210 Switches</td>
<td></td>
</tr>
<tr>
<td>Memory util.</td>
<td>Indicates the memory used in the master Routing Engine. Click the backup Routing Engine to view the memory used in the backup Routing Engine.</td>
</tr>
<tr>
<td>CPU load</td>
<td>Indicates the average CPU usage over 15 minutes.</td>
</tr>
<tr>
<td>Flash</td>
<td>Indicates the usage and capacity of internal flash memory and any external USB flash drive.</td>
</tr>
<tr>
<td>EX8208 Switches</td>
<td></td>
</tr>
<tr>
<td>Memory util.</td>
<td>Indicates the memory used in the external Routing Engine. In an EX8200 Virtual Chassis, the memory utilization value of the XRE200 External Routing Engine in the master role is displayed. Click the XRE200 External Routing Engine in the backup role to view the memory used in the backup external Routing Engine.</td>
</tr>
<tr>
<td>CPU load</td>
<td>Indicates the average CPU usage over 15 minutes.</td>
</tr>
<tr>
<td>EX8216 Switches</td>
<td></td>
</tr>
<tr>
<td>Memory util.</td>
<td>Indicates the memory used in the external Routing Engine. In an EX8200 Virtual Chassis, the memory utilization value of the XRE200 External Routing Engine in the master role is displayed. Click the XRE200 External Routing Engine in the backup role to view the memory used in the backup external Routing Engine.</td>
</tr>
<tr>
<td>CPU load</td>
<td>Indicates the average CPU usage over 15 minutes.</td>
</tr>
<tr>
<td>Flash</td>
<td>Indicates the usage and capacity of internal flash memory and any external USB flash drive.</td>
</tr>
<tr>
<td>XRE200 External Routing Engines</td>
<td></td>
</tr>
<tr>
<td>Memory util.</td>
<td>Indicates the memory used in the external Routing Engine. In an EX8200 Virtual Chassis, the memory utilization value of the XRE200 External Routing Engine in the master role is displayed. Click the backup XRE200 External Routing Engine to view the memory used in backup external Routing Engine.</td>
</tr>
<tr>
<td>CPU load</td>
<td>Indicates the average CPU usage over 15 minutes.</td>
</tr>
<tr>
<td>Flash</td>
<td>Indicates the usage and capacity of internal flash memory and any external USB flash drive.</td>
</tr>
<tr>
<td>Fan Status</td>
<td>Indicates the status of the fans in the fan tray. The possible values are OK, Failed, and Absent.</td>
</tr>
</tbody>
</table>
Capacity Utilization Panel

Table 116: Capacity Utilization

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of active ports</td>
<td>Indicates the number of active ports in the switch. Configured Virtual Chassis ports (VCPs) are considered as active ports.</td>
</tr>
<tr>
<td>Total number of ports</td>
<td>Indicates the number of ports in the switch.</td>
</tr>
<tr>
<td>Used-up MAC-Table entries</td>
<td>Indicates the number of MAC table entries.</td>
</tr>
<tr>
<td>Supported MAC-Table entries</td>
<td>Indicates the maximum number of MAC table entries permitted.</td>
</tr>
<tr>
<td>Number of VLANs configured</td>
<td>Indicates the number of VLANs configured.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only tagged VLANs are counted.</td>
</tr>
<tr>
<td>Number of VLANs supported</td>
<td>Indicates the maximum number of VLANs supported.</td>
</tr>
</tbody>
</table>

Alarms Panel

Displays information about the last five alarms raised in the system. For example, if there are 5 major alarms, then details of all 5 major alarms are displayed. If there are 4 major alarms and 3 minor alarms, then details of the 4 major alarms and 1 minor alarm are displayed. Major alarms are displayed in red and minor alarms are displayed in yellow.

In an EX8200 Virtual Chassis, the top 5 alarms for the master external Routing Engine are displayed by default. If you select an EX8200 member switch of the Virtual Chassis, the top 5 alarms for that member switch are displayed.

File System Usage

To display the file system storage details of a switch in the backup or linecard role, click the image of that switch.

Chassis Viewer

Click the Rear View button to see the back of the chassis image. Click the Front View button to see the front of the chassis image. In a Virtual Chassis configuration, the Rear View button is disabled if the switch is not selected.

- Table 117 on page 676—Describes the chassis viewer for EX2200 switches.
- Table 118 on page 676—Describes the chassis viewer for EX2200-C switches.
- Table 119 on page 677—Describes the chassis viewer for EX3200, EX3300, and EX4200 switches.
- Table 120 on page 678—Describes the chassis viewer for EX4300 switches.
- Table 121 on page 680—Describes the chassis viewer for EX4500 switches.
- Table 122 on page 681—Describes the chassis viewer for EX4550 switches.
- **Table 123 on page 682**—Describes the chassis viewer for EX6210 switches.
- **Table 124 on page 682**—Describes the chassis viewer for EX8208 switches.
- **Table 125 on page 684**—Describes the chassis viewer for EX8216 switches.
- **Table 126 on page 684**—Describes the chassis viewer for the XRE200 External Routing Engines.

### Table 117: Chassis Viewer for EX2200 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
<tr>
<td>Interface status</td>
<td>In the image, the colors listed below denote the interface status:</td>
</tr>
<tr>
<td></td>
<td>- Green—Interface is up and operational.</td>
</tr>
<tr>
<td></td>
<td>- Yellow—Interface is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>- Gray—Interface is down and nonoperational.</td>
</tr>
<tr>
<td>Mouse over the interface (port) to view more information.</td>
<td></td>
</tr>
<tr>
<td><strong>Rear View</strong></td>
<td></td>
</tr>
<tr>
<td>Management (me0) port</td>
<td>The management port is used to connect the switch to a management device for out-of-band management.</td>
</tr>
<tr>
<td>Console port</td>
<td>The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)</td>
</tr>
<tr>
<td>USB port</td>
<td>Indicates the USB port for the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
<tr>
<td>Fan tray</td>
<td>Mouse over the fan tray icon to display name, status, and description information.</td>
</tr>
<tr>
<td>Power supply</td>
<td>Mouse over the power outlet icon to display name, status, and description information.</td>
</tr>
</tbody>
</table>

### Table 118: Chassis Viewer for EX2200-C Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
<tr>
<td>Interface status</td>
<td>In the image, the colors listed below denote the interface status:</td>
</tr>
<tr>
<td></td>
<td>- Green—Interface is up and operational.</td>
</tr>
<tr>
<td></td>
<td>- Yellow—Interface is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>- Gray—Interface is down and nonoperational.</td>
</tr>
<tr>
<td>Mouse over the interface (port) to view more information.</td>
<td></td>
</tr>
<tr>
<td>Management (me0) port</td>
<td>The management port is used to connect the switch to a management device for out-of-band management.</td>
</tr>
</tbody>
</table>
Table 118: Chassis Viewer for EX2200-C Switches (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console port</td>
<td>The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)</td>
</tr>
<tr>
<td>USB port</td>
<td>Indicates the USB port for the switch. NOTE: We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
</tbody>
</table>

Rear View

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power supply</td>
<td>Mouse over the power outlet icon to display name, status, and description information.</td>
</tr>
</tbody>
</table>

Table 119: Chassis Viewer for EX3200, EX3300, and EX4200 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front View</td>
<td>In the image, the colors listed below denote the interface status:</td>
</tr>
<tr>
<td>Interface status</td>
<td>• Green—Interface is up and operational.&lt;br&gt;• Yellow—Interface is up but is nonoperational.&lt;br&gt;• Gray—Interface is down and nonoperational. Mouse over the interface (port) to view more information. For a Virtual Chassis configuration, select the switch to view the interface status. If an SFP+ uplink module is installed in the switch, mouse over the port icon to display whether the module is configured to operate in 1-gigabit mode or in 10-gigabit mode. If the module is configured to operate in 1-gigabit mode, the tool tip information is displayed for all 4 ports. If the module is configured to operate in 10-gigabit mode, the tool tip information is displayed only for 2 ports. On an EX3300 switch with the 4x GE/XE SFP+ module, mouse over the port icon to display whether the module is configured to operate in 1-gigabit mode or 10-gigabit mode. For SFP, SFP+, and XFP ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays Transceiver not plugged-in when you mouse over the port icon.</td>
</tr>
<tr>
<td>LCD panel</td>
<td>LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.</td>
</tr>
</tbody>
</table>

Rear View of the EX3200 Switch

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management (me0) port</td>
<td>The management port is used to connect the switch to a management device for out-of-band management.</td>
</tr>
<tr>
<td>Console port</td>
<td>The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)</td>
</tr>
</tbody>
</table>
### Table 119: Chassis Viewer for EX3200, EX3300, and EX4200 Switches (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB port</td>
<td>Indicates the USB port for the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
<tr>
<td>Fan tray</td>
<td>Mouse over the fan tray icon to display name, status, and description information.</td>
</tr>
<tr>
<td>Power supply</td>
<td>Mouse over the power supply icon to display name, status, and description information.</td>
</tr>
</tbody>
</table>

#### Rear View of the EX3300 and EX4200 Switch

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan tray</td>
<td>Mouse over the fan tray icon to display name, status, and description information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed.</td>
</tr>
<tr>
<td>Virtual Chassis port</td>
<td>Displayed only when EX4200 switches are configured as a Virtual Chassis. The colors listed below denote the Virtual Chassis port (VCP) status:</td>
</tr>
<tr>
<td></td>
<td>• Green—VCP is up and operational.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—VCP is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>• Gray—VCP is down and nonoperational.</td>
</tr>
<tr>
<td>USB port</td>
<td>Indicates the USB port for the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
<tr>
<td>Management (me0) port</td>
<td>The management port is used to connect the switch to a management device for out-of-band management.</td>
</tr>
<tr>
<td>Console port</td>
<td>The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)</td>
</tr>
<tr>
<td>Power supplies</td>
<td>Mouse over the power supply icons to display name, status, and description information.</td>
</tr>
</tbody>
</table>

### Table 120: Chassis Viewer for EX4300 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front View</td>
<td></td>
</tr>
<tr>
<td>Interface status</td>
<td>In the image, the colors listed below denote the interface status for both copper and fiber media type of ports:</td>
</tr>
<tr>
<td></td>
<td>• Green—Interface is up and operational.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—Interface is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>• Gray—Interface is down and nonoperational.</td>
</tr>
<tr>
<td>LCD panel</td>
<td>LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.</td>
</tr>
</tbody>
</table>
Table 120: Chassis Viewer for EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mini USB console</td>
<td>The mini console port is used to connect the switch to the management console.</td>
</tr>
</tbody>
</table>
| 4x 1G/10G SFP/SFP+ uplink module | If you install a 4-port 1-gigabit or 10-gigabit SFP or SFP+ uplink module in the switch, mouse over the interface (ports) on the module for more information. For SFP or SFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays Transceiver not plugged in when you mouse over the port icon. When an SFP+ port is configured as a Virtual Chassis Port (VCP), the colors listed below denote the interface status:  
  • Green—Interface is up and operational.  
  • Yellow—Interface is up but is nonoperational.  
  • Gray—Interface is down and nonoperational. |

NOTE: In EX4300 switches the LEDs are seen in the front panel, these are not active.

Rear View of the EX4300 Switch

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management port</td>
<td>The management port is used to connect the switch to a management device for out-of-band management.</td>
</tr>
<tr>
<td>Console port</td>
<td>The Console port (RJ-45) is used to connect the switch to a management console or to a console server.</td>
</tr>
<tr>
<td>USB port</td>
<td>Indicates the USB port for the switch.</td>
</tr>
<tr>
<td>Fan tray</td>
<td>Mouse over the fan tray icons to display name, status, and description information.</td>
</tr>
<tr>
<td>Power supplies</td>
<td>Mouse over the power supply icons to display name, status, and description information.</td>
</tr>
</tbody>
</table>
| 4x 40GE QSFP+ module | When you insert an "et" interface (40G fiber type) into the port, in the image, the colors listed below denote the interface status:  
  • Green—Interface is up and operational.  
  • Yellow—Interface is up but is nonoperational.  
  • Gray—Interface is down and nonoperational.  
  For QSFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays Transceiver not plugged in when you mouse over the port icon. When a QSFP+ port (et) is converted to a configured Virtual Chassis Port (VCP), the colors listed below denote the VCP status:  
  • Green—VCP is up and operational.  
  • Yellow—VCP is up but is nonoperational.  
  • Gray—VCP is down and nonoperational. |
## Table 121: Chassis Viewer for EX4500 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
<tr>
<td>Interface status</td>
<td>In the image, the colors listed below denote the interface status:   [20pt]</td>
</tr>
<tr>
<td></td>
<td>• Green—Interface is up and operational.   [10pt]</td>
</tr>
<tr>
<td></td>
<td>• Yellow—Interface is up but is nonoperational.   [10pt]</td>
</tr>
<tr>
<td></td>
<td>• Gray—Interface is down and nonoperational.   [10pt]</td>
</tr>
<tr>
<td></td>
<td>Mouse over the interface (port) to view more information.</td>
</tr>
<tr>
<td></td>
<td>For a Virtual Chassis configuration, select the switch to view the interface status.</td>
</tr>
<tr>
<td></td>
<td>If an SFP+ uplink module is installed in the switch, mouse over the interface (ports) on the module for more information.</td>
</tr>
<tr>
<td></td>
<td>For SFP and SFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays <em>Transceiver not plugged-in</em> when you mouse over the port icon.</td>
</tr>
<tr>
<td>LCD panel</td>
<td>LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.</td>
</tr>
<tr>
<td>Console port</td>
<td>The console port is used to connect the switch to a management console or to a console server.</td>
</tr>
<tr>
<td>Management (me0) port</td>
<td>The management port is used to connect the switch to a management device for out-of-band management. Use this port for initial switch configuration.</td>
</tr>
<tr>
<td>USB port</td>
<td>Indicates the USB port for the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
<tr>
<td><strong>Rear View of the EX4500 Switch</strong></td>
<td></td>
</tr>
<tr>
<td>Fan tray</td>
<td>Mouse over the fan tray icon to display status of the fans and airflow direction information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed.</td>
</tr>
<tr>
<td>Virtual Chassis port</td>
<td>Displayed only when switches are configured as a Virtual Chassis. The colors listed below denote the Virtual Chassis port (VCP) status:   [20pt]</td>
</tr>
<tr>
<td></td>
<td>• Green—VCP is up and operational.   [10pt]</td>
</tr>
<tr>
<td></td>
<td>• Yellow—VCP is up but is nonoperational.   [10pt]</td>
</tr>
<tr>
<td></td>
<td>• Gray—VCP is down and nonoperational.</td>
</tr>
<tr>
<td>Power supplies</td>
<td>Mouse over the power supply icons to display name, status, and description information.</td>
</tr>
<tr>
<td>Intraconnect module</td>
<td>Mouse over the module to display details of the intraconnect module. The intraconnect module helps the switch achieve line rate on all its ports.</td>
</tr>
<tr>
<td>Virtual Chassis module</td>
<td>Mouse over to display details of the switches in the Virtual Chassis configuration.</td>
</tr>
</tbody>
</table>
### Table 122: Chassis Viewer for EX4550 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
<tr>
<td>Interface status</td>
<td>In the image, the colors listed below denote the interface status:</td>
</tr>
<tr>
<td></td>
<td>• Green—Interface is up and operational.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—Interface is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>• Gray—Interface is down and nonoperational.</td>
</tr>
<tr>
<td></td>
<td>Mouse over the interface (port) to view more information.</td>
</tr>
<tr>
<td></td>
<td>For a Virtual Chassis configuration, select the switch to view the interface status.</td>
</tr>
<tr>
<td></td>
<td>If an expansion module or a Virtual Chassis module is installed in the switch, mouse over the interface (ports) on the module for more information.</td>
</tr>
<tr>
<td></td>
<td>On an EX4550-32F switch, for SFP and SFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays <strong>Transceiver (1G/10G) not plugged in</strong> when you mouse over the port icon.</td>
</tr>
<tr>
<td>LCD panel</td>
<td>LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.</td>
</tr>
<tr>
<td>Console port</td>
<td>The console port is used to connect the switch to a management console or to a console server.</td>
</tr>
<tr>
<td>Mini Console port</td>
<td>The mini console port is used to connect the switch to the management console.</td>
</tr>
<tr>
<td>Management (me0) port</td>
<td>The management port is used to connect the switch to a management device for out-of-band management. Use this port for initial switch configuration.</td>
</tr>
<tr>
<td>PIC1 slot</td>
<td>You can insert an uplink module or a Virtual Chassis module in the PIC1 slot. Mouse over to display the details of the module inserted (uplink or Virtual Chassis).</td>
</tr>
<tr>
<td>USB port</td>
<td>Indicates the USB port for the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
<tr>
<td><strong>Rear View of the EX4550 Switch</strong></td>
<td></td>
</tr>
<tr>
<td>Fan tray</td>
<td>Mouse over the fan tray icon to display the status of the fans and airflow direction information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed.</td>
</tr>
<tr>
<td>Virtual Chassis port</td>
<td>Displayed only when switches are configured as a Virtual Chassis. In the image, the colors listed below denote the Virtual Chassis port (VCP) status:</td>
</tr>
<tr>
<td></td>
<td>• Green—VCP is up and operational.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—VCP is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>• Gray—VCP is down and nonoperational.</td>
</tr>
<tr>
<td>Power supplies</td>
<td>Mouse over the power supply icons to display name, status, and description information.</td>
</tr>
<tr>
<td>PIC2 slot</td>
<td>You can insert an uplink module or a Virtual Chassis module into the PIC2 slot. Mouse over to display the details of the module inserted (uplink or Virtual Chassis).</td>
</tr>
</tbody>
</table>
### Table 123: Chassis Viewer for EX6210 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
<tr>
<td>Temperature</td>
<td>Mouse over the temperature icon to display the temperature of the CB or line card.</td>
</tr>
<tr>
<td>Interface status</td>
<td>Select the CB or line card.</td>
</tr>
<tr>
<td></td>
<td>In the image, the colors listed below denote the interface status:</td>
</tr>
<tr>
<td></td>
<td>• Green—Interface is up and operational.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—Interface is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>• Gray—Interface is down and nonoperational.</td>
</tr>
<tr>
<td></td>
<td>Mouse over the interface (port) to view more information.</td>
</tr>
<tr>
<td></td>
<td>You can view status for the following ports on the SRE module:</td>
</tr>
<tr>
<td></td>
<td>• USB port—Indicates the USB port for the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
<tr>
<td></td>
<td>• Management (me0) port—The management port is used to connect the switch to a management device for out-of-band management. There are 2 management ports: fiber and copper. The same status is displayed for both the me0 ports.</td>
</tr>
<tr>
<td></td>
<td>• Console port—The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)</td>
</tr>
<tr>
<td></td>
<td>CBs support 4 SFP+ uplink ports. Mouse over the interface on the CB for more information.</td>
</tr>
<tr>
<td></td>
<td>For SFP and SFP+ ports, the interfaces appear dimmed if no transceiver is inserted. The chassis viewer displays <strong>Transceiver not plugged-in</strong> when you mouse over the port icon.</td>
</tr>
<tr>
<td>Power supplies</td>
<td>Mouse over the power supply icons to display name, status, and description information.</td>
</tr>
<tr>
<td>LCD panel</td>
<td>LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display of the master Routing Engine. The EX6210 switch has 2 LCD panels, one for each Routing Engine. The backup Routing Engine LCD displays <strong>Backup</strong>.</td>
</tr>
<tr>
<td>Rear View of the EX6210 Switch</td>
<td></td>
</tr>
<tr>
<td>Fan tray</td>
<td>Mouse over the fan tray icon to display information regarding the cooling fans.</td>
</tr>
</tbody>
</table>

### Table 124: Chassis Viewer for EX8208 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
</tbody>
</table>
Table 124: Chassis Viewer for EX8208 Switches *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface status</td>
<td>In the image, click any line card, SRE module, or SF module to view the front view of the selected component. In the image, the colors listed below denote the interface status:</td>
</tr>
<tr>
<td></td>
<td>• Green—Interface is up and operational.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—Interface is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>• Gray—Interface is down and nonoperational.</td>
</tr>
<tr>
<td></td>
<td>Mouse over the interface (port) to view more information.</td>
</tr>
<tr>
<td></td>
<td>You can view status for the following ports on the SRE module:</td>
</tr>
<tr>
<td></td>
<td>• USB port—Indicates the USB port for the switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.</td>
</tr>
<tr>
<td></td>
<td>• Auxiliary port—This port is unavailable.</td>
</tr>
<tr>
<td></td>
<td>• Management <em>(me0)</em> port—The management port is used to connect the switch to a management device for out-of-band management.</td>
</tr>
<tr>
<td></td>
<td>• Console port—The console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.)</td>
</tr>
<tr>
<td></td>
<td>Because the SF module has no ports, no status information is displayed.</td>
</tr>
<tr>
<td>Slot numbers</td>
<td>Slots on the switch are labeled, from the top of the switch down:</td>
</tr>
<tr>
<td></td>
<td>• 0–3 (line cards)</td>
</tr>
<tr>
<td></td>
<td>• SRE0, SRE1 (SRE and SF modules)</td>
</tr>
<tr>
<td></td>
<td>• 4–7 (line cards)</td>
</tr>
<tr>
<td>Temperature</td>
<td>The active slots contain a gray temperature icon. Mouse over the icon to display temperature information for the slot.</td>
</tr>
<tr>
<td>Fan status</td>
<td>Mouse over the fan tray icon to display name, status, and description information.</td>
</tr>
<tr>
<td>Power supplies</td>
<td>Mouse over the power supply icons to display name, status, and description information.</td>
</tr>
<tr>
<td>LCD panel</td>
<td>LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.</td>
</tr>
<tr>
<td>Rear View</td>
<td>The EX8208 switch does not have any components on the rear of the chassis.</td>
</tr>
</tbody>
</table>
### Table 125: Chassis Viewer for EX8216 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Interface status    | In the image, click any line card or RE module to display the front view of the selected component. In the image, the colors listed below denote the interface status:  
  - Green—Interface is up and operational.  
  - Yellow—Interface is up but is nonoperational.  
  - Gray—Interface is down and nonoperational.  
  Mouse over the interface (port) to view more information.  
  You can view status for the following ports on the RE module:  
  - USB port—Indicates the USB port for the switch.  
  **NOTE:** We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.  
  - Auxiliary port—This port is unavailable.  
  - Management (me0) port—the management port is used to connect the switch to a management device for out-of-band management.  
  - Console port—the console port is used to connect the switch to a management console or to a console server. (You might do this for initial switch configuration.) |
| Slot numbers        | Slots on the switch are labeled, from the top of the switch down:  
  - RE0 (RE module)  
  - RE1 (RE module)  
  - 0–15 (line cards) |
| Temperature         | The active slots contain a gray temperature icon. Mouse over the icon to display temperature information for the slot. |
| Fan status          | Mouse over the fan tray icon to display consolidated information about the fans.                                                                |
| Power supplies      | Mouse over the power supply icons to display name, status, and description information.                                                         |
| LCD panel           | LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.                                       |
| **Rear View**       |                                                                                                                                               |
| SF modules          | Mouse over the SF module icons in their respective slots to display information. Slots are numbered SF7–SF0, from left to right.       |

### Table 126: Chassis Viewer for XRE200 External Routing Engines

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Front View</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Table 126: Chassis Viewer for XRE200 External Routing Engines (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface status</td>
<td>In the image, the colors listed below denote the interface status:</td>
</tr>
<tr>
<td></td>
<td>• Green—Interface is up and operational.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—Interface is up but is nonoperational.</td>
</tr>
<tr>
<td></td>
<td>• Gray—Interface is down and nonoperational.</td>
</tr>
<tr>
<td></td>
<td>Mouse over the interface (port) to view more information.</td>
</tr>
<tr>
<td></td>
<td>For a Virtual Chassis configuration, select the switch to view the interface status.</td>
</tr>
</tbody>
</table>

| Console port           | The console port is used to connect the switch to a management console or to a console server.                                               |

| Management (me0) port  | The management port is used to connect the switch to a management device for out-of-band management. Use this port for initial switch configuration. |

| Virtual Chassis port   | In the image, the colors listed below denote the Virtual Chassis port (VCP) status:                                                          |
|                        | • Green—VCP is up and operational.                                                                                                           |
|                        | • Yellow—VCP is up but is nonoperational.                                                                                                   |
|                        | • Gray—VCP is down and nonoperational.                                                                                                       |
|                        | Mouse over the interface (port) to view more information.                                                                                   |

| LCD panel              | LCD panel configured for the LEDs on the ports. Mouse over the icon to view the current character display.                                 |

| Temperature            | The active slots contain a gray temperature icon. Mouse over the icon to display temperature information for the slot.                    |

| USB port               | Indicates the USB port for the switch.                                                                                                      |
|                        | **NOTE:** We recommend that you use USB flash drives purchased from Juniper Networks for your EX Series switch.                            |

| PIC1 slot              | You can install a Virtual Chassis module in the PIC1 slot. Mouse over the Virtual Chassis ports to display the port status details.       |

| PIC2 slot              | You can install a Virtual Chassis module in the PIC2 slot. Mouse over the Virtual Chassis ports to display the port status details.       |

| Rear View of the XRE200 |                                                                                                                                       |
| External Routing Engine |                                                                                                                                       |
| Fan modules            | Mouse over the fan modules to display status of the fans and airflow direction information. For a Virtual Chassis, the status of the fans of the selected member switch is displayed. |

| Power supplies         | Mouse over the power supply icons to display name, status, and description information.                                                |

### Related Documentation
- J-Web User Interface for EX Series Switches Overview on page 389
- EX2200 Switches Hardware Overview
- EX3200 Switches Hardware Overview
This topic describes the hardware terms used in EX4300 switch documentation and the corresponding terms used in the Junos OS command-line interface (CLI). See Table 127 on page 686.

### Table 127: CLI Equivalents of Terms Used in the Documentation for EX4300 Switches

<table>
<thead>
<tr>
<th>Hardware Item (CLI)</th>
<th>Description (CLI)</th>
<th>Value (CLI)</th>
<th>Item in Documentation</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>One of the following:</td>
<td>--</td>
<td>Switch chassis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-24T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-24P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-48T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-48P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routing Engine (n)</td>
<td>One of the following:</td>
<td>(n) is a value in the range 0 through 9.</td>
<td>Routing Engine</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-24T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-24P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-48T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-48P</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 127: CLI Equivalents of Terms Used in the Documentation for EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Hardware Item (CLI)</th>
<th>Description (CLI)</th>
<th>Value (CLI)</th>
<th>Item In Documentation</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FPC (n)</strong></td>
<td>Abbreviated name of the Flexible PIC Concentrator (FPC)</td>
<td><em>n</em> is a value in the range 0 through 9.</td>
<td></td>
<td>&quot;Understanding Interface Naming Conventions on EX Series Switches&quot; on page 2270</td>
</tr>
<tr>
<td></td>
<td>One of the following:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-24T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-24P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-48T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EX4300-48P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>On a standalone switch, the default value is 0.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>On a Virtual Chassis configuration, the values correspond to the assigned member IDs of switches in the Virtual Chassis.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this case, FPC refers to the switch itself.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In this case, the FPC number refers to the member ID assigned to the switch.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PIC (n)</strong></td>
<td>Abbreviated name of the Physical Interface Card (PIC)</td>
<td><em>n</em> is a value in the range 0 through 2.</td>
<td></td>
<td>&quot;Understanding Interface Naming Conventions on EX Series Switches&quot; on page 2270</td>
</tr>
<tr>
<td></td>
<td>One of the following:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 24x 10/100/1000 BASE-T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 48x 10/100/1000 BASE-T</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EX4300 Switches Hardware Overview</td>
<td></td>
</tr>
<tr>
<td><strong>4x 40GE</strong></td>
<td>PIC 0</td>
<td>Built-in network ports on the switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4x 1G/10G SFP/SFP+</strong></td>
<td>PIC 1</td>
<td>Built-in QSFP+ ports on the switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Xcvr (n)</strong></td>
<td>Abbreviated name of the transceiver</td>
<td><em>n</em> is a value equivalent to the number of the port in which the transceiver is installed.</td>
<td></td>
<td>Optical transceivers</td>
</tr>
<tr>
<td><strong>Power supply (n)</strong></td>
<td>One of the following:</td>
<td></td>
<td></td>
<td>Pluggable Transceivers Supported on EX4300 Switches</td>
</tr>
<tr>
<td></td>
<td>• JPSU-350-AC-AFO-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• JPSU-350-AC-AFI-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• JPSU-715-AC-AFO-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• JPSU-1100-AC-AFO-A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>n</em> has a value 0 or 1, corresponding to the power supply slot number.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CAUTION:</strong> Do not mix:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AC and DC power supplies in the same chassis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Power supplies with different airflow labels (AIR IN (AFI)) and AIR OUT</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 127: CLI Equivalents of Terms Used in the Documentation for EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Hardware Item (CLI)</th>
<th>Description (CLI)</th>
<th>Value (CLI)</th>
<th>Item in Documentation</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(AFO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JPSU-550-DC-AFO-A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JPSU-550-DC-AFI-A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Fan tray**: One of the following:
  - Fan Module, Airflow In (AFI)
  - Fan Module, Airflow Out (AFO)

  * $n$ has a value 0 or 1, corresponding to the fan module slot number.

  **CAUTION**: Do not mix fan modules with different airflow labels (AIR IN (AFI) and AIR OUT (AFO)) in the same chassis.

- **Fan module**: *Cooling System and Airflow in an EX4300 Switch*

---

**Related Documentation**

- *EX4300 Switches Hardware Overview*
CHAPTER 23

Configuration

• Configuration Statements on page 689

Configuration Statements

facility-override

Syntax

facility-override facility;

Hierarchy Level

[edit system syslog host]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Substitute an alternate facility for the default facilities used when messages are directed to a remote destination.

Options

facility—Alternate facility to substitute for the default facilities. For a list of the possible facilities, see Junos OS System Log Alternate Facilities for Remote Logging.

Required Privilege

Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Changing the Alternative Facility Name for Remote System Log Messages
• Junos OS System Log Messages Reference
file (System Logging)

Syntax

```
file filename {
    facility severity;
    archive {
        files number;
        size size;
        (no-world-readable | world-readable);
    }
    explicit-priority;
    match "regular-expression";
    structured-data {
        brief;
    }
}
```

Hierarchy Level
[edit system syslog]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure the logging of system messages to a file.

Options
- **facility**—Class of messages to log. To specify multiple classes, include multiple `facility severity` statements. For a list of the facilities, see Junos OS System Logging Facilities and Message Severity Levels.
- **file filename**—File in the severity directory in which to log messages from the specified facility. To log messages to more than one file, include more than one `file` statement.
- **severity**—Severity of the messages that belong to the facility specified by the paired `facility` name. Messages with severities of the specified level and higher are logged. For a list of the severities, see Junos OS System Logging Facilities and Message Severity Levels.

The remaining statements are explained separately.

Required Privilege Level
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation
- Directing System Log Messages to a Log File
- Junos OS System Log Messages Reference
files

**Syntax**

```
files number;
```

**Hierarchy Level**

- [edit system syslog archive].
- [edit system syslog file filename archive]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for EX Series switches.

**Description**

Configure the maximum number of archived log files to retain. When the Junos OS logging utility has written a defined maximum amount of data to a log file `logfile`, it closes the file, compresses it, and renames it to `logfile.0.gz` (for information about the maximum file size, see `size`). The utility then opens and writes to a new file called `logfile`. When the new file reaches the maximum size, the `logfile.0.gz` file is renamed to `logfile.1.gz`, and the new file is closed, compressed, and renamed `logfile.0.gz`. By default, the logging facility creates up to ten archive files in this manner. Once the maximum number of archive files exists, each time the active log file reaches the maximum size, the contents of the oldest archive file are lost (overwritten by the next oldest file).

**Options**

- **number**—Maximum number of archived files.
  - **Range:** 1 through 1000
  - **Default:** 10 files

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Specifying Log File Size, Number, and Archiving Properties
- Junos OS System Log Messages Reference
- `size` on page 696
**host (System)**

**Syntax**

```plaintext
host (hostname | other-routing-engine) {
    facility severity;
    exclude-hostname
    explicit-priority;
    facility-overrides facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
        brief;
    }
}
```

**QFX Series**

```plaintext
host (hostname {
    facility severity;
    explicit-priority;
    facility-overrides facility;
    log-prefix string;
    match "regular-expression";
    port;
    source-address source-address;
}
```

**TX Matrix Router and EX Series Switches**

```plaintext
host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-overrides facility;
    log-prefix string;
    match "regular-expression";
    port;
    source-address source-address;
}
```

**TX Matrix Plus Router**

```plaintext
host (hostname | other-routing-engine | sfc0-master) {
    facility severity;
    allow-duplicates;
    explicit-priority;
    facility-overrides facility;
    log-prefix string;
    match "regular-expression";
    port;
    source-address source-address;
}
```

**Hierarchy Level**

[edit logical-systems logical-system-name system syslog],
[edit system syslog]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Configure the logging of system messages to a remote destination.
Options

**facility**—Class of messages to log. To specify multiple classes, include multiple **facility severity** statements. For a list of the facilities, see *Junos OS System Logging Facilities and Message Severity Levels*.

**hostname**—IPv4 address, IPv6 address, or fully qualified hostname of the remote machine to which to direct messages. To direct messages to multiple remote machines, include a **host** statement for each one.

**other-routing-engine**—Direct messages to the other Routing Engine on a router or switch with two Routing Engines installed and operational.

---

**NOTE:** The **other-routing-engine** option is not applicable to the QFX Series.

**port**—Port number of the remote syslog server that can be modified.

**scc-master**—(TX Matrix routers only) On a T640 router that is part of a routing matrix, direct messages to the TX Matrix router.

**severity**—Severity of the messages that belong to the facility specified by the paired **facility** name. Messages with severities of the specified level and higher are logged. For a list of the severities, see *Junos OS System Logging Facilities and Message Severity Levels*.

**sfc0-master**—(TX Matrix Plus routers only) On a T1600 or T4000 router that is part of a routing matrix, direct messages to the TX Matrix Plus router.

The remaining statements are explained separately.

**Related Documentation**

- Directing System Log Messages to a Remote Machine or the Other Routing Engine
- Directing Messages to a Remote Destination from the Routing Matrix Based on the TX Matrix Router
- Directing Messages to a Remote Destination from the Routing Matrix Based on a TX Matrix Plus Router
- Junos OS System Log Messages Reference

**Required Privilege**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
**interface (Accounting or Sampling)**

**Syntax**

```plaintext
interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
}
```

**Hierarchy Level**

- [edit forwarding-options accounting group-name output],
- [edit forwarding-options sampling family family-name output]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Specify the output interface for sending copies of packets elsewhere to be analyzed.

**Options**

- `engine-id number` — Identity of the accounting interface.
- `engine-type number` — Type of this accounting interface.
- `interface-name` — Name of the accounting interface.
- `source-address address` — Address used for generating packets.

**Related Documentation**

- [Configuring Discard Accounting](#)
- [Configuring the Output File for Traffic Sampling](#)

**log-prefix (System)**

**Syntax**

```plaintext
log-prefix string;
```

**Hierarchy Level**

- [edit system syslog host]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Include a text string in each message directed to a remote destination.

**Options**

- `string` — Text string to include in each message.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- [Adding a Text String to System Log Messages](#)
- [Junos OS System Log Messages Reference](#)
### match

**Syntax**

match "regular-expression";

**Hierarchy Level**

- [edit logical-systems logical-system-name system syslog file filename],
- [edit logical-systems logical-system-name system syslog user (username | *)],
- [edit system syslog file filename],
- [edit system syslog host hostname | other-routing-engine| scc-master]),
- [edit system syslog user (username | *)]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Specify a text string that must (or must not) appear in a message for the message to be logged to a destination.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Using Regular Expressions to Refine the Set of Logged Messages
size (System)

Syntax  
size size;

Hierarchy Level  
[edit system syslog archive],  
[edit system syslog file filename archive]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Configure the maximum amount of data that the Junos OS logging utility writes to a log file logfile before archiving it (closing it, compressing it, and changing its name to logfile.0.gz). The utility then opens and writes to a new file called logfile. For information about the number of archive files that the utility creates in this way, see files.

Options  
size—Maximum size of each system log file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

Syntax:  xk to specify the number of kilobytes, xm for the number of megabytes, or xg for the number of gigabytes

Range:  64 KB through 1 GB

Default:  1 MB for MX Series routers and the QFX Series

Required Privilege Level  
system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation  
• Specifying Log File Size, Number, and Archiving Properties
• Junos OS System Log Messages Reference
• files on page 691
structured-data

Syntax

structured-data {
  brief;
}

Hierarchy Level

[edit logical-systems logical-system-name system syslog file filename],
[edit system syslog file filename]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Write system log messages to the log file in structured-data format, which complies with
Internet draft draft-ietf-syslog-protocol-23, The syslog Protocol

NOTE: When this statement is included, other statements that specify the
format for messages written to the file are ignored (the explicit-priority
statement at the [edit system syslog file filename] hierarchy level and the
time-format statement at the [edit system syslog] hierarchy level).

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Logging Messages in Structured-Data Format
• Junos OS System Log Messages Reference
• explicit-priority
• time-format on page 700
syslog (System)

Syntax

```plaintext
syslog {
  archive {
    (binary-data|no-binary-data);
    files number;
    size maximum-file-size;
    start-time "YYYY-MM-DD:hh:mm";
    transfer-interval minutes;
    (world-readable | no-world-readable);
  }
  console {
    facility severity;
  }
  file filename {
    facility severity;
    explicit-priority;
    match "regular-expression";
    archive {
      (binary-data|no-binary-data);
      files number;
      size maximum-file-size;
      start-time "YYYY-MM-DD:hh:mm";
      transfer-interval minutes;
      (world-readable | no-world-readable);
    }
    structured-data {
      brief;
    }
  }
  host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
    source-address source-address;
    structured-data {
      brief;
    }
    port portnumber;
  }
  log-rotate-frequency frequency;
  server servername;
  source-address source-address;
  time-format (millisecond | year | year-millisecond);
  user (username | *) {
    facility severity;
    match "regular-expression";
  }
}
```

Hierarchy Level
[edit logical-systems logical-system-name system],
[edit system]
Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Support at the [edit logical-systems logical-system-name system] hierarchy level introduced in Junos OS Release 11.4.

Description

Configure the types of system log messages to send to files, to a remote destination, to user terminals, or to the system console.

The remaining statements are explained separately.

Options

archive—Define parameters for archiving log messages.
console—Send log messages of a specified class and severity to the console.
file—Send log messages to a named file.
host—Remote location to be notified of specific log messages.
log-rotate-frequency—Configure the interval for checking logfile size and archiving messages.
server—Name of the system log server in the inet.0 routing instance.
source-address—Include a specified address as the source address for log messages.
time-format—Additional information to include in the system log time stamp.
user—Notify a specific user of the log event.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Junos OS System Log Configuration Overview
- Junos OS System Log Messages Reference
- Overview of Single-Chassis System Logging Configuration
### time-format

**Syntax**

time-format (year | millisecond | year millisecond);

**Hierarchy Level**

[edit system syslog]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Include the year, the millisecond, or both, in the timestamp on every standard-format system log message. The additional information is included for messages directed to each destination configured by a `file`, `console`, or `user` statement at the [edit system syslog] hierarchy level. As of Junos OS Release 11.4, the additional time information is also sent to destinations configured by a `host` statement.

By default, the timestamp specifies the month, date, hour, minute, and second when the message was logged—for example, `Aug 21 12:36:30`. However, the timestamp for `traceoption` messages is specified in milliseconds by default, and is independent of the [edit system syslog time-format] statement.

---

**NOTE:** When the `structured-data` statement is included at the [edit system syslog file `filename`] hierarchy level, this statement is ignored for the file.

**Options**

- `millisecond`—Include the millisecond in the timestamp.
- `year`—Include the year in the timestamp.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Including the Year or Millisecond in Timestamps
- Junos OS System Log Messages Reference
- structured-data on page 697
time-zone

**Syntax**

time-zone (GMT hour-offset | time-zone);

**Hierarchy Level**

[edit system]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**GMT hour-offset** option added in Junos OS Release 7.4.

**Description**

Set the local time zone. To have the time zone change take effect for all processes running on the router or switch, you must reboot the router or switch.

**Default**

UTC

**Options**

**GMT hour-offset**—Set the time zone relative to UTC time.

**Range:** –14 through +12

**Default:** 0

**time-zone**—Specify the time zone as UTC, which is the default time zone, or as a string such as PDT (Pacific Daylight Time), or use one of the following continents and major cities:

- America/Adak, America/Anchorage, America/Argentina, America/Anguilla, America/Antigua, America/Aruba, America/Asuncion, America/Barbados, America/Belize, America/Bogota, America/Boise, America/Buenos_Aires, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Cordoba, America/Costa_Rica, America/Cuaba, America/Curacao, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/El_Salvador, America/Ensenada, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Peru, America/Indiana/Vevay, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Mexico_City, America/Miquelon, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince,
America/Port_of_Spain, America/Porto_Acre, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Regina, America/Rosario, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Tortola, America/Vancouver, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife
Antarctica/Casey, Antarctica/DumontDUrville, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/South_Pole
Arctic/Longyearbyen
Asia/Aden, Asia/Alma-Ata, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Asmakhbad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hong_Kong, Asia/irkutsk, Asia/Ishigaki, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Katmandu, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Magadan, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novosibirsk, Asia/Omsk, Asia/Phnom_Penh, Asia/Pyongyang, Asia/Qatar, Asia/Rangoon, Asia/Riyadh, Asia/Quang, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Thimbu, Asia/Tojo, Asia/Ujing_Pandang, Asia/Ulan_Bator, Asia/Urumqi, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan
Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Darwin, Australia/Hobart, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/Perth, Australia/Sydney
Indian/Andamanarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion

Required Privilege
Level
system—to view this statement in the configuration.

system-control—to add this statement to the configuration.
user (System Logging)

Syntax

```
user (username | *) {
    facility severity;
    match "regular-expression";
}
```

Hierarchy Level
[edit system syslog]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure the logging of system messages to user terminals.

Options
* (the asterisk)—Log messages to the terminal sessions of all users who are currently logged in.

- **facility**—Class of messages to log. To specify multiple classes, include multiple `facility severity` statements. For a list of the facilities, see Junos OS System Logging Facilities and Message Severity Levels.

- **severity**—Severity of the messages that belong to the facility specified by the paired `facility` name. Messages with severities the specified level and higher are logged. For a list of the severities, see Junos OS System Logging Facilities and Message Severity Levels.

- **username**—Junos OS login name of the user whose terminal session is to receive system log messages. To log messages to more than one user’s terminal session, include more than one `user` statement.

The remaining statement is explained separately.

Required Privilege
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation
- Directing System Log Messages to a User Terminal
- Junos OS System Logging Facilities and Message Severity Levels
- Junos OS System Log Messages Reference
world-readable (System)

Syntax  world-readable | no-world-readable;

Hierarchy Level  [edit system syslog archive],
                 [edit system syslog file filename archive]

Release Information  Statement introduced before OS Release 7.4.
                     Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Grant all users permission to read log files, or restrict the permission only to the root user
              and users who have the Junos maintenance permission.

Default  no-world-readable

Required Privilege Level  system—To view this statement in the configuration.
                          system-control—To add this statement to the configuration.

Related Documentation  • Specifying Log File Size, Number, and Archiving Properties
                       • Junos System Log Messages Reference
CHAPTER 24

Administration

• Routine Monitoring on page 705
• Operational Commands on page 721

Routine Monitoring

• Monitoring System Log Messages on page 705
• Checking Active Alarms with the J-Web Interface on page 708
• Monitoring Chassis Alarms for an EX8200 Switch on page 709
• Monitoring Switch Control Traffic on page 712
• Monitoring System Properties on page 714
• Monitoring Chassis Information on page 716
• Monitoring System Process Information on page 718
• Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure) on page 719

Monitoring System Log Messages

Purpose Use the monitoring functionality to filter and view system log messages for EX Series switches.

Action To view events in the J-Web interface, select Monitor > Events and Alarms > View Events. Apply a filter or a combination of filters to view messages. You can use filters to display relevant events. Table 128 on page 706 describes the different filters, their functions, and the associated actions.

To view events in the CLI, enter the following command:

show log
### Table 128: Filtering System Log Messages

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Log File</strong></td>
<td>Specifies the name of a system log file for which you want to display the recorded events.</td>
<td>To specify events recorded in a particular file, select the system log filename from the list—for example, messages. Select <strong>include archived files</strong> to include archived files in the search.</td>
</tr>
<tr>
<td></td>
<td>Lists the names of all the system log files that you configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default, a log file, messages, is included in the /var/log/ directory.</td>
<td></td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td>Specifies the name of the process generating the events you want to display.</td>
<td>To specify events generated by a process, type the name of the process. For example, type <strong>mgd</strong> to list all messages generated by the management process.</td>
</tr>
<tr>
<td></td>
<td>To view all the processes running on your system, enter the CLI command <strong>show system processes</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about processes, see the Junos OS Installation and Upgrade Guide.</td>
<td></td>
</tr>
<tr>
<td><strong>Date From</strong></td>
<td>Specifies the time period in which the events you want displayed are generated.</td>
<td>To specify the time period:</td>
</tr>
<tr>
<td><strong>To</strong></td>
<td>Displays a calendar that allows you to select the year, month, day, and time. It also allows you to select the local time.</td>
<td>• Click the Calendar icon and select the year, month, and date—for example, 02/10/2007.</td>
</tr>
<tr>
<td></td>
<td>By default, the messages generated in the last hour are displayed. End Time shows the current time and Start Time shows the time one hour before End Time.</td>
<td>• Click the Calendar icon and select the year, month, and date—for example, 02/10/2007.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click to select the time in hours, minutes, and seconds.</td>
</tr>
<tr>
<td><strong>Event ID</strong></td>
<td>Specifies the event ID for which you want to display the messages.</td>
<td>To specify events with a specific ID, type the partial or complete ID—for example, TFTP_D_AF_ERR.</td>
</tr>
<tr>
<td></td>
<td>Allows you to type part of the ID and completes the remainder automatically.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An event ID, also known as a system log message code, uniquely identifies a system log message. It begins with a prefix that indicates the generating software process or library.</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Specifies text from the description of events that you want to display.</td>
<td>To specify events with a specific description, type a text string from the description with regular expression. For example, type ^Initial+ to display all messages with lines beginning with the term Initial.</td>
</tr>
<tr>
<td></td>
<td>Allows you to use regular expressions to match text from the event description.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Regular expression matching is case-sensitive.</td>
<td></td>
</tr>
<tr>
<td><strong>Search</strong></td>
<td>Applies the specified filter and displays the matching messages.</td>
<td>To apply the filter and display messages, click Search.</td>
</tr>
</tbody>
</table>

**Meaning:** Table 129 on page 707 describes the Event Summary fields.
NOTE: By default, the View Events page in the J-Web interface displays the most recent 25 events, with severity levels highlighted in different colors. After you specify the filters, Event Summary displays the events matching the specified filters. Click the First, Next, Prev, and Last links to navigate through messages.

Table 129: Viewing System Log Messages

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Displays the name and ID of the process that generated the system log message.</td>
<td>The information displayed in this field is different for messages generated on the local Routing Engine than for messages generated on another Routing Engine (on a system with two Routing Engines installed and operational). Messages from the other Routing Engine also include the identifiers re0 and re1 to identify the Routing Engine.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity level of a message is indicated by different colors.</td>
<td>A severity level indicates how seriously the triggering event affects switch functions. When you configure a location for logging a facility, you also specify a severity level for the facility. Only messages from the facility that are rated at that level or higher are logged to the specified file.</td>
</tr>
<tr>
<td></td>
<td>• Unknown—Gray—Indicates no severity level is specified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Debug/Info/Notice—Green—Indicates conditions that are not errors but are of interest or might warrant special handling.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Warning—Yellow—Indicates conditions that warrant monitoring.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Error—Blue—Indicates standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Critical—Pink—Indicates critical conditions, such as hard-drive errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Alert—Orange—Indicates conditions that require immediate correction, such as a corrupted system database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Emergency—Red—Indicates system panic or other conditions that cause the switch to stop functioning.</td>
<td></td>
</tr>
<tr>
<td>Event ID</td>
<td>Displays a code that uniquely identifies the message.</td>
<td>The event ID begins with a prefix that indicates the generating software process. Some processes on a switch do not use codes. This field might be blank in a message generated from such a process. An event can belong to one of the following type categories:</td>
</tr>
<tr>
<td></td>
<td>The prefix on each code identifies the message source, and the rest of the code indicates the specific event or error.</td>
<td>• Error—Indicates an error or failure condition that might require corrective action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Event—Indicates a condition or occurrence that does not generally require corrective action.</td>
</tr>
</tbody>
</table>
Table 129: Viewing System Log Messages (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Description</td>
<td>Displays a more detailed explanation of the message.</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Displays the time at which the message was logged.</td>
<td></td>
</tr>
</tbody>
</table>

Related Documentation
- Checking Active Alarms with the J-Web Interface on page 708
- Understanding Alarm Types and Severity Levels on EX Series Switches on page 669

Checking Active Alarms with the J-Web Interface

**Purpose**
Use the monitoring functionality to view alarm information for the EX Series switches including alarm type, alarm severity, and a brief description for each active alarm on the switching platform.

**Action**
To view the active alarms:

1. Select **Monitor > Events and Alarms > View Alarms** in the J-Web interface.
2. Select an alarm filter based on alarm type, severity, description, and date range.
3. Click **Go**.

   All the alarms matching the filter are displayed.

**NOTE:** When the switch is reset, the active alarms are displayed.

**Meaning**
Table 130 on page 708 lists the alarm output fields.

Table 130: Summary of Key Alarm Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Category of the alarm:</td>
</tr>
<tr>
<td></td>
<td>• Chassis—Indicates an alarm condition on the chassis (typically an environmental alarm such as one related to temperature).</td>
</tr>
<tr>
<td></td>
<td>• System—Indicates an alarm condition in the system.</td>
</tr>
<tr>
<td>Severity</td>
<td>Alarm severity—either major (red) or minor (yellow).</td>
</tr>
<tr>
<td>Description</td>
<td>Brief synopsis of the alarm.</td>
</tr>
<tr>
<td>Time</td>
<td>Date and time when the failure was detected.</td>
</tr>
</tbody>
</table>
Monitoring Chassis Alarms for an EX8200 Switch

Purpose

This document provides information on chassis alarm conditions, and how you should respond when a certain chassis alarm is seen on your switch.

Various conditions related to the chassis components trigger yellow and red alarms. You cannot configure these conditions. See “Understanding Alarm Types and Severity Levels on EX Series Switches” on page 669.

Action

You can monitor chassis alarms by watching the ALM chassis status LED and using the LCD panel to gather information about the alarm. See Chassis Status LEDs in an EX8200 Switch and LCD Panel in an EX8200 Switch.

To display switch chassis alarms in the CLI, use the following command

```
user@host> show chassis alarms
```

The command output displays the number of alarms currently active, the time when the alarm began, the severity level, and an alarm description. Note the date and time of an alarm so that you can correlate it with error messages in the messages system log file.

You can also monitor chassis alarms using the J-Web interface. See “Checking Active Alarms with the J-Web Interface” on page 708.

Table 131 on page 709 lists some of the chassis alarms that an EX8200 switch can generate.

Table 131: Chassis Alarms for EX8200 Switches

<table>
<thead>
<tr>
<th>Component</th>
<th>Alarm Condition</th>
<th>Remedy</th>
<th>Severity</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan tray</td>
<td>The fan tray has been removed from the chassis.</td>
<td>Install the fan tray.</td>
<td>Yellow/Red</td>
<td>The switch will eventually get too hot to operate if a fan tray is removed. Temperature alarms will follow.</td>
</tr>
<tr>
<td>Fan tray</td>
<td>One or more fans in a fan tray is spinning below the required speed.</td>
<td>Replace the fan tray.</td>
<td>Red</td>
<td>Individual fans cannot be replaced; you must replace the fan tray.</td>
</tr>
</tbody>
</table>
### Table 131: Chassis Alarms for EX8200 Switches (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Alarm Condition</th>
<th>Remedy</th>
<th>Severity</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan tray</td>
<td>The fan tray’s internal connection to the switch is not functioning properly.</td>
<td>Remove and reinsert the fan tray.</td>
<td>Red</td>
<td>The switch will eventually get too hot to operate if a fan tray is not operating.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If removing and reinserting the fan tray does not resolve the problem, reboot the switch.</td>
<td></td>
<td>Temperature alarms will follow.</td>
</tr>
<tr>
<td>Power supply</td>
<td>A power supply slot that contained a power supply at bootup is now empty.</td>
<td>Install a power supply in the empty power supply slot.</td>
<td>Yellow</td>
<td>You can ignore this alarm in cases in which a power supply slot can remain empty.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>You will not see this alarm if the switch is booted with an empty power supply slot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This alarm is expected during power supply removal and installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This alarm can be triggered by a line card insertion. The alarm condition corrects itself when seen for this reason.</td>
</tr>
<tr>
<td>Power supply</td>
<td>A power supply has failed due to an input or output failure, or due to temperature issues.</td>
<td>Replace the failed power supply.</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>Power supply</td>
<td>A power supply’s internal connection to the switch is not operating properly.</td>
<td>Remove and reinsert the power supply.</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If removing and reinserting the power supply does not resolve the problem, reboot the switch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature</td>
<td>The chassis warm temperature threshold has been exceeded and fan speeds have increased.</td>
<td>Adjust room temperature downward, if possible.</td>
<td>Yellow</td>
<td>The chassis is warm and should be cooled down. The switch is still functioning normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ensure airflow through the switch is unobstructed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To monitor temperature:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><code>user@switch&gt; show chassis environment</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To monitor temperature thresholds:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><code>user@switch&gt; show chassis temperature-thresholds</code></td>
</tr>
</tbody>
</table>
### Table 131: Chassis Alarms for EX8200 Switches (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Alarm Condition</th>
<th>Remedy</th>
<th>Severity</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>The chassis high temperature threshold has been exceeded and the fans are not operating properly. The operating fans are running at full speed.</td>
<td>Adjust room temperature downward, if possible. Ensure airflow through the switch is unobstructed.</td>
<td>Red</td>
<td>The chassis is hot and should be cooled down. The switch might still function normally but is close to shutting down if it hasn’t already.</td>
</tr>
<tr>
<td>Temperature</td>
<td>The chassis warm temperature threshold has been exceeded, and one or more fans are not operating properly. The operating fans are running at full speed.</td>
<td>Replace the fan tray that has the faulty fan or fans. Adjust room temperature downward, if possible. Ensure airflow through the switch is unobstructed.</td>
<td>Yellow</td>
<td>The chassis is warm and should be cooled down. The switch is still functioning normally.</td>
</tr>
<tr>
<td>Temperature</td>
<td>The chassis high temperature threshold has been exceeded, and one or more fans is not operating properly. The operating fans are running at full speed.</td>
<td>Replace the fan tray that has the faulty fan or fans. Adjust room temperature downward, if possible. Ensure airflow through the switch is unobstructed.</td>
<td>Red</td>
<td>The chassis is hot and should be cooled down. The switch might still function normally but is close to shutting down if it hasn’t already.</td>
</tr>
<tr>
<td>Temperature</td>
<td>The temperature sensor on a hardware component has failed.</td>
<td>Replace the hardware component.</td>
<td>Yellow</td>
<td>The RE, SRE, or SF module has failed. The RE, SRE, or SF module must be replaced.</td>
</tr>
<tr>
<td>Routing Engine (RE), Switch Fabric and Routing Engine (SRE), or Switch Fabric (SF) module</td>
<td>The RE, SRE, or SF module has failed.</td>
<td>The RE, SRE, or SF module must be replaced.</td>
<td>Red</td>
<td></td>
</tr>
</tbody>
</table>
Table 131: Chassis Alarms for EX8200 Switches (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Alarm Condition</th>
<th>Remedy</th>
<th>Severity</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Status</td>
<td>The link to the network is down.</td>
<td>Check network connectivity.</td>
<td>Red or Yellow</td>
<td>The network link is disabled by default, so you might see this alarm before you connect the switch to the network.</td>
</tr>
</tbody>
</table>

Related Documentation
- Checking Active Alarms with the J-Web Interface on page 708
- Chassis Status LEDs in an EX8200 Switch

Monitoring Switch Control Traffic

Purpose
Use the packet capture feature when you need to quickly capture and analyze switch control traffic on a switch. The packet capture feature allows you to capture traffic destined for or originating from the Routing Engine.

Action
To use the packet capture feature in the J-Web interface, select **Troubleshoot > Packet Capture**.

To use the packet capture feature in the CLI, enter the following CLI command:

```
monitor traffic
```

Meaning
You can use the packet capture feature to compose expressions with various matching criteria to specify the packets that you want to capture. You can decode and view the captured packets in the J-Web interface as they are captured. The packet capture feature does not capture transient traffic.

Table 132: Packet Capture Field Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Specifies the interface on which the packets are captured. If you select default, packets on the Ethernet management port 0, are captured.</td>
<td>From the list, select an interface—for example, ge-0/0/0.</td>
</tr>
<tr>
<td>Detail level</td>
<td>Specifies the extent of details to be displayed for the packet headers.</td>
<td>From the list, select <strong>Detail</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Brief—Displays the minimum packet header information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• This is the default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Detail—Displays packet header information in moderate detail.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Extensive—Displays the maximum packet header information.</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>Specifies the number of packets to be captured. Values range from 1 to 1000. Default is 10. Packet capture stops capturing packets after this number is reached.</td>
<td>From the list, select the number of packets to be captured—for example, 10.</td>
</tr>
</tbody>
</table>
### Table 132: Packet Capture Field Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Addresses</td>
<td>Specifies the addresses to be matched for capturing the packets using a combination of the following parameters:</td>
<td>Select address-matching criteria. For example:</td>
</tr>
<tr>
<td></td>
<td>• Direction—Matches the packet headers for IP address, hostname, or network address of the source, destination or both.</td>
<td>1. From the Direction list, select <code>source</code>.</td>
</tr>
<tr>
<td></td>
<td>• Type—Specifies if packet headers are matched for host address or network address.</td>
<td>2. From the Type list, select <code>host</code>.</td>
</tr>
<tr>
<td></td>
<td>You can add multiple entries to refine the match criteria for addresses.</td>
<td>3. In the Address box, type <code>10.1.40.48</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <code>Add</code>.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Matches the protocol for which packets are captured. You can choose to capture TCP, UDP, or ICMP packets or a combination of TCP, UDP, and ICMP packets.</td>
<td>From the list, select a protocol—for example, <code>tcp</code>.</td>
</tr>
<tr>
<td>Ports</td>
<td>Matches packet headers containing the specified source or destination TCP or UDP port number or port name.</td>
<td>Select a direction and a port. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• From the Type list, select <code>src</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the Port box, type <code>23</code>.</td>
</tr>
</tbody>
</table>

#### Advanced Options

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute TCP Sequence</td>
<td>Specifies that absolute TCP sequence numbers are to be displayed for the packet headers.</td>
<td>To display absolute TCP sequence numbers in the packet headers, select this check box.</td>
</tr>
<tr>
<td>Layer 2 Headers</td>
<td>Specifies that link-layer packet headers are to be displayed.</td>
<td>To include link-layer packet headers while capturing packets, select this check box.</td>
</tr>
<tr>
<td>Non-Promiscuous</td>
<td>Specifies not to place the interface in promiscuous mode, so that the interface reads only packets addressed to it. In promiscuous mode, the interface reads every packet that reaches it.</td>
<td>To read all packets that reach the interface, select this check box.</td>
</tr>
<tr>
<td>Display Hex</td>
<td>Specifies that packet headers, except link-layer headers, are to be displayed in hexadecimal format.</td>
<td>To display the packet headers in hexadecimal format, select this check box.</td>
</tr>
<tr>
<td>Display ASCII and Hex</td>
<td>Specifies that packet headers are to be displayed in hexadecimal and ASCII format.</td>
<td>To display the packet headers in ASCII and hexadecimal formats, select this check box.</td>
</tr>
<tr>
<td>Header Expression</td>
<td>Specifies the match condition for the packets to be captured. The match conditions you specify for Addresses, Protocols, and Ports are displayed in expression format in this field.</td>
<td>You can enter match conditions directly in this field in expression format or modify the expression composed from the match conditions you specified for Addresses, Protocols, and Ports. If you change the match conditions specified for Addresses, Protocols, and Ports again, packet capture overwrites your changes with the new match conditions.</td>
</tr>
<tr>
<td>Packet Size</td>
<td>Specifies the number of bytes to be displayed for each packet. If a packet header exceeds this size, the display is truncated for the packet header. The default value is 96 bytes.</td>
<td>Type the number of bytes you want to capture for each packet header—for example, 256.</td>
</tr>
</tbody>
</table>
Table 132: Packet Capture Field Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t Resolve Addresses</td>
<td>Specifies that IP addresses are not to be resolved into hostnames in the packet headers displayed.</td>
<td>To prevent packet capture from resolving IP addresses to hostnames, select this check box.</td>
</tr>
<tr>
<td>No Timestamp</td>
<td>Suppresses the display of packet header timestamps.</td>
<td>To stop displaying timestamps in the captured packet headers, select this check box.</td>
</tr>
<tr>
<td>Write Packet Capture File</td>
<td>Writes the captured packets to a file in PCAP format in /var/tmp. The files are named with the prefix jweb-pcap and the extension .pcap. If you select this option, the decoded packet headers are not displayed on the packet capture page.</td>
<td>To decode and display the packet headers on the J-Web page, clear this check box.</td>
</tr>
</tbody>
</table>

Related Documentation

- Using the J-Web CLI Terminal on page 395

Monitoring System Properties

**Purpose**

Use the monitoring functionality to view system properties such as the name and IP address of the switch and resource usage.

**Action**

To monitor system properties in the J-Web interface, select Monitor > System View > System Information.

To monitor system properties in the CLI, enter the following commands:

- show system uptime
- show system users
- show system storage

**Meaning**

Table 133 on page 714 summarizes key output fields in the system properties display.

Table 133: Summary of Key System Properties Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number for the switch.</td>
<td></td>
</tr>
<tr>
<td>Junos OS Version</td>
<td>Version of Junos OS active on the switch, including whether the software is for domestic or export use.</td>
<td>Export software is for use outside of the U.S. and Canada.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The name of switch.</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the switch.</td>
<td></td>
</tr>
</tbody>
</table>
Table 133: Summary of Key System Properties Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback Address</td>
<td>The loopback address.</td>
<td></td>
</tr>
<tr>
<td>Domain Name Server</td>
<td>The address of the domain name server.</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone on the switch.</td>
<td></td>
</tr>
<tr>
<td>Current Time</td>
<td>Current system time, in Coordinated Universal Time (UTC).</td>
<td></td>
</tr>
<tr>
<td>System Booted Time</td>
<td>Date and time when the switch was last rebooted and how long it has been running.</td>
<td></td>
</tr>
<tr>
<td>Protocol Started Time</td>
<td>Date and time when the switching protocols were last started and how long they have been running.</td>
<td></td>
</tr>
<tr>
<td>Last Configured Time</td>
<td>Date and time when a configuration was last committed. This field also shows the name of the user who issued the last commit command, through either the J-Web interface or the CLI.</td>
<td></td>
</tr>
<tr>
<td>Load Average</td>
<td>The CPU load average for 1, 5, and 15 minutes.</td>
<td></td>
</tr>
<tr>
<td>Storage Media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Flash Memory</td>
<td>Memory usage details of internal flash.</td>
<td></td>
</tr>
<tr>
<td>External Flash Memory</td>
<td>Usage details of external flash memory.</td>
<td></td>
</tr>
<tr>
<td>Logged in Users Details</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>Username of any user logged in to the switching platform.</td>
<td></td>
</tr>
<tr>
<td>Terminal</td>
<td>Terminal through which the user is logged in.</td>
<td></td>
</tr>
<tr>
<td>From</td>
<td>System from which the user has logged in. A hyphen indicates that the user is logged in through the console.</td>
<td></td>
</tr>
<tr>
<td>Login Time</td>
<td>Time when the user logged in.</td>
<td>This is the LOGIN@ field in the show system users command output.</td>
</tr>
</tbody>
</table>
Table 133: Summary of Key System Properties Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Time</td>
<td>How long the user has been idle.</td>
<td></td>
</tr>
</tbody>
</table>

Related Documentation
- Monitoring System Process Information on page 718
- Understanding J-Web User Interface Sessions on page 393

Monitoring Chassis Information

Purpose
Use the monitoring functionality to view chassis properties such as general switch information, temperature and fan status, and resource information for the EX Series switch.

Action
To view chassis properties in the J-Web interface, select Monitor > System View > Chassis Information. For an EX8200 Virtual Chassis configuration, select the Virtual Chassis member from the list.

To view chassis properties in the CLI, enter the following commands:
- `show chassis environment`
- `show chassis fpc`
- `show chassis hardware`

Meaning
Table 134 on page 716 gives information about the key output fields for chassis information.

NOTE: For an EX2200, EX2200-C, EX3200, or EX4500 switch or an EX4200, EX4300, or EX4550 standalone switch, the FPC slot number refers to the switch itself and is always 0. In a Virtual Chassis configuration, the FPC slot number refers to the member ID.

Table 134: Summary of the Key Output Fields for Chassis Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Engine Details</td>
<td>Select the Master tab to view details about the master Routing Engine or select Backup to view details about the backup Routing Engine.</td>
</tr>
</tbody>
</table>
### Table 134: Summary of the Key Output Fields for Chassis Information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name/Value</strong></td>
<td>This table displays the following details of the master Routing Engine:</td>
</tr>
<tr>
<td></td>
<td>• Routing Engine module</td>
</tr>
<tr>
<td></td>
<td>• Model</td>
</tr>
<tr>
<td></td>
<td>• Version</td>
</tr>
<tr>
<td></td>
<td>• Part number</td>
</tr>
<tr>
<td></td>
<td>• Serial number</td>
</tr>
<tr>
<td></td>
<td>• Memory utilization</td>
</tr>
<tr>
<td></td>
<td>• Temperature</td>
</tr>
<tr>
<td></td>
<td>• Start time</td>
</tr>
<tr>
<td></td>
<td>• CPU load average for 1, 5, and 15 minutes</td>
</tr>
</tbody>
</table>

**Power and Fan Tray Details**

**Power**

Select the **Power** tab to view details of the power supplies.

**Name/Value**

Displays the status and model number of each power supply.

**Fan**

Select the **Fan** tab to view details about the fans.

**Name/Value**

Displays the status of each fan in the corresponding FPC.

**Chassis Component Details**

**Select component**

Select an FPC to view general, temperature, resource, and subcomponent details.

**General**

Select the **General** tab to view the general information about the chassis components.

**Name/Value**

Displays general information:

- **Version**—Revision level. Supply the version number when reporting hardware problems to customer support.
- **Part number**
- **Serial number**—Supply the serial number when contacting customer support about the switch chassis.
- **Description**—Brief text description.

**Temperature**

Select the **Temperature** tab to view the temperature details of the components in the selected FPC.

**Name/Value**

Displays the temperature details of the sensors present in the selected FPC.

**Resource**

Select the **Resource** tab to view the resource details of the selected FPC.
Table 134: Summary of the Key Output Fields for Chassis Information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Value</td>
<td>Displays resource details:</td>
</tr>
<tr>
<td></td>
<td>• State:</td>
</tr>
<tr>
<td></td>
<td>• Dead—Held in reset because of errors.</td>
</tr>
<tr>
<td></td>
<td>• Diag—The FPC is running diagnostics.</td>
</tr>
<tr>
<td></td>
<td>• Dormant—Held in reset.</td>
</tr>
<tr>
<td></td>
<td>• Empty—No FPC is present.</td>
</tr>
<tr>
<td></td>
<td>• Online—The FPC is online and running.</td>
</tr>
<tr>
<td></td>
<td>• Probed—Probe is complete. The FPC is</td>
</tr>
<tr>
<td></td>
<td>awaiting restart of the Packet</td>
</tr>
<tr>
<td></td>
<td>Forwarding Engine.</td>
</tr>
<tr>
<td></td>
<td>• Probe-wait—The FPC is waiting for the</td>
</tr>
<tr>
<td></td>
<td>probe operation to start.</td>
</tr>
<tr>
<td></td>
<td>• Total CPU DRAM—Total DRAM, in</td>
</tr>
<tr>
<td></td>
<td>megabytes, available to the FPC.</td>
</tr>
<tr>
<td></td>
<td>• Start time—Date and time the switch</td>
</tr>
<tr>
<td></td>
<td>was last rebooted.</td>
</tr>
</tbody>
</table>

Related Documentation
- Monitoring System Process Information on page 718
- Monitoring System Properties on page 714
- Dashboard for EX Series Switches on page 670

Monitoring System Process Information

**Purpose**
Use the monitoring functionality to view the processes running on the switch.

**Action**
To view the software processes running on the switch in the J-Web interface, select Monitor > System View > Process Details.

To view the software processes running on the switch in the CLI, enter the following command.

```
show system processes
```

**Meaning**
Table 135 on page 718 summarizes the output fields in the system process information display.

The display includes the total CPU load and total memory utilization.

Table 135: Summary of System Process Information Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Identifier of the process.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Owner of the process.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Current state of the process.</td>
<td></td>
</tr>
</tbody>
</table>
Table 135: Summary of System Process Information Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Load</td>
<td>Percentage of the CPU that is being used by the process.</td>
<td></td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>Amount of memory that is being used by the process.</td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>Time of day when the process started.</td>
<td></td>
</tr>
</tbody>
</table>

Related Documentation

- Monitoring System Properties on page 714
- For more information about show system properties command, see show system uptime on page 4549

Managing Log, Temporary, and Crash Files on the Switch (J-Web Procedure)

You can use the J-Web interface to rotate log files and delete unnecessary log, temporary, and crash files on the switch.

1. Cleaning Up Files on page 719
2. Downloading Files on page 720
3. Deleting Files on page 720

Cleaning Up Files

If you are running low on storage space, use the file cleanup procedure to quickly identify files to delete.

The file cleanup procedure performs the following tasks:

- Rotates log files—Archives the current log files, and creates fresh log files.
- Deletes log files in `/var/log`—Deletes files that are not currently being written to.
- Deletes temporary files in `/var/tmp`—Deletes files that have not been accessed within two days.
- Deletes all crash files in `/var/crash`—Deletes core files that the switch has written during an error.

To rotate log files and delete unnecessary files with the J-Web interface:

1. Select Maintain > Files.
2. In the Clean Up Files section, click Clean Up Files. The switching platform rotates log files and identifies files that can be safely deleted.
   - The J-Web interface displays the files that you can delete and the amount of space that will be freed on the file system.
3. Click one of the following options:
To delete the files and return to the Files page, click OK.

To cancel your entries and return to the list of files in the directory, click Cancel.

**Downloading Files**

You can use the J-Web interface to download a copy of an individual log, temporary, or crash file from the switching platform. When you download a file, it is not deleted from the file system.

To download files with the J-Web interface:

1. In the J-Web interface, select Maintain > Files.
2. In the Download and Delete Files section, click one of the following options:
   - Log Files—Log files in the /var/log directory on the switch.
   - Temporary Files—Lists the temporary files in the /var/tmp directory on the switching platform.
   - Jailed Temporary Files (Install, Session, etc)—Lists the files in the /var/jail/tmp directory on the switching platform.
   - Crash (Core) Files—Lists the core files in the /var/crash directory on the switching platform.

   The J-Web interface displays the files located in the directory.
3. Select the files that you want to download and click Download.
4. Choose a location for the saved file.

   The file is saved as a text file, with a .txt file extension.

**Deleting Files**

You can use the J-Web interface to delete an individual log, temporary, and crash file from the switching platform. When you delete the file, it is permanently removed from the file system.

---

**CAUTION:** If you are unsure whether to delete a file from the switching platform, we recommend using the Clean Up Files tool described in Cleaning Up Files. This tool determines which files can be safely deleted from the file system.

To delete files with the J-Web interface:

1. Select Maintain > Files.
2. In the Download and Delete Files section, Click one of the following options:
- Log Files—Lists the log files in the `/var/log` directory on the switching platform.
- Temporary Files—Lists the temporary files in the `/var/tmp` directory on the switching platform.
- Jailed Temporary Files (Install, Session, etc) — Lists the files in the `/var/jail/tmp` directory on the switching platform.
- Crash (Core) Files—Lists the core files in the `/var/crash` directory on the switching platform.

The J-Web interface displays the files in the directory.

3. Select the box next to each file you plan to delete.
4. Click **Delete**.

The J-Web interface displays the files you can delete and the amount of space that will be freed on the file system.

5. Click one of the following buttons on the confirmation page:
   - To delete the files and return to the Files page, click **OK**.
   - To cancel your entries and return to the list of files in the directory, click **Cancel**.

**Related Documentation**

- [J-Web User Interface for EX Series Switches Overview](#) on page 389

**Operational Commands**
clear log

**Syntax**

```
clear log filename
<all>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Remove contents of a log file.

**Options**

- `filename`—Name of the specific log file to delete.
- `all`—(Optional) Delete the specified log file and all archived versions of it.

**Required Privilege**

- Level: `clear`

**Related Documentation**

- `show log` on page 1091

**List of Sample Output**

- `clear log` on page 722

**Output Fields**

See `file list` for an explanation of output fields.

**Sample Output**

The following sample commands list log file information, clear the contents of a log file, and then display the updated log file information:

```
user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
-----------------------------
-rw-r----- 1 root wheel 26450 Jun 23 18:47 /var/log/sampled
total 1

user@host> clear log lcc0-re0:sampled
lcc0-re0:
-----------------------------

user@host> file list lcc0-re0:/var/log/sampled detail
lcc0-re0:
-----------------------------
-rw-r----- 1 root wheel 57 Sep 15 03:44 /var/log/sampled
total 1
```
file archive

Syntax

file archive destination destination source source
<compress>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Archive, and optionally compress, one or multiple local system files as a single file, locally or at a remote location.

Options

destination destination—Destination of the archived file or files. Specify the destination as a URL or filename. The Junos OS adds one of the following suffixes if the destination filename does not already have it:
- For archived files—The suffix .tar
- For archived and compressed files—The suffix .tgz

source source—Source of the original file or files. Specify the source as a URL or filename.

compress—(Optional) Compress the archived file with the GNU zip (gzip) compression utility. The compressed files have the suffix .tgz.

Required Privilege

maintenance

List of Sample Output

file archive (Multiple Files) on page 723
file archive (Single File) on page 723
file archive (with Compression) on page 724

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

file archive (Multiple Files)

The following sample command archives all message files in the local directory /var/log/messages as the single file messages-archive.tar.

user@host> file archive source /var/log/messages* destination /var/log/messages-archive.tar
/usr/bin/tar: Removing leading / from absolute path names in the archive.
user@host>

file archive (Single File)

The following sample command archives one message file in the local directory /var/log/messages as the single file messages-archive.tar.

user@host> file archive source /var/log/messages destination /var/log/messages-archive.tar
file archive (with Compression)

The following sample command archives and compresses all message files in the local directory `/var/log/messages` as the single file `messages-archive.tgz`.

```
user@host> file archive compress source /var/log/messages* destination /var/log/messages-archive.tgz
/usr/bin/tar: Removing leading / from absolute path names in the archive.
```
**file checksum md5**

**Syntax**  
`file checksum md5 <pathname> filename`

**Release Information**  
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**  
Calculate the Message Digest 5 (MD5) checksum of a file.

**Options**  
- `pathname`—(Optional) Path to a filename.  
- `filename`—Name of a local file for which to calculate the MD5 checksum.

**Required Privilege Level**  
maintenance

**Related Documentation**  
- Configuring Checksum Hashes for a Commit Script in the Junos OS Configuration and Operations Automation Guide  
- Configuring Checksum Hashes for an Event Script in the Junos OS Configuration and Operations Automation Guide  
- Configuring Checksum Hashes for an Op Script in the Junos OS Configuration and Operations Automation Guide  
- Executing an Op Script from a Remote Site in the Junos OS Configuration and Operations Automation Guide  
- file checksum sha-256 on page 534  
- file checksum sha1 on page 533  
- op on page 169

**List of Sample Output**  
file checksum md5 on page 725

**Output Fields**  
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
user@host> file checksum md5 jbundle-5.3R2.4-export-signed.tgz
MD5 (jbundle-5.3R2.4-export-signed.tgz) = 2a3b69e43f9bd4893729cc16f505a0f5
```
**file checksum sha1**

**Syntax**

`file checksum sha1 <pathname> filename`

**Release Information**

Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Calculate the Secure Hash Algorithm (SHA-1) checksum of a file.

**Options**

- `pathname` — (Optional) Path to a filename.
- `filename` — Name of a local file for which to calculate the SHA-1 checksum.

**Required Privilege**

maintenance

**Related Documentation**

- Configuring Checksum Hashes for a Commit Script in the Junos OS Configuration and Operations Automation Guide
- Configuring Checksum Hashes for an Event Script in the Junos OS Configuration and Operations Automation Guide
- Configuring Checksum Hashes for an Op Script in the Junos OS Configuration and Operations Automation Guide
- Executing an Op Script from a Remote Site in the Junos OS Configuration and Operations Automation Guide
- `file checksum md5` on page 532
- `file checksum sha-256` on page 534
- `op` on page 169

**List of Sample Output**

- `file checksum sha1` on page 726

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```bash
user@host> file checksum sha1 /var/db/scripts/opscript.slax
SHA1 (/var/db/scripts/opscript.slax) = ba9e47120c7ce55c572a079af73eacd370e162c676
```
file checksum sha-256

Syntax

file checksum sha-256 <pathname> filename

Release Information

Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Calculate the Secure Hash Algorithm 2 family (SHA-256) checksum of a file.

Options

pathname—(Optional) Path to a filename.
filename—Name of a local file for which to calculate the SHA-256 checksum.

Required Privilege

level maintenance

Related Documentation

• Configuring Checksum Hashes for a Commit Script in the Junos OS Configuration and Operations Automation Guide
• Configuring Checksum Hashes for an Event Script in the Junos OS Configuration and Operations Automation Guide
• Configuring Checksum Hashes for an Op Script in the Junos OS Configuration and Operations Automation Guide
• Executing an Op Script from a Remote Site in the Junos OS Configuration and Operations Automation Guide
• file checksum md5 on page 532
• file checksum sha1 on page 533
• op on page 169

List of Sample Output

file checksum sha-256 on page 727

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

file checksum sha-256

user@host> file checksum sha-256 /var/db/scripts/commitscript.slax
SHA256 (/var/db/scripts/commitscript.slax) =
94c2b061fb55399e15babd2529453815601a602b5c98e5c12ed929c9d343dd71
file compare

Syntax
file compare (files filename filename)
<context | unified>
<ignore-white-space>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Compare two local files and describe the differences between them in default, context, or unified output styles:

- **Default**—In the first line of output, c means lines were changed between the two files, d means lines were deleted between the two files, and a means lines were added between the two files. The numbers preceding this alphabetical marker represent the first file, and the lines after the alphabetical marker represent the second file. A left angle bracket (<) in front of output lines refers to the first file. A right angle bracket (>) in front of output lines refers to the second file.

- **Context**—The display is divided into two parts. The first part is the first file; the second part is the second file. Output lines preceded by an exclamation point (!) have changed. Additions are marked with a plus sign (+), and deletions are marked with a minus sign (-).

- **Unified**—The display is preceded by the line number from the first and the second file (xx,xxx,x). Before the line number, additions to the file are marked with a plus sign (+), and deletions to the file are marked with a minus sign (-). The body of the output contains the affected lines. Changes are viewed as additions plus deletions.

Options
files filename—Names of two local files to compare.
context—(Optional) Display output in context format.
ignore-white-space—(Optional) Ignore changes in the amount of white space.
unified—(Optional) Display output in unified format.

Required Privilege
none

List of Sample Output
file compare files on page 729
file compare files context on page 729
file compare files unified on page 729
file compare files unified ignore-white-space on page 729

Output Fields
When you enter this command, you are provided feedback on the status of your request.
Sample Output

file compare files

```shell
user@host> file compare files /tmp/one /tmp/two
100c100
<             full-name "File 1";
---
>             full-name "File 2";
102c102
<             class foo; # 'foo' is not defined
---
>             class super-user;
```

file compare files context

```shell
user@host> file compare files /tmp/one /tmp/two context
*** /tmp/one    Wed Dec  3 17:12:50 2003
--- /tmp/two    Wed Dec  3 09:13:14 2003
***************
*** 97,104 ****
}            }
user bill {
!             full-name "Bill Smith";
!             class foo; # 'foo' is not defined
|              authentication {  
|               encrypted-password SECRET;
|              }
--- 97,105 ----
}            }
user bill {
!             full-name "Bill Smith";
!             uid 1089;
!             class super-user;
|              authentication {  
|               encrypted-password SECRET;
|              }
```

file compare files unified

```shell
user@host> file compare files /tmp/one /tmp/two unified
--- /tmp/one    Wed Dec  3 17:12:50 2003
+++ /tmp/two    Wed Dec  3 09:13:14 2003
@@ -97,8 +97,9 @@
}            }
user bill {
-             full-name "Bill Smith";
-             class foo; # 'foo' is not defined
+             full-name "Bill Smith";
+             uid 1089;
+             class super-user;
|              authentication {  
|               encrypted-password SECRET;
|              }
```

file compare files unified ignore-white-space

```shell
user@host> file compare files /tmp/one /tmp/two unified ignore-white-space
```
user bill {
    full-name "Bill Smith";
    uid 1089;
    class super-user;
    authentication {
        encrypted-password <SECRET>; # SECRET-DATA
    }
}
file copy

**Syntax**

```
file copy source destination
<source-address address>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- `source-address` option added in Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for QFX Series switches.

**Description**

Copy files from one location to another location on the local device or to a location on a remote device reachable by the local device.

**Required Privilege Level**

maintenance

**Related Documentation**

- Format for Specifying Filenames and URLs in Junos OS CLI Commands
- Default Directories for Junos OS File Storage on the Router or Switch
- Copying a Configuration File from One Routing Engine to the Other

**List of Sample Output**

- Copy a File from the Local Device to a Personal Computer on page 731
- Copy a Configuration File between Routing Engines on page 731
- Copy a Log File between Routing Engines on page 731
- Copy a File from a TX Matrix Plus Router to a T1600 Router Connected to the TX Matrix Plus on page 732
- Copy a File Using File Transfer Protocol on page 732
- Copy a File Using File Transfer Protocol and Requiring a Password on page 732
- Copy a File Using Secure Copy Protocol (scp) on page 732

**Sample Output**

The following are examples of a variety of file copy scenarios.

**Copy a File from the Local Device to a Personal Computer**

```
user@host> file copy /var/tmp/rpd.core.4 mypc:/c/junipero/tmp

...transferring.file...... |          0 KB |   0.3 kB/s | ETA: 00:00:00 | 100%
```

**Copy a Configuration File between Routing Engines**

The following sample command copies a configuration file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy /config/juniper.conf re1:/var/tmp/copied-juniper.conf
```

**Copy a Log File between Routing Engines**

The following sample command copies a log file from Routing Engine 0 to Routing Engine 1:

```
user@host> file copy lcc0-re0:/var/log/chassisd lcc0-re1:/var/tmp
```
Copy a File from a TX Matrix Plus Router to a T1600 Router Connected to the TX Matrix Plus

The following sample command copies a text file from Routing Engine 1 on the switch-fabric chassis sfc0 to Routing Engine 1 on the line-card chassis lcc0:

```
user@host> filecopy sfc0-re1:/tmp/sample.txt lcc0-re1:/var/tmp
```

Copy a File Using File Transfer Protocol

To use anonymous FTP to copy a local file to a remote system, enter the following command:

```
user@host> filecopy filename ftp://hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
user@host> filecopy /config/juniper.conf ftp://hostname/juniper.conf
Receiving ftp://hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using File Transfer Protocol and Requiring a Password

To use FTP where you require more privacy and are prompted for a password, enter the following command:

```
root@host> filecopy filename ftp://user@hostname/filename
```

In the following example, `/config/juniper.conf` is the local file and `hostname` is the FTP server:

```
root@host> filecopy /config/juniper.conf ftp://user@hostname/juniper.conf
Password for user@hostname: ******
Receiving ftp://user@hostname/juniper.conf (2198 bytes): 100%
2198 bytes transferred in 0.0 seconds (2.69 MBps)
```

Copy a File Using Secure Copy Protocol (scp)

To use scp to copy a local file to a remote system, enter the following command:

```
root@host> filecopy filename scp://user@hostname/path/filename
```

In the following example, `/config/juniper.conf` is the local file, user is the username, and ssh-host is the scp server:

```
root@host> filecopy /config/juniper.conf scp://user@ssh-host/tmp/juniper.conf
user@ssh-host's password: ******
juniper.conf 100%
|*************************************************************************|
2198 00:00
```
file delete

Syntax  
file delete filename
<purge>

Release Information  
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Delete a file on the local router or switch.

Options  
filename—Name of the file to delete. For a routing matrix, include chassis information in the filename if the file to be deleted is not local to the Routing Engine from which the command is issued.

purge—(Optional) Overwrite regular files before deleting them.

Required Privilege  
Level  
maintenance

List of Sample Output  
file delete on page 733
file delete (Routing Matrix) on page 733

Output Fields  
When you enter this command, you are provided feedback on the status of your request.

Sample Output  
file delete

user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core

user@host> file delete /var/tmp/snmpd.core
user@host> file list /var/tmp
dcd.core
rpd.core

file delete (Routing Matrix)

user@host> file list lcc0-re0:/var/tmp
dcd.core
rpd.core
snmpd.core

user@host> file delete lcc0-re0:/var/tmp/snmpd.core
user@host> file list /var/tmp
dcd.core
rpd.core
file list

Syntax

```
file list
<detail | recursive>
<filename>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display a list of files on the local router or switch.

Options

```
none—Display a list of all files for the current directory.

detail | recursive—(Optional) Display detailed output or descend recursively through the
directory hierarchy, respectively.

filename—(Optional) Display a list of files. For a routing matrix, the filename must include
the chassis information.
```

Additional Information

The default directory is the home directory of the user logged in to the router or switch.
To view available directories, enter a space and then a backslash (/) after the `file list`
command. To view files within a specific directory, include a backslash followed by the
directory and, optionally, subdirectory name after the `file list` command.

Required Privilege

Level

maintenance

List of Sample Output

file list on page 734
file list (Routing Matrix) on page 734

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

file list

```
user@host> file list /var/tmp
dcd.core
rpdp.core
snmpd.core
```

file list (Routing Matrix)

```
user@host> file list lcc0-re0:var/tmp
lcc0-re0:
-------------------------------------------------------------------
/var/tmp/:
  .gdbinit
  .pccardd
  Test/
  chassisd*
  chassisd.nathan*
  check_time*
```
cores/
diagTestPrep*
diagtest*
diagtest.regress*
do_switchovers*
dump_test*
err.manoj.log
esw_clearstats*
esw_counter*
esw_debug*
esw_debug_ge*
esw_filt_test*
esw_filter_tnp_addr*
esw_getstats*
esw_phy*
esw_stats*
### Rename

**Syntax**

file rename source destination

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Rename a file on the local router or switch.

**Options**

- **destination**—New name for the file.
- **source**—Original name of the file. For a routing matrix, the filename must include the chassis information.

**Required Privilege**

maintenance

**List of Sample Output**

file rename on page 736
file rename (Routing Matrix) on page 736

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

**file rename**

The following example lists the files in `/var/tmp`, renames one of the files, and then displays the list of files again to reveal the newly named file.

```
user@host> file list /var/tmp
dcd.core
rpd.core
snmpd.core
user@host> file rename /var/tmp/dcd.core /var/tmp/dcd.core.990413
user@host> file list /var/tmp
dcd.core.990413
rpd.core
snmpd.core
```

**file rename (Routing Matrix)**

The following example lists the files in `/var/tmp`, renames one of the files, and then displays the list of files again to reveal the newly named file.

```
user@host> file list lcc0-rel:/var/tmp
lcc0-rel:
-----------------------------------------------
/var/tmp:
.pccardd
sartre.conf
```
snmpd
syslogd.core-tarball.0.tgz

user@host> file rename lcc0-re0:/var/tmp/snmpd /var/tmp/snmpd.rr
user@host> file list lcc0-re1:/var/tmp
lcc0-re1:

/var/tmp:
  .pccardd
  sartre.conf
  snmpd.rr
  syslogd.core-tarball.0.tgz
### file show

**Syntax**

```
file show filename
<encoding (base64 | raw)>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display the contents of a file.

**Options**

- `filename`—Name of a file. For a routing matrix, the filename must include the chassis information.

- `encoding (base64 | raw)`—(Optional) Encode file contents with base64 encoding or show raw text.

**Required Privilege**

- `maintenance`

**List of Sample Output**

- file show on page 738
- file show (Routing Matrix) on page 738

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

#### Sample Output

**file show**

```
user@host> file show /var/log/messages
Apr 13 21:00:08 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:00:40 romney /kernel: so-1/1/2: loopback suspected; going to standby.
Apr 13 21:02:48 romney last message repeated 4 times
Apr 13 21:07:04 romney last message repeated 8 times
Apr 13 21:07:13 romney /kernel: so-1/1/0: Clearing SONET alarm(s) RDI-P
Apr 13 21:07:29 romney /kernel: so-1/1/0: Asserting SONET alarm(s) RDI-P
```

**file show (Routing Matrix)**

```
user@host> file show lcc0-re0:/var/tmp/.gdbinit
lcc0-re0:
------------------------------------------------------------------------
# Settings
------------------------------------------------------------------------
set print pretty

# Basic stuff
------------------------------------------------------------------------
define msgbuf
    printf "%s", msgbufp->msg_ptr
end
```
# hex dump of a block of memory
# usage: dump address length
define dump
  p $arg0, $arg1
  set $ch = $arg0
  set $j = 0
  set $n = $arg1
  while ($j < $n)
    printf "%x %x ",&$ch[$j],$ch[$j]
    printf "%x ",$ch[$j]
    set $j = $j + 1
    if (!($j % 16))
      printf "\n"
  end
end
end
monitor list

Syntax

monitor list

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display the status of monitored log and trace files.

Options
This command has no options.

Additional Information
Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the syslog statement at the [edit system] hierarchy level and the options statement at the [edit routing-options] hierarchy level. The trace files generated by the routing protocol process are those configured with traceoptions statements at the [edit routing-options], [edit interfaces], and [edit protocols protocol] hierarchy levels.

Required Privilege Level
trace

Related Documentation
• monitor start on page 741
• monitor stop on page 743

List of Sample Output
monitor list on page 740

Output Fields
Table 136 on page 740 describes the output fields for the monitor list command. Output fields are listed in the approximate order in which they appear.

Table 136: monitor list Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor start</td>
<td>Indicates the file is being monitored.</td>
</tr>
<tr>
<td>&quot;filename&quot;</td>
<td>Name of the file that is being monitored.</td>
</tr>
<tr>
<td>Last changed</td>
<td>Date and time at which the file was last modified.</td>
</tr>
</tbody>
</table>

Sample Output

guest@host> monitor list
monitor start "vrrpd" (Last changed Dec 03:11:06 20)
monitor start "cli-commands" (Last changed Nov 07:3)
**monitor start**

**Syntax**

```plaintext
monitor start filename
```

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Start displaying the system log or trace file and additional entries being added to those files.

**Options**

`filename`—Specific log or trace file.

**Additional Information**

Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are configured with the `syslog` statement at the `[edit system]` hierarchy level and the `options` statement at the `[edit routing-options]` hierarchy level. The trace files generated by the routing protocol process are configured with `traceoptions` statements at the `[edit routing-options]`, `[edit interfaces]`, and `[edit protocols protocol]` hierarchy levels.

![NOTE:](image)

**NOTE:** To monitor a log file within a logical system, issue the `monitor start logical-system-name/filename` command.

**Required Privilege Level**

`trace`

**Related Documentation**

- `monitor list on page 740`
- `monitor stop on page 743`

**List of Sample Output**

`monitor start on page 742`

**Output Fields**

Table 137 on page 741 describes the output fields for the `monitor start` command. Output fields are listed in the approximate order in which they appear.

**Table 137: monitor start Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em><strong>filename</strong></em></td>
<td>Name of the file from which entries are being displayed. This line is displayed initially and when the command switches between log files.</td>
</tr>
<tr>
<td>Date and time</td>
<td>Timestamp for the log entry.</td>
</tr>
</tbody>
</table>
Sample Output

monitor start

user@host> monitor start system-log
*** system-log***
Jul 20 15:07:34 hang sshd[5845]: log: Generating 768 bit RSA key.
Jul 20 15:07:35 hang sshd[5845]: log: Connection from 204.69.248.180 port 912
Jul 20 15:07:37 hang sshd[5845]: log: ROOT LOGIN as 'root' from trip.jcmax.com
Jul 20 15:07:37 hang sshd[5845]: log: Closing connection to 204.69.248.180
**monitor stop**

**Syntax**

```
monitor stop filename
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Stop displaying the system log or trace file.

**Options**

`filename`—Specific log or trace file.

**Additional Information**

Log files are generated by the routing protocol process or by system logging. The log files generated by system logging are those configured with the `syslog` statement at the `[edit system]` hierarchy level and the `options` statement at the `[edit routing-options]` hierarchy level. The trace files generated by the routing protocol process are those configured with `traceoptions` statements at the `[edit routing-options]`, `[edit interfaces]`, and `[edit protocols protocol]` hierarchy levels.

**Required Privilege**

`trace`

**Related Documentation**

- monitor list on page 740
- monitor start on page 741

**List of Sample Output**

- `monitor stop on page 743`

**Output Fields**

This command produces no output.

**Sample Output**

```
monitor stop

user@host> monitor stop
```
request chassis cb

Syntax  request chassis cb (offline | online) slot slot-number

Syntax (TX Matrix Router)  request chassis cb (offline | online) < slot slot-number | lcc number slot cb-slot-number | scc number slot cb-slot-number>

Syntax (TX Matrix Plus Router)  request chassis cb (offline | online) < slot slot-number | lcc number slot cb-slot-number | sfc number slot cb-slot-number>

Syntax (QFabric System)  request chassis cb (offline | online) interconnect-device name slot slot-number < interconnect-device name slot slot-number (offline | online)>

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS 9.4 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS 11.3 for QFX Series.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

Description  (M120, M320, and MX Series routers and T Series routers, QFabric systems, and EX8200 switches only) Control the operation of the Control Board (CB). For information about the meaning of “CBs” on the switches, see “EX Series Switches Hardware and CLI Terminology Mapping” on page 389.

Options  offline—Take the Control Board offline.

NOTE: On a QFabric system, to bring the backup Control Board on a QFX3008-I Interconnect device offline, issue the request chassis cb slot backup-slot-number offline command.

NOTE: Only backup Control Board can be turned offline or online. To turn a Control Board offline or to bring it back online, the Routing Engine should be turned offline first.

online—Bring the Control Board online.

interconnect-device name—(QFabric systems only) (Optional) Bring the QFX3008-I Interconnect device Control Board either offline or online:

slot slot-number—Control Board slot number:
• (TX Matrix and TX Matrix Plus routers only) On a TX Matrix router, if you specify the number of the T640 router by using the lcc number option (the recommended method), replace cb-slot-number with a value from 0 through 1.

Likewise, on a TX Matrix Plus router, if you specify the number of the T1600 or T4000 router by using the lcc number option (the recommended method), replace cb-slot-number with a value from 0 through 1.

• M320 router—Replace slot-number with a value from 0 through 1.
• MX480/MX240 routers—Replace slot-number with a value from 0 through 1.
• MX960 router—Replace slot-number with a value from 0 through 2.
• MX2020 and MX2010 routers—Replace slot-number with 0 or 1.
• EX8208 switch—Replace slot-number with a value from 0 through 2.
• EX8216 switch—Replace slot-number with a value from 0 through 1.
• QFabric System—Replace slot-number with a value from 0 through 1.

lcc number—(TX Matrix, TX Matrix Plus routers only) (Optional) Line-card chassis number. Replace number with the following values depending on the LCC configuration:

• 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
• 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
• 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
• 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

sfc number—(TX Matrix Plus routers only) (Optional) Change the CB status for the TX Matrix Plus router (switch-fabric chassis). Replace number with 0.

Required Privilege Level maintenance

Related Documentation
• show chassis environment cb on page 824
• Switching Control Board Redundancy
• Routing Engine and Switching Control Board Redundancy Configuration Statements

List of Sample Output
request chassis cb on page 746
request chassis cb interconnect-device (QFabric System) on page 746
request chassis cb (MX2020 Router) on page 746
request chassis cb (MX2010 Router) on page 746

Output Fields When you enter this command, you are provided feedback on the status of your request.
Sample Output

request chassis cb

user@host> request chassis cb offline slot 1
Backup CB 1 cannot be set offline, backup RE is online

request chassis cb interconnect-device (QFabric System)

user@switch> request chassis cb interconnect-device interconnect1 offline slot 1
Backup CB 1 cannot be set offline, backup RE is online

request chassis cb (MX2020 Router)

user@host> request chassis cb offline slot 1
Backup CB 1 cannot be set offline, backup RE is online

request chassis cb (MX2010 Router)

user@host> request chassis cb offline slot 1
Backup CB 1 cannot be set offline, backup RE is online
request chassis fabric plane

Syntax
request chassis fabric plane plane-number (offline | online)

Release Information
Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.4 for EX Series switches.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

Description
Control the operation of the specified fabric plane.

Options
offline—Take the fabric plane offline. Use the request chassis fabric plane plane-number offline command to clear a FAULT state on a fabric plane. To bring the fabric plane back online, use the request chassis fabric plane plane-number online command.
online—Bring the fabric plane online.

plane plane-number—Fabric plane number.
  • For the M120 router, replace plane-number with a value from 0 through 3.
  • For the MX480 and MX240 routers, replace plane-number with a value from 0 through 7.
  • For the MX2020 and MX2010 routers, replace plane-number with a value from 0 through 7.
  • For the MX960 router, replace plane-number with a value from 0 through 5.
  • For the EX8208 switch, replace plane-number with a value from 0 through 11.
  • For the EX8216 switch, replace plane-number with a value from 0 through 7.

Required Privilege Level
maintenance

Related Documentation
• show chassis fabric plane on page 960
• show chassis fabric plane-location on page 1002
• show chassis fabric summary on page 1006
• Fabric Management Overview

List of Sample Output
request chassis fabric plane 0 online on page 748
request chassis fabric plane 0 offline on page 748
request chassis fabric plane 0 online (EX8200 switch) on page 748
request chassis fabric plane (MX2020 Router) on page 748
request chassis fabric plane (MX2010 Router) on page 748

Output Fields
When you enter this command, you are provided feedback on the status of your request.
Sample Output

```plaintext
request chassis fabric plane 0 online

user@host> request chassis fabric plane 0 online
Online initiated, use "show chassis fabric plane" to verify

request chassis fabric plane 0 offline

user@host> request chassis fabric plane 0 offline
Offline initiated, use "show chassis fabric plane" to verify

request chassis fabric plane 0 online (EX8200 switch)

user@host> request chassis fabric plane 0 online
Plane 0 is already active

request chassis fabric plane (MX2020 Router)

user@host> request chassis fabric plane 2 online
Plane 2 is already active

request chassis fabric plane (MX2010 Router)

user@host> request chassis fabric plane 4 online
Plane 4 is already active
```
### request chassis fpc

**Syntax**

request chassis fpc (offline | online | restart) slot *slot-number*

**Syntax (TX Matrix and TX Matrix Plus Routers)**

request chassis fpc (offline | online | restart) slot *slot-number*<lcc number>

**Syntax (MX Series Routers)**

request chassis fpc (offline | online | restart) slot *slot-number*<all-members>
<local><member member-id>

**Syntax (MX2020 3D Universal Edge Routers)**

request chassis fpc (offline | online | restart) slot *slot-number*

**Syntax (MX2010 3D Universal Edge Routers)**

request chassis fpc (offline | online | restart) slot *slot-number*

**Syntax (QFabric System)**

request chassis fpc<interconnect-device name slot *slot-number* (offline | online)>
<(offline | online) interconnect-device name slot *slot-number*>
<slot *slot-number* interconnect-device name (offline | online)>

**Syntax (PTX Series Packet Transport Routers)**

request chassis fpc (offline | online | restart) slot *slot-number*

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS 11.3 for QFX Series.
- Command introduced in Junos OS 12.1x48 for PTX Series Packet Transport Routers.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

**Description**

(M20, M40, M40e, M120, M160, M320, MX Series, and T Series routers, QFabric systems, EX Series switches, and PTX Series Packet Transport Routers only) Control the operation of the Flexible PIC Concentrator (FPC). For information about the meaning of “FPCs” on the switches, see "EX Series Switches Hardware and CLI Terminology Mapping" on page 389.

**Options**

- **offline**—Take the FPC offline.
- **online**—Bring the FPC online.
- **interconnect-device name**—(QFabric systems only) Bring the Flexible Port Concentrator (FPC) on the QFX3008-I Interconnect device either offline or online:
• (QFabric System) On a QFabric system, specify the name of the QFX3008-I interconnect device containing the Flexible Port Concentrator (FPC) you want to bring either offline or online.

restart—Restart the FPC.

slot slot-number—FPC slot number:
  • M20 router—0 through 3.
  • M120 router—0 through 5.
  • MX240 router—0 through 2. On the MX240 router, slot-number corresponds to the Dense Port Concentrator (DPC) slot number. If an MPC is installed, slot-number corresponds to the MPC slot number.
  • MX480 router—0 through 5. On the MX480 router, slot-number corresponds to the Dense Port Concentrator (DPC) slot number. If an MPC is installed, slot-number corresponds to the MPC slot number.
  • MX960 router—0 through 11. On the MX960 router, slot-number corresponds to the Dense Port Concentrator (DPC) slot number. If an MPC is installed, slot-number corresponds to the MPC slot number.
  • MX2020 router—0 through 19.
  • MX2010 router—0 through 9.
  • TX Matrix and TX Matrix Plus routers only—On the TX Matrix router, if you specify the number of the T640 router by using the lcc number option (the recommended method), replace slot-number with a value from 0 through 7. Otherwise, replace slot-number with a value from 0 through 31. Likewise, on a TX Matrix Plus router, if you specify the number of the T1600 or T4000 router by using the lcc number option (the recommended method), replace slot-number with a value from 0 through 7. Otherwise, replace slot-number with a value from 0 through 31. In case of TX Matrix Plus router with 3D SIBs, replace slot-number with a value from 0 through 63. For example, the following commands have the same result:

        user@host> request chassis fpc lcc 1 slot 1 offline
        user@host> request chassis fpc slot 9 offline
  • Other routers—0 through 7.
  • QFabric System—Replace slot-number with a value from 0 through 2.
  • EX Series switches:
    • EX4200 switches in a Virtual Chassis configuration—Replace slot-number with a value from 0 through 9.
    • EX6210 switches—Replace slot-number with a value from 0 through 9.
NOTE: These commands are not supported for slots 4 and 5 when a Switch Fabric and Routing Engine (SRE) module is installed in those slots. These commands are supported for slots 4 and 5 only if a line card is installed in them.

- EX8208 switches—Replace `slot-number` with a value from 0 through 7.
- EX8216 switches—Replace `slot-number` with a value from 0 through 15.
- PTX5000 Packet Transport Router—Replace `slot-number` with a value from 0 through 7.

`all-members`—(MX Series routers only) (Optional) Change FPC status of all members of the Virtual Chassis configuration.

`local`—(MX Series routers only) (Optional) Change FPC status of the local Virtual Chassis member.

`member member-id`—(MX Series routers only) (Optional) Change FPC status of the specified member of the Virtual Chassis configuration. Replace `member-id` with a value of 0 or 1.

`lcc number`—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.
Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**Required Privilege Level**
maintenance

**Related Documentation**
- `show chassis fpc` on page 1011
- `show chassis fpc-feb-connectivity`
- `show chassis fabric fpcs` on page 916
- Configuring the Junos OS to Make a Flexible PIC Concentrator Stay Offline
- Configuring the Junos OS to Resynchronize FPC Sequence Numbers with Active FPCs when an FPC Comes Online
• MX960 Flexible PIC Concentrator Description

List of Sample Output

request chassis fpc on page 752
request chassis fpc (MX Series Routers with Media Services Blade [MSB]) on page 752
request chassis fpc (MX2020 Router) on page 752
request chassis fpc (MX2010 Router) on page 752

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request chassis fpc

user@host> request chassis fpc online slot 0
FPC 0 already online

request chassis fpc (MX Series Routers with Media Services Blade [MSB])

user@host> request chassis fpc slot 0
Possible completions:
    offline    Take FPC offline
    online     Bring FPC online
    restart    Restart FPC

request chassis fpc (MX2020 Router)

user@host >request chassis fpc online slot 2
FPC 2 already online

request chassis fpc (MX2010 Router)

user@host >request chassis fpc offline slot 5
Offline initiated, use "show chassis fpc" to verify
request system configuration rescue delete

**Syntax**
request system configuration rescue delete

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Delete an existing rescue configuration.

**NOTE:** The [edit system configuration] hierarchy is not available on QFabric systems.

**Options**
This command has no options.

**Required Privilege Level**
maintenance

**Related Documentation**
- request system configuration rescue save on page 548
- request system software rollback on page 633
- show system commit on page 557

**List of Sample Output**
request system configuration rescue delete on page 753

**Output Fields**
This command produces no output.

**Sample Output**

request system configuration rescue delete

user@host> request system configuration rescue delete
request system configuration rescue save

Syntax  request system configuration rescue save

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  Save the most recently committed configuration as the rescue configuration so that you can return to it at any time by using the rollback command.

NOTE:  The [edit system configuration] hierarchy is not available on QFabric systems.

Options  This command has no options.

Required Privilege Level  maintenance

Related Documentation  • request system software delete on page 629
• request system software rollback on page 633
• show system commit on page 557

List of Sample Output  request system configuration rescue save on page 754

Output Fields  This command produces no output.

Sample Output  request system configuration rescue save

  user@host> request system configuration rescue save
request system scripts refresh-from commit

Syntax
request system scripts refresh-from commit file file-name url url-path

Release Information
Command introduced in Junos OS Release 10.1 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Automatically download the initial Junos OS configuration and a set of standard commit
scripts during a Junos XML management protocol/NETCONF session when a switch is
brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command
is:

```xml
<request-script-refresh-from>
  <type>commit</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

Options
- **file file-name**—Name of the file to be downloaded.
- **url url-path**—URL of the file to be downloaded.

Required Privilege Level
maintenance

Related Documentation
- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Junos OS NETCONF XML Management Protocol Guide

List of Sample Output
request system scripts refresh-from commit file config.txt url
http://host1.juniper.net on page 755

Sample Output
request system scripts refresh-from commit file config.txt url http://host1.juniper.net

user@switch> request system scripts refresh-from commit file config.txt url http://host1.juniper.net
user@switch>
request system scripts refresh-from event

Syntax

request system scripts refresh-from event file file-name url url-path

Release Information


Description

Automatically download the initial Junos OS configuration and a set of standard event scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:

```xml
<request-script-refresh-from>
  <type>event</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

Options

file file-name—Name of the file to be downloaded.

url url-path—URL of the file to be downloaded.

Required Privilege Level

maintenance

Related Documentation

- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Junos OS NETCONF XML Management Protocol Guide

List of Sample Output

request system scripts refresh-from event file config.txt url http://host1.juniper.net on page 756

Sample Output

request system scripts refresh-from event file config.txt url http://host1.juniper.net

user@switch> request system scripts refresh-from event file config.txt url http://host1.juniper.net
user@switch>
request system scripts refresh-from op

Syntax  
request system scripts refresh-from op file file-name url url-path

Release Information  
Command introduced in Junos OS Release 10.1 for EX Series switches.

Description  
Automatically download the initial Junos OS configuration and a set of standard op scripts during a Junos XML management protocol/NETCONF session when a switch is brought up for the first time.

The Junos XML management protocol equivalent for this operational mode command is:

```xml
<request-script-refresh-from>
  <type>op</type>
  <file>file-name</file>
  <URL>URL</URL>
</request-script-refresh-from>
```

Options  
- **file file-name**—Name of the file to be downloaded.
- **url url-path**—URL of the file to be downloaded.

Required Privilege  
Level
maintenance

Related Documentation
- Understanding Automatic Refreshing of Scripts on EX Series Switches on page 496
- Junos OS NETCONF XML Management Protocol Guide

List of Sample Output  
request system scripts refresh-from op file config.txt url http://host1.juniper.net on page 757

Sample Output

```
user@switch> request system scripts refresh-from op file config.txt url http://host1.juniper.net
```

Copyright © 2013, Juniper Networks, Inc.
### show chassis alarms

**Syntax**

- **show chassis alarms**
- **Syntax (TX Matrix Routers)**
  ```
  show chassis alarms
  <lcc number | scc>
  ```
- **Syntax (TX Matrix Plus Routers)**
  ```
  show chassis alarms
  <lcc number | sfc number>
  ```
- **Syntax (MX Series Routers)**
  ```
  show chassis alarms
  <all-members>
  <local>
  <member member-id>
  ```
- **Syntax (MX104, MX2010, and MX2020 3D Universal Edge Routers)**
  ```
  show chassis alarms
  ```
- **Syntax (QFX Series)**
  ```
  show chassis alarms
  <interconnect-device name>
  <node-device name>
  ```
- **Syntax (PTX Series Packet Transport Routers)**
  ```
  show chassis alarms
  ```
- **Syntax (ACX Series Universal Access Routers)**
  ```
  show chassis alarms
  ```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- **sfc** option for the TX Matrix Plus router introduced in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- Command introduced in Junos OS Release 12.1 for the PTX Series Packet Transport Routers.
- Command introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
- Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

**Description**

Display information about the conditions that have been configured to trigger alarms.

**Options**

- **none**—Display information about the conditions that have been configured to trigger alarms.
- **all-members**—(MX Series routers only) (Optional) Display information about alarm conditions for all the member routers of the Virtual Chassis configuration.
interconnect-device name—(QFabric systems only) (Optional) Display information about alarm conditions for the Interconnect device.

lcc number—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.
   Replace number with the following values depending on the LCC configuration:
   • 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
   • 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
   • 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
   • 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers only) (Optional) Display information about alarm conditions for the local Virtual Chassis member.

member member-id—(MX Series routers only) (Optional) Display information about alarm conditions for the specified member of the Virtual Chassis configuration. Replace member-id variable with a value of 0 or 1.

node-device name—(QFabric systems only) (Optional) Display information about alarm conditions for the Node device.

scc—(TX Matrix router only) (Optional) Show information about the TX Matrix router (switch-card chassis).

sfc number—(TX Matrix Plus router only) (Optional) Show information about the respective TX Matrix Plus router, which is the switch-fabric chassis. Replace number variable with 0.

Additional Information

You cannot clear the alarms for chassis components. Instead, you must remedy the cause of the alarm. When a chassis alarm LED is lit, it indicates that you are running the router or switch in a manner that we do not recommend.

On routers, you can manually silence external devices connected to the alarm relay contacts by pressing the alarm cutoff button, located on the craft interface. Silencing the device does not remove the alarm messages from the display (if present on the router) or extinguish the alarm LEDs. In addition, new alarms that occur after you silence an external device reactivate the external device.

In Junos OS release 11.1 and later, alarms for fans also show the slot number of the fans in the CLI output.

In Junos OS Release 11.2 and later, the command output on EX8200 switches shows the detailed location (Plane/FPC/PFE) for link errors in the chassis.
In Junos OS Release 10.2 and later, an alarm is shown on T Series routers for a standby sonic clock generator (SCG) that is offline or absent.

You may often see the following error messages, in which only the error code is shown and no other information is provided:

```
Apr 12 08:04:10 send: redalarmset, device FPC 6, reason FPC 6 Major Errors - Error code: 257
Apr 12 08:04:19 send: redalarmset, device FPC 1, reason FPC 1 Major Errors - Error code: 559
```

To understand what CM_ALARM error codes mean, you need to first identify the structure of the CM Alarm codes. A CM_ALARM code has the following structure:

<table>
<thead>
<tr>
<th>Bits:</th>
<th>Error type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-31</td>
<td>Major (1)</td>
</tr>
<tr>
<td>0</td>
<td>Minor (0)</td>
</tr>
</tbody>
</table>

According to the table above, the LSB (bit 0) identifies the **Error Type** (major alarm, if the bit is set and minor alarm if the bit is unset). The rest of the bits (1 - 31) identify the actual error code.

Take an example of the following error code, which was logged on a T1600:

```
Apr 12 08:04:10 send: red alarm set, device FPC 1, reason FPC 1 Major Errors - Error code: 559
```

First, you have to convert 559 to binary; that is **100010111**. The LSB in this case is **1**, which means that this is a major alarm. After removing the LSB, you are left with **10001011**. This is equal to 279 in decimal. This is the actual error code, its meaning can be found from the following list:

<table>
<thead>
<tr>
<th>Chip Type: L Chip</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMALARM_LCHIP_LOUT_DESRD_PARITY_ERR</td>
<td>1</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_DESRD_UNINIT_ERR</td>
<td>2</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_DESRD_ILLEGALLINK_ERR</td>
<td>3</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_DESRD_ILLEGALSIZE_ERR</td>
<td>4</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_HDRF_TOERR_ERR</td>
<td>5</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_HDRF_PARITY_ERR</td>
<td>6</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_HDRF_UCERR_ERR</td>
<td>7</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_NLIF_CRCDROP_ERR</td>
<td>8</td>
</tr>
<tr>
<td>Code Chip</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_NLIF_CRCERR_ERR</td>
<td>9</td>
</tr>
<tr>
<td>CMALARM_LCHIP_UCODE_TIMEOUT_ERR</td>
<td>10</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LIN_SRCTL_ACCT_DROP_ERR</td>
<td>11</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LIN_SRCTL_ACCT_ADDR_SIZE_ERR</td>
<td>12</td>
</tr>
<tr>
<td>CMALARM_LCHIP_SRAM_PARITY_ERR</td>
<td>13</td>
</tr>
<tr>
<td>CMALARM_LCHIP_UCODE_OVFLW_ERR</td>
<td>14</td>
</tr>
<tr>
<td>CMALARM_LCHIP_LOUT_HDRF_MTU_ERR</td>
<td>15</td>
</tr>
</tbody>
</table>

**Chip Type: M Chip**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMALARM_MCHIP_ECC_UNCORRECT_ERR</td>
<td>128</td>
</tr>
</tbody>
</table>

**Chip Type: N Chip**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMALARM_NCHIP_RDDMA_JBUS_TIMEOUT_ERR</td>
<td>256</td>
</tr>
<tr>
<td>CMALARM_NCHIP_RDDMA_FIFO_OVFLW_ERR</td>
<td>257</td>
</tr>
<tr>
<td>CMALARM_NCHIP_RDDMA_FIFO_UNFLW_ERR</td>
<td>258</td>
</tr>
<tr>
<td>CMALARM_NCHIP_RDDMA_SIZE_ERR</td>
<td>259</td>
</tr>
<tr>
<td>CMALARM_NCHIP_RDDMA_JBUS_CRC_ERR</td>
<td>260</td>
</tr>
<tr>
<td>CMALARM_NCHIP_WRDMA_PKTR_ERR</td>
<td>261</td>
</tr>
<tr>
<td>CMALARM_NCHIP_WRDMA_PKT_CRC_ERR</td>
<td>262</td>
</tr>
<tr>
<td>CMALARM_NCHIP_WRDMA_JBUS_TIMEOUT_ERR</td>
<td>263</td>
</tr>
<tr>
<td>CMALARM_NCHIP_WRDMA_FIFO_OVFLW_ERR</td>
<td>264</td>
</tr>
<tr>
<td>CMALARM_NCHIP_WRDMA_FIFO_UNFLW_ERR</td>
<td>265</td>
</tr>
<tr>
<td>CMALARM_NCHIP_WRDMA_PKT_LEN_ERR</td>
<td>266</td>
</tr>
<tr>
<td>CMALARM_NCHIP_WRDMA_JBUS_CRC_ERR</td>
<td>267</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_DMA_AGE_ERR</td>
<td>268</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_ICELLSIG_ERR</td>
<td>269</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_FTTL_ERR</td>
<td>270</td>
</tr>
<tr>
<td>Chip Type: R Chip</td>
<td>Code</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>CMALARM_NCHIP_RODR_OFFSET_OVFLW_ERR</td>
<td>271</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_TMO_CELL_ERR</td>
<td>272</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_TMO_OUTRANGE_ERR</td>
<td>273</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_MD_REQUEST_Q_OVFLW_ERR</td>
<td>274</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_DMA_BUFFER_OVFLW_ERR</td>
<td>275</td>
</tr>
<tr>
<td>CMALARM_NCHIP_PKTR_GRT_OVFLW_ERR</td>
<td>276</td>
</tr>
<tr>
<td>CMALARM_NCHIP_FRQ_ERR</td>
<td>277</td>
</tr>
<tr>
<td>CMALARM_NCHIP_RODR_IN_Q_OVFLW_ERR</td>
<td>278</td>
</tr>
<tr>
<td>CMALARM_NCHIP_DBUF_CRC_ERR</td>
<td>279</td>
</tr>
</tbody>
</table>

**CodeChipType: RChip**

<table>
<thead>
<tr>
<th>Chip Type: R Chip</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMALARM_RCHIP_SRAM_PARITY_ERR</td>
<td>512</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chip Type: R Chip</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMALARM_ICHIP_WO_DESRD_ID_ERR</td>
<td>601</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_DESRD_DATA_ERR</td>
<td>602</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_DESRD_OFLOW_ERR</td>
<td>603</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_HDRF_UCERR_ERR</td>
<td>604</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_HDRF_MITUERR_ERR</td>
<td>605</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_HDRF_PARITY_ERR</td>
<td>606</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_HDRF_TOERR_ERR</td>
<td>607</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_IP_CRC_ERR</td>
<td>608</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WO_IP_INTER_ERR</td>
<td>609</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WI_WAN_TIMEOUT_ERR</td>
<td>625</td>
</tr>
<tr>
<td>CMALARM_ICHIP_WI_FAB_TIMEOUT_ERR</td>
<td>626</td>
</tr>
<tr>
<td>CMALARM_ICHIP_RLDREAM_BIST_ERR</td>
<td>630</td>
</tr>
<tr>
<td>CMALARM_ICHIP_SDRAM_BIST_ERR</td>
<td>631</td>
</tr>
</tbody>
</table>
According to the table above, the 279 error code corresponds to **CMALARM_NCHIP_DBUF_CRC_ERR**; this means that new CRC errors were seen on the NCHIP of this particular FPC, which is FPC as per the logs.

If you do not want to convert decimal to binary and vice versa, you may use the following shortcut:

For major alarms, the Actual Error Code = (Error Code - 1)/2, where Error Code is the code that you get in the log message. For example, if you get the following log:

```
Apr 12 08:04:10 send: red alarm set, device FPC 6, reason FPC 6 Major Errors - Error code: 257
```

Actual Error Code = (257-1)/2 = 128. Similarly, for minor alarms, Actual Error Code = (Error Code)/2

**Related Documentation**
- Configuring an Alarm Entry and Its Attributes
- Chassis Conditions That Trigger Alarms

**List of Sample Output**
- show chassis alarms (Alarms Active) on page 764
- show chassis alarms (No Alarms Active) on page 764
- show chassis alarms (Fan Tray) on page 764
- show chassis alarms (MX104 Router) on page 764
- show chassis alarms (MX2010 Router) on page 764
- show chassis alarms (MX2020 Router) on page 765
- show chassis alarms (T4000 Router) on page 765
- show chassis alarms (Unreachable Destinations Present on a T Series Router) on page 765
- show chassis alarms (FPC Offline Due to Unreachable Destinations on a T Series Router) on page 765
- show chassis alarms (SCG Absent on a T Series Router) on page 766
- show chassis alarms (Alarms Active on a TX Matrix Router) on page 766
- show chassis alarms (TX Matrix Plus router with 3D SIBs) on page 766
- show chassis alarms (Alarms on a T4000 Router After the enhanced-mode Statement is Enabled) on page 767
- show chassis alarms (Backup Routing Engine) on page 767
- show chassis alarms (Alarms Active on the QFX Series) on page 767
show chassis alarms node-device (Alarms Active on the QFabric System) on page 767
show chassis alarms (Alarms Active on the QFabric System) on page 766
show chassis alarms (Alarms Active on an EX8200 Switch) on page 768
show chassis alarms (Alarms Active on a PTX5000 Packet Transport Router) on page 768
show chassis alarms (Alarms Active on an ACX2000 Universal Access Router) on page 769

Output Fields

Table 138 on page 764 lists the output fields for the show chassis alarms command. Output fields are listed in the approximate order in which they appear.

Table 138: show chassis alarms Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm time</td>
<td>Date and time the alarm was first recorded.</td>
</tr>
<tr>
<td>Class</td>
<td>Severity class for this alarm: Minor or Major.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about the alarm.</td>
</tr>
</tbody>
</table>

Sample Output

show chassis alarms (Alarms Active)

user@host> show chassis alarms
3 alarms are currently active
Alarm time               Class  Description
2000-02-07 10:12:22 UTC Major fxp0: ethernet link down
2000-02-07 10:11:54 UTC Minor YELLOW ALARM - PEM 1 Removed
2000-02-07 10:11:03 UTC Minor YELLOW ALARM - Lower Fan Tray Removed

show chassis alarms (No Alarms Active)

user@host> show chassis alarms
No alarms are currently active

show chassis alarms (Fan Tray)

user@host> show chassis alarms
4 alarms currently active
Alarm time               Class  Description
2010-11-11 20:27:38 UTC Major Side Fan Tray 7 Failure
2010-11-11 20:27:13 UTC Minor Side Fan Tray 7 Overspeed
2010-11-11 20:27:13 UTC Major Side Fan Tray 5 Failure
2010-11-11 20:27:13 UTC Major Side Fan Tray 0 Failure

show chassis alarms (MX104 Router)

user@host> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2013-06-05 14:43:31 IST Minor Backup RE Active

show chassis alarms (MX2010 Router)

user@host> show chassis alarms
### show chassis alarms (MX2020 Router)

<table>
<thead>
<tr>
<th>Alarm time</th>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-08-07 00:46:06 PDT</td>
<td>Major</td>
<td>Fan Tray 2 Failure</td>
</tr>
<tr>
<td>2012-08-06 18:24:36 PDT</td>
<td>Minor</td>
<td>Redundant feed missing for PSM 6</td>
</tr>
<tr>
<td>2012-08-06 07:41:04 PDT</td>
<td>Minor</td>
<td>Redundant feed missing for PSM 8</td>
</tr>
<tr>
<td>2012-08-04 02:42:06 PDT</td>
<td>Minor</td>
<td>Redundant feed missing for PSM 5</td>
</tr>
<tr>
<td>2012-08-03 21:14:24 PDT</td>
<td>Minor</td>
<td>Loss of communication with Backup RE</td>
</tr>
<tr>
<td>2012-08-03 12:26:03 PDT</td>
<td>Minor</td>
<td>Redundant feed missing for PSM 4</td>
</tr>
<tr>
<td>2012-08-03 10:40:18 PDT</td>
<td>Minor</td>
<td>Redundant feed missing for PSM 7</td>
</tr>
</tbody>
</table>

### show chassis alarms (T4000 Router)

<table>
<thead>
<tr>
<th>Alarm time</th>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-06-02 01:41:10 UTC</td>
<td>Minor</td>
<td>RE 0 Not Supported</td>
</tr>
<tr>
<td>2007-06-02 01:41:10 UTC</td>
<td>Minor</td>
<td>CB 0 Not Supported</td>
</tr>
<tr>
<td>2007-06-02 01:41:10 UTC</td>
<td>Minor</td>
<td>Mixed Master and Backup RE types</td>
</tr>
<tr>
<td>2007-05-30 19:37:33 UTC</td>
<td>Major</td>
<td>SPMB 1 not online</td>
</tr>
<tr>
<td>2007-05-30 19:37:29 UTC</td>
<td>Minor</td>
<td>Front Bottom Fan Tray Absent</td>
</tr>
<tr>
<td>2007-05-30 19:37:13 UTC</td>
<td>Major</td>
<td>PEM 1 Input Failure</td>
</tr>
<tr>
<td>2007-05-30 19:37:13 UTC</td>
<td>Major</td>
<td>PEM 0 Not OK</td>
</tr>
<tr>
<td>2007-05-30 19:37:03 UTC</td>
<td>Major</td>
<td>PEM 0 Improper for Platform</td>
</tr>
<tr>
<td>2007-05-30 19:37:03 UTC</td>
<td>Minor</td>
<td>Backup RE Active</td>
</tr>
</tbody>
</table>

### show chassis alarms (Unreachable Destinations Present on a T Series Router)

<table>
<thead>
<tr>
<th>Alarm time</th>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-08-30 18:43:53 PDT</td>
<td>Major</td>
<td>FPC 7 has unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:53 PDT</td>
<td>Major</td>
<td>FPC 5 has unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:52 PDT</td>
<td>Major</td>
<td>FPC 3 has unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:52 PDT</td>
<td>Major</td>
<td>FPC 2 has unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:52 PDT</td>
<td>Minor</td>
<td>SIB 0 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:33 PDT</td>
<td>Minor</td>
<td>SIB 4 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:28 PDT</td>
<td>Minor</td>
<td>SIB 3 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:05 PDT</td>
<td>Minor</td>
<td>SIB 2 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:28 PDT</td>
<td>Minor</td>
<td>SIB 1 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:05 PDT</td>
<td>Major</td>
<td>PEM 1 Not Ok</td>
</tr>
</tbody>
</table>

### show chassis alarms (FPC Offline Due to Unreachable Destinations on a T Series Router)

<table>
<thead>
<tr>
<th>Alarm time</th>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-08-30 18:43:53 PDT</td>
<td>Major</td>
<td>FPC 7 offline due to unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:53 PDT</td>
<td>Major</td>
<td>FPC 5 offline due to unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:52 PDT</td>
<td>Major</td>
<td>FPC 3 offline due to unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:52 PDT</td>
<td>Major</td>
<td>FPC 2 offline due to unreachable destinations</td>
</tr>
<tr>
<td>2011-08-30 18:43:52 PDT</td>
<td>Minor</td>
<td>SIB 0 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:33 PDT</td>
<td>Minor</td>
<td>SIB 4 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:28 PDT</td>
<td>Minor</td>
<td>SIB 3 Not Online</td>
</tr>
<tr>
<td>2011-08-30 18:43:05 PDT</td>
<td>Minor</td>
<td>SIB 2 Not Online</td>
</tr>
</tbody>
</table>
### show chassis alarms (SCG Absent on a T Series Router)

```
user@host> show chassis alarms
4 alarms currently active
  Alarm time               Class  Description
  2011-01-23 21:42:46 PST  Major  SCG 0 NO EXT CLK MEAS-BKUP SCG ABS
```

### show chassis alarms (Alarms Active on a TX Matrix Router)

```
user@host> show chassis alarms
  scc-re0:
  8 alarms currently active
  Description
  2004-08-05 18:43:53 PDT  Minor  LCC 0 Minor Errors
  2004-08-05 18:43:53 PDT  Minor  SIB 3 Not Online
  2004-08-05 18:43:52 PDT  Major  SIB 2 Absent
  2004-08-05 18:43:52 PDT  Major  SIB 1 Absent
  2004-08-05 18:43:52 PDT  Major  SIB 0 Absent
  2004-08-05 18:43:33 PDT  Major  LCC 2 Major Errors
  2004-08-05 18:43:28 PDT  Major  LCC 0 Major Errors
  2004-08-05 18:43:05 PDT  Minor  LCC 2 Minor Errors
```

```
user@host> show chassis alarms
  scc-re0:
  5 alarms currently active
  Description
  2004-08-05 18:43:53 PDT  Minor  SIB 3 Not Online
  2004-08-05 18:43:49 PDT  Major  SIB 2 Absent
  2004-08-05 18:43:49 PDT  Major  SIB 1 Absent
  2004-08-05 18:43:49 PDT  Major  SIB 0 Absent
  2004-08-05 18:43:28 PDT  Major  PEM 0 Not OK
```

```
user@host> show chassis alarms
  lcc2-re0:
  5 alarms currently active
  Description
  2004-08-05 18:43:35 PDT  Minor  SIB 3 Not Online
  2004-08-05 18:43:33 PDT  Major  SIB 2 Absent
  2004-08-05 18:43:33 PDT  Major  SIB 1 Absent
  2004-08-05 18:43:33 PDT  Major  SIB 0 Absent
  2004-08-05 18:43:05 PDT  Minor  PEM 1 Absent
```

### show chassis alarms (TX Matrix Plus router with 3D SIBs)

```
user@host> show chassis alarms
  sfc0-re0:
  Description
  2012-07-19 10:07:32 UTC  Minor  SIB F13 0 Temperature Warm
  2012-07-19 10:07:07 UTC  Minor  SIB F2S 0/6 Temperature Warm
  2012-07-19 10:07:07 UTC  Minor  SIB F2S 0/4 Temperature Warm
  2012-07-19 10:07:07 UTC  Minor  SIB F2S 0/2 Temperature Warm
  2012-07-19 10:07:07 UTC  Minor  SIB F2S 0/0 Temperature Warm
  2012-07-19 10:07:07 UTC  Minor  SIB F13 6 Temperature Warm
  2012-07-19 10:06:42 UTC  Minor  SIB F2S 2/6 Temperature Warm
  2012-07-19 10:06:42 UTC  Minor  SIB F2S 2/4 Temperature Warm
  2012-07-19 10:06:42 UTC  Minor  SIB F2S 2/2 Temperature Warm
  2012-07-19 10:06:42 UTC  Minor  SIB F2S 2/0 Temperature Warm
  2012-07-19 10:06:42 UTC  Minor  SIB F13 3 Temperature Warm
  2012-07-19 10:06:17 UTC  Minor  Temperature Warm
```
show chassis alarms (Alarms on a T4000 Router After the enhanced-mode Statement is Enabled)

To enable improved virtual private LAN service (VPLS) MAC address learning on T4000 routers, you must include the `enhanced-mode` statement at the `edit chassis network-services` hierarchy level and reboot the router. When router reboots, only the T4000 Type 5 FPCs are required to be present on the router. If there are any other FPCs (apart from T4000 Type 5 FPCs) on the T4000 router, such FPCs become offline, and FPC misconfiguration alarms are generated. The `show chassis alarm` command output displays FPC misconfiguration (FPC `fpc-slot misconfig`) as the reason for the generation of the alarms.

```
user@host> show chassis alarms
2 alarms currently active
  Alarm time               Class  Description
  2011-10-22 10:10:47 PDT  Major  FPC 1 misconfig
  2011-10-22 10:10:46 PDT  Major  FPC 0 misconfig
```

show chassis alarms (Backup Routing Engine)

```
user@host> show chassis alarms
2 alarms currently active
  Alarm time               Class  Description
  2005-04-07 10:12:22 PDT  Minor  Host 1 Boot from alternate media
  2005-04-07 10:11:54 PDT  Major  Host 1 compact-flash missing in Boot List
```

show chassis alarms (Alarms Active on the QFX Series)

```
user@switch> show chassis alarms
1 alarms currently active
  Alarm time               Class  Description
  2012-03-05 2:10:24 UTC  Major  FPC 0 PEM 0 Airflow not matching Chassis Airflow
```

show chassis alarms node-device (Alarms Active on the QFabric System)

```
user@switch> show chassis alarms node-device ED3691
node-device ED3694
3 alarms currently active
  Alarm time               Class  Description
  2011-08-24 16:04:15 UTC  Major  ED3694:fte-0/1/2: Link down
```
show chassis alarms (Alarms Active on the QFabric System)

```
user@switch> show chassis alarms
IC-A0001:

1 alarms currently active
Alarm time               Class  Description
2011-08-24 16:04:15 UTC  Minor  Backup RE Active

ED3694:

3 alarms currently active
Alarm time               Class  Description
2011-08-24 16:04:15 UTC  Major  ED3694:fte-0/1/2: Link down
2011-08-24 16:04:14 UTC  Major  ED3694:fte-0/1/0: Link down
2011-08-24 14:21:14 UTC  Major  ED3694 PEM 0 is not supported/powered

SN-0:

NW-NG-0:

1 alarms currently active
Alarm time               Class  Description
2011-08-24 15:49:27 UTC  Major  ED3691 PEM 0 is not supported/powered
```

show chassis alarms (Alarms Active on an EX8200 Switch)

```
user@switch> show chassis alarms

6 alarms currently active
Alarm time               Class  Description
2010-12-02 19:15:22 UTC  Major  Fan Tray Failure
2010-12-02 19:15:22 UTC  Major  Fan Tray Failure
2010-12-02 19:15:14 UTC  Minor  Check CB 0 Fabric Chip 1 on Plane/FPC/PFE: 1/5/0, 1/5/1, 1/5/2, 1/5/3, 1/7/0, 1/7/1, 1/7/2, 1/7/3, 2/5/0, 2/5/1, ...
2010-12-02 19:15:14 UTC  Minor  Check CB 0 Fabric Chip 0 on Plane/FPC/PFE: 1/5/0, 1/5/1, 1/5/2, 1/5/3, 1/7/0, 1/7/1, 1/7/2, 1/7/3, 2/5/0, 2/5/1, ...
2010-12-02 19:15:14 UTC  Minor  PSU 1 Output Failure
2010-12-02 19:14:18 UTC  Minor  Loss of communication with Backup RE
```

show chassis alarms (Alarms Active on a PTX5000 Packet Transport Router)

```
user@switch> show chassis alarms

23 alarms currently active
Alarm time               Class  Description
2011-07-12 16:22:05 PDT  Minor  No Redundant Power for Rear Chassis
2011-07-12 16:22:05 PDT  Minor  PDU 0 PSM 1 Not OK
2011-07-12 16:21:57 PDT  Minor  PDU 0 PSM 0 Not OK
2011-07-12 15:56:06 PDT  Major  PDU 1 PSM 2 Not OK
2011-07-12 15:56:06 PDT  Minor  No Redundant Power for FPC 0-7
2011-07-12 15:56:06 PDT  Major  PDU 0 PSM 3 Not OK
2011-07-12 15:28:20 PDT  Major  PDU 0 PSM 2 Not OK
2011-07-12 15:19:14 PDT  Minor  Backup RE Active
```
show chassis alarms (Alarms Active on an ACX2000 Universal Access Router)

```plaintext
user@host> show chassis alarms
7 alarms currently active

<table>
<thead>
<tr>
<th>Alarm time</th>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-05-22 11:19:09 UTC</td>
<td>Major</td>
<td>xe-0/3/1: Link down</td>
</tr>
<tr>
<td>2012-05-22 11:19:09 UTC</td>
<td>Major</td>
<td>xe-0/3/0: Link down</td>
</tr>
<tr>
<td>2012-05-22 11:19:09 UTC</td>
<td>Major</td>
<td>ge-0/1/7: Link down</td>
</tr>
<tr>
<td>2012-05-22 11:19:09 UTC</td>
<td>Major</td>
<td>ge-0/1/6: Link down</td>
</tr>
<tr>
<td>2012-05-22 11:19:09 UTC</td>
<td>Major</td>
<td>ge-0/1/3: Link down</td>
</tr>
<tr>
<td>2012-05-22 11:19:09 UTC</td>
<td>Major</td>
<td>ge-0/1/2: Link down</td>
</tr>
<tr>
<td>2012-05-22 11:19:09 UTC</td>
<td>Major</td>
<td>ge-0/1/1: Link down</td>
</tr>
</tbody>
</table>
```
### show chassis environment

**Syntax**  
show chassis environment

**Syntax (T320, T640, T1600, and T4000 Routers)**  
```
show chassis environment
<cb cb-slot-number>
<fpc fpc-slot-number>
<fpm>
<pem pem-slot-number>
<routing-engine re-slot-number>
<scg scg-slot-number>
<sib sib-slot-number>
```

**Syntax (TX Matrix Routers)**  
```
show chassis environment
<lcc number | scc>
```

**Syntax (TX Matrix Plus Routers)**  
```
show chassis environment
<cb cb-slot-number>
<clp clp-slot-number>
<fpc fpc-slot-number>
<fpm>
<lcc number>
<pem pem-slot-number>
<routing-engine re-slot-number>
<scg scg-slot-number>
<sfc number>
<sib sib-slot-number>
```

**Syntax (MX Series Routers)**  
```
show chassis environment
<all-members>
<local>
<member member-id>
```

**Syntax (MX104 3D Universal Edge Routers)**  
```
show chassis environment
<cb>
<pem pem-slot-number>
<routing-engine re-slot-number>
```

**Syntax (MX2010 and MX2020 3D Universal Edge Routers)**  
```
show chassis environment
<adc adc-slot-number>
<cb cb-slot-number>
<fpc fpc-slot-number>
<fpm>
<monitored>
<psm psm-slot-number>
<routing-engine re-slot-number>
<sfb sfb-slot-number>
```

**Syntax (EX Series Switch)**  
```
show chassis environment
<all-members>
<cb cb-slot-number>
<fpc fpc-slot-number>
<local>
```
<member member-id>
<routing-engine re-slot-number>

Syntax (EX Series Switch)  show chassis environment
<all-members>
<cb cb-slot-number>
<fpc fpc-slot-number>
<local>
<member member-id>
<power-supply-unit psu-slot-number>
<routing-engine slot-number>

Syntax (QFX Series)  show chassis environment
<cb slot-number <interconnect-device name>>
<fpc slot-number <interconnect-device name>>
<interconnect-device name <slot-number>
<node-device name>
<pem slot-number (interconnect-device name slot-number) | (node-device name)>
<routing-engine name <interconnect-device name slot-number>

Syntax (PTX Series Packet Transport Routers)  show chassis environment
<cb cb-slot-number>
<ccg ccg-slot-number>
<fpc fpc-slot-number>
<fpm>
<monitored>
<pdu pdu-slot-number>
<routing-engine re-slot-number>
<sib sib-slot-number>

Syntax (ACX Series Universal Access Routers)  show chassis environment
<cb cb-slot-number>
<pem pem-slot-number>
<routing-engine re-slot-number>

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for QFX Series.
Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
monitored option added in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
Command introduced in Junos OS Release 12.1 for T4000 Core Routers.
Command introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
pem option introduced in Junos OS Release 12.3 for ACX4000 Universal Access Routers.
Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

Description  Display environmental information about the router or switch chassis, including the temperature and information about the fans, power supplies, and Routing Engine.
In addition on ACX4000 routers, display temperature information about the different channels of a Modular Interface Card (MIC). The number of channels displayed depends on the type of MIC installed.

**Options**

none—Display environmental information about the router or switch chassis. On a TX Matrix router, display environmental information about the TX Matrix router and its attached T640 routers. On a TX Matrix Plus router, display environmental information about the TX Matrix Plus router and its attached routers.

all-members—(MX Series routers and EX Series switches only) (Optional) Display chassis environmental information for all the members of the Virtual Chassis configuration.

adc adc-slot-number—(MX2020 and MX2010 routers only) (Optional) Display chassis environmental information for the adapter cards. For MX2020 routers, replace `adc-slot-number` with a value from 0 through 19. For MX2010 routers, replace `adc-slot-number` with a value from 0 through 9.

cb cb-slot-number—(ACX Series Universal Access Routers, EX Series switches, M120, M320, and M40e routers, MX Series routers, MX2020 routers, MX2010 routers, PTX Series Packet Transport Routers, QFX Series, and T Series routers, and TX Matrix Plus routers only) (Optional) Display chassis environmental information for the Control Board. On devices other than EX Series switches, replace `cb-slot` with 0 or 1. For the EX Series switches, see “EX Series Switches Hardware and CLI Terminology Mapping” on page 389 for information on CB slot numbering.

cip cip-slot-number—(TX Matrix Plus routers only) (Optional) Display chassis environmental information for the Connection Interface Panel (CIP). Replace the `cip-slot-number` variable with a value of 0 or 1.

cb interconnect-device name—(QFabric systems only) (Optional) Display chassis environmental information for the Control Board on an Interconnect device.

ccg ccg-slot-number—(PTX Series only) (Optional) Display chassis environmental information for the Centralized Clock Generator. Replace `cb-slot` with a value of 0 or 1.

fpc fpc-slot—(EX Series switches, M120, M320, and M40e routers, MX Series routers, MX2010 routers, MX2020 routers, PTX Series Packet Transport Routers, QFX Series, QFX3500 switches, QFabric systems, T Series routers, and TX Matrix Plus routers) (Optional) Display chassis environmental information for a specified Flexible PIC Concentrator. For MX2010 routers, replace `fpc-slot` with a value from 0 through 9. For MX2020 routers, replace `fpc-slot` with a value from 0 through 19. For information about FPC numbering, see `show chassis environment fpc`. On a QFabric system, display chassis environmental information for a specified Flexible PIC Concentrator on an Interconnect device. On an EX Series switch, display chassis environmental information for a specified Flexible PIC Concentrator; see “EX Series Switches Hardware and CLI Terminology Mapping” on page 389 for information on FPC numbering. On a TX Matrix Plus router with 3D SiBs replace `fpc-slot` with a value from 0 through 63.
fpm—(M120, M320, and M40e routers, MX2010 routers, MX2020 routers, PTX Series, Packet Transport Routers, T Series routers, and TX Matrix Plus routers only) (Optional) Display chassis environmental information for the craft interface (FPM).

interconnect-device name—(QFabric systems only) (Optional) Display chassis environmental information for the Interconnect device.

monitored—(MX2020 routers and PTX Series Packet Transport Routers only) (Optional) Display chassis environmental information for monitored temperatures only. Temperatures that are not included in temperature alarm computations are not displayed.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers and EX Series switches) (Optional) Display chassis environmental information for the local Virtual Chassis member.

member member-id—(MX Series routers and EX Series switches only) (Optional) Display chassis environmental information for the specified member of the Virtual Chassis configuration. On MX Series routers, replace member-id variable with a value of 0 or 1. For EX Series switches, see member for member ID values.

node-device name—(QFabric systems only) (Optional) Display chassis environmental information for the Node device.

pdu pdu-slot-number—(PTX Series only) (Optional) Display chassis environmental information for the specified power distribution unit.

pem—(QFX3500 switches and QFabric systems only) (Optional) Display chassis environmental information for the Power Entry Module on the specified Interconnect device or Node device.

pem pem-slot-number—(ACX Series Universal Access Routers, M120, M320, and M40e routers, MX Series routers, MX104 routers, QFX Series, and T Series routers only) (Optional) Display chassis environmental information for the Power Entry Module on the specified Power Entry Module. For information about the options, see show chassis environment pem.
**psm psm-slot-number**—(MX2020 and MX2010 routers only) (Optional) Display chassis environmental information for the power supply module. For MX2020 routers, replace `psm-slot-number` with a value from 0 through 17. For MX2010 routers, replace `psm-slot-number` with a value from 0 through 8.

**psupu-slot-number**—(EX Series switches only) (Optional) Display chassis environmental information for a specified power supply. See “EX Series Switches Hardware and CLI Terminology Mapping” on page 389 for detailed information.

**routing-engine**—(QFX3500 switches and QFabric systems only) (Optional) Display chassis environmental information for the Routing Engine on the specified Interconnect device.

**routing-engine re-slot-number**—(Optional) Display chassis environmental information for the specified Routing Engine. For information about the options, see `show chassis environment routing-engine`.

**scg**—(T Series routers only) (Optional) Display chassis environmental information about the SONET Clock Generator.

**scc**—(TX Matrix routers only) (Optional) Display chassis environmental information about the TX Matrix router (switch-card chassis).

**sfb sfb-slot-number**—(MX2020 and MX2010 routers only) (Optional) Display chassis environmental information for the power supply module. Replace `sfb-slot-number` with a value from 0 through 7.

**sfc number**—(TX Matrix Plus routers only) (Optional) Display chassis environmental information about the respective TX Matrix Plus router (switch-fabric chassis). Replace `number` variable with 0.

**sib sib-slot-number**—(M320 routers, PTX Series Packet Transport Routers, and T Series routers only) (Optional) Display chassis environmental information about the specified switch interface board. For information about the options, see `show chassis environment sib`.

---

**Required Privilege Level**

- `view`

**Related Documentation**

- `show chassis environment adc`
- `show chassis environment cb on page 824`
- `show chassis environment ccg`
- `show chassis environment cip`
- `show chassis environment fpc on page 842`
- `show chassis environment fpm`
- `show chassis environment lcc`
- `show chassis environment mcs`
- `show chassis environment monitored`
- `show chassis environment pcg`
- `show chassis environment pdu`
- `show chassis environment pem`
- `show chassis environment psm`
- `show chassis environment psu`
- `show chassis environment routing-engine` on page 867
- `show chassis environment scg`
- `show chassis environment sfb`
- `show chassis environment sib`
- `show chassis environmentafc`

**List of Sample Output**

- `show chassis environment (J2300 Router)` on page 777
- `show chassis environment (J4300 or J6300 Router)` on page 777
- `show chassis environment (M5 Router)` on page 777
- `show chassis environment (M7i Router)` on page 778
- `show chassis environment (M10 Router)` on page 778
- `show chassis environment (M10i Router)` on page 778
- `show chassis environment (M20 Router)` on page 779
- `show chassis environment (M40 Router)` on page 779
- `show chassis environment (M40e Router)` on page 779
- `show chassis environment (M120 Router)` on page 780
- `show chassis environment (M160 Router)` on page 781
- `show chassis environment (M320 Router)` on page 781
- `show chassis environment (MX104 Router)` on page 782
- `show chassis environment (MX240 Router)` on page 783
- `show chassis environment (MX240 Router with Enhanced MX SCB)` on page 784
- `show chassis environment (MX480 Router)` on page 785
- `show chassis environment (MX480 Router with Enhanced MX SCB)` on page 786
- `show chassis environment (MX960 Router)` on page 787
- `show chassis environment (MX960 Router with Enhanced MX SCB)` on page 787
- `show chassis environment (MX2020 Router)` on page 790
- `show chassis environment (MX2020 Router)` on page 799
- `show chassis environment (T320 Router)` on page 805
- `show chassis environment (T640 Router)` on page 806
- `show chassis environment (T4000 Router)` on page 806
- `show chassis environment (TX Matrix Router)` on page 808
- `show chassis environment (T1600 Router)` on page 810
- `show chassis environment (TX Matrix Plus Router)` on page 811
- `show chassis environment (TX Matrix Plus router with 3D SIBs)` on page 813
- `show chassis environment (EX4200 Standalone Switch)` on page 816
- `show chassis environment (EX8216 Switch)` on page 816
- `show chassis environment (QFX Series)` on page 817
Output Fields  Table 139 on page 776 lists the output fields for the show chassis environment command. Output fields are listed in the approximate order in which they appear.

Table 139: show chassis environment Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Information about the category or class of chassis component:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Power</strong>: Power information:</td>
</tr>
<tr>
<td></td>
<td>• (M5, M10, M20, and M40 routers and EX Series switches only) Power supply status: <strong>OK</strong>, <strong>Testing</strong>, (during initial power-on), <strong>Failed</strong>, or <strong>Absent</strong>.</td>
</tr>
<tr>
<td></td>
<td>• (M7i, M10i, M40e, M120, M160, M320, and T Series routers and EX Series switches only) Power Entry Modules status: <strong>OK</strong>, <strong>Testing</strong>, (during initial power-on), <strong>Check</strong>, <strong>Failed</strong>, or <strong>Absent</strong>.</td>
</tr>
<tr>
<td></td>
<td>• (PTX Series only) Power information is reported in PDU or PSM combinations. The status is: <strong>OK</strong>, <strong>Testing</strong>, (during initial power-on), <strong>Check</strong>, <strong>Failed</strong>, or <strong>Absent</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Temp</strong>: Temperature of air flowing through the chassis in degrees Celsius (C) and Fahrenheit (F). On PTX Series Packet Transport Routers and MX2010 and MX2020 Routers, multiple cooling zones are supported. FRU temperatures in each zone are coordinated with the fan speed of fan trays in those zones.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Pic</strong>: On ACX4000 Routers, multiple temperature channels on a MIC. The status is: <strong>OK</strong> and the <strong>Measurement</strong> is in degrees Celsius (C) and Fahrenheit (F).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fan</strong>: Fan status: <strong>OK</strong>, <strong>Testing</strong> (during initial power-on), <strong>Failed</strong>, or <strong>Absent</strong>. On PTX Series Packet Transport Routers and MX2010 and MX2020 Routers, multiple fan trays are supported. Fan status is reported in Fan Tray or Fan combinations. <strong>Measurement</strong> indicates actual fan RPM (PTX and MX2010 and MX2020 Routers only).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Misc</strong>: Information about other components of the chassis.</td>
</tr>
<tr>
<td></td>
<td>• On some routers, this field indicates the status of one or more additional components.</td>
</tr>
<tr>
<td></td>
<td>• On the M40e, M160, and M320 router, <strong>Misc</strong> includes <strong>CIP</strong> (Connector Interface Panel). <strong>OK</strong> indicates that the CIP is present. <strong>Absent</strong> indicates that the CIP is not present.</td>
</tr>
<tr>
<td></td>
<td>• On T Series routers, <strong>Misc</strong> includes <strong>CIP</strong> and <strong>SPMB</strong> (Switch Processor Mezzanine Board). <strong>OK</strong> indicates that the <strong>CIP</strong> or <strong>SPMB</strong> is present. <strong>Absent</strong> indicates that the <strong>CIP</strong> or <strong>SPMB</strong> is not present.</td>
</tr>
<tr>
<td></td>
<td>• On PTX Series Packet Transport Routers, <strong>Misc</strong> includes the <strong>SPMB</strong> (Switch Processor Mezzanine Board). The SPMB is located on the control boards. <strong>OK</strong> indicates that the control board is present. <strong>Absent</strong> indicates that the control board is not present.</td>
</tr>
<tr>
<td>Item</td>
<td>(MX2010 and MX2020 Routers) Information about the chassis component: Routing Engines, Controls Boards (CBs), Switch Fabric Boards (SFBs), PICs, Flexible PIC Concentrators (FPCs), and Adapter Cards (ADCs).</td>
</tr>
<tr>
<td>Item</td>
<td>(MX104 Routers) Information about the chassis components: Routing Engines, Control Board (CB), Power Entry Module (PEM), and Compact Forwarding Engine Board (AFEB).</td>
</tr>
</tbody>
</table>
### Table 139: show chassis environment Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Status** | (MX104, MX2010, and MX2020 Routers) Status of the specified chassis component. For example, if the Class is Fan, the fan status can be:
- **OK**: The fans are operational.
- **Testing**: The fans are being tested during initial power-on.
- **Failed**: The fans have failed or the fans are not spinning.
- **Absent**: The fan tray is not installed.

If the Class is Power, the power supply status can be:

- **OK**: The power component is operational.
- **Testing**: The power component is being tested during initial power-on.
- **Check**: There is insufficient power—-that is, fewer than the minimum required feeds are connected.
- **Failed**: The inputs leads have failed.
- **Absent**: The power component is not installed. |

| **Measurement** | (MX104, MX2010, and MX2020 Routers) Dependant on the Class. For example, if the Class is Temp, indicates the temperature in degree Celsius and degrees Fahrenheit. If the Class is Fan, indicates actual fan RPM. |

### Sample Output

**show chassis environment (J2300 Router)**

```
user@host> show chassis environment
Class Item                   Status     Measurement
Temp  Routing Engine         OK         40 degrees C / 104 degrees F
Fan   Fan                    OK         |
```

**show chassis environment (J4300 or J6300 Router)**

```
user@host> show chassis environment
Class Item                   Status     Measurement
Temp  Routing Engine         OK         41 degrees C / 105 degrees F
Fan   Fan 0                  OK         10
Fan   Fan 1                  OK         |
```

**show chassis environment (M5 Router)**

```
user@host> show chassis environment
Class Item                   Status     Measurement
Power Power Supply A         OK         30 degrees C / 86 degrees F
Power Supply B               Absent    |
Temp  FPC 0                  OK         33 degrees C / 91 degrees F
      FEB                    OK         27 degrees C / 80 degrees F
      PS Intake              OK         27 degrees C / 80 degrees F
      PS Exhaust             OK         34 degrees C / 93 degrees F
      Routing Engine         OK         |
Fans  Left Fan 1             OK         Spinning at normal speed
      Left Fan 2             OK         Spinning at normal speed
      Left Fan 3             OK         Spinning at normal speed
      Left Fan 4             OK         Spinning at normal speed
```
### show chassis environment (M7i Router)

```bash
user@host> show chassis environment
Class Item                   Status     Measurement
Power  Power Supply 0         OK
       Power Supply 1         Absent
Temp   Intake                 OK         22 degrees C / 71 degrees F
       FPC 0                  OK         23 degrees C / 73 degrees F
       Power Supplies        OK         23 degrees C / 73 degrees F
       CFEB Intake            OK         29 degrees C / 84 degrees F
       CFEB Exhaust           OK         29 degrees C / 84 degrees F
       Routing Engine         OK         26 degrees C / 78 degrees F
Fans   Fan 1                  OK         Spinning at normal speed
       Fan 2                  OK         Spinning at normal speed
       Fan 3                  OK         Spinning at normal speed
       Fan 4                  OK         Spinning at normal speed
Misc   Craft Interface        OK
```

### show chassis environment (M10 Router)

```bash
user@host> show chassis environment
Class Item                   Status     Measurement
Power  Power Supply A         OK
       Power Supply B         Failed
Temp   FPC 0                  OK         36 degrees C / 96 degrees F
       FPC 1                  OK         35 degrees C / 95 degrees F
       FEB                    OK         34 degrees C / 93 degrees F
       PS Intake              OK         31 degrees C / 87 degrees F
       PS Exhaust             OK         34 degrees C / 93 degrees F
       Routing Engine         OK         35 degrees C / 95 degrees F
Fans   Left Fan 1             OK         Spinning at normal speed
       Left Fan 2             OK         Spinning at normal speed
       Left Fan 3             OK         Spinning at normal speed
       Left Fan 4             OK         Spinning at normal speed
Misc   Craft Interface        OK
```

### show chassis environment (M10i Router)

```bash
user@host> show chassis environment
Class Item                   Status     Measurement
Power  Power Supply 0         OK
       Power Supply 1         OK
       Power Supply 2         Absent
       Power Supply 3         Absent
Temp   Intake                 OK         26 degrees C / 78 degrees F
       FPC 0                  OK         27 degrees C / 80 degrees F
       FPC 1                  OK         28 degrees C / 82 degrees F
       Lower Power Supplies   OK         29 degrees C / 84 degrees F
       Upper Power Supplies   OK         28 degrees C / 82 degrees F
       CFEB Intake            OK         27 degrees C / 80 degrees F
       CFEB Exhaust           OK         36 degrees C / 96 degrees F
       Routing Engine 0       OK         31 degrees C / 87 degrees F
       Routing Engine 1       OK         27 degrees C / 80 degrees F
Fans   Fan Tray 0 Fan 1       OK         Spinning at normal speed
       Fan Tray 0 Fan 2       OK         Spinning at normal speed
       Fan Tray 0 Fan 3       OK         Spinning at normal speed
       Fan Tray 0 Fan 4       OK         Spinning at normal speed
       Fan Tray 0 Fan 5       OK         Spinning at normal speed
```
### show chassis environment (M20 Router)

```
user@host> show chassis environment
Class     Item                   Status     Measurement
Power     Power Supply A         OK         Spinning at normal speed
Power     Power Supply B         Absent
Temp      FPC 0                  OK         28 degrees C / 82 degrees F
Temp      FPC 1                  OK         27 degrees C / 80 degrees F
Temp      Power Supply A         OK         22 degrees C / 71 degrees F
Temp      Power Supply B         Absent
Temp      SSB 0                  OK         30 degrees C / 86 degrees F
Temp      Backplane              OK         22 degrees C / 71 degrees F
Temp      Routing Engine 0       OK         26 degrees C / 78 degrees F
Temp      Routing Engine 1       Testing
Fans      Rear Fan               OK         Spinning at normal speed
Fans      Front Upper Fan        OK         Spinning at normal speed
Fans      Front Middle Fan       OK         Spinning at normal speed
Fans      Front Bottom Fan       OK         Spinning at normal speed
Misc      Craft Interface        OK
```

### show chassis environment (M40 Router)

```
user@host> show chassis environment
Class     Item                   Status     Measurement
Power     Power Supply A         OK         24 degrees C / 75 degrees F
Power     Power Supply B         Absent
Temp      FPC 3                  OK         26 degrees C / 78 degrees F
Temp      FPC 6                  OK         24 degrees C / 75 degrees F
Temp      SCB                    OK         26 degrees C / 78 degrees F
Temp      Backplane @ A1         OK         28 degrees C / 82 degrees F
Temp      Backplane @ A2         OK         23 degrees C / 73 degrees F
Temp      Routing Engine         OK         26 degrees C / 78 degrees F
Fans      Top Impeller           OK         Spinning at normal speed
Fans      Bottom impeller        OK         Spinning at normal speed
Fans      Rear Left Fan          OK         Spinning at normal speed
Fans      Rear Center Fan        OK         Spinning at normal speed
Fans      Rear Right Fan         OK         Spinning at normal speed
Misc      Craft Interface        OK
```

### show chassis environment (M40e Router)

```
user@host> show chassis environment
Class     Item                   Status     Measurement
Power     PEM 0                  OK         44 degrees C / 111 degrees F
Power     PEM 1                  Absent
Temp      PCG 0                  OK         47 degrees C / 116 degrees F
Temp      PCG 1                  OK         44 degrees C / 111 degrees F
```
<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>OK</td>
<td>43 degrees C / 109 degrees F</td>
</tr>
<tr>
<td></td>
<td>PEM 1</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Intake</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Exhaust A</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Exhaust B</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Intake</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Exhaust A</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Exhaust B</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td></td>
<td>FEB 3 Intake</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td></td>
<td>FEB 3 Exhaust A</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>FEB 3 Exhaust B</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>FEB 4 Intake</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td></td>
<td>FEB 4 Exhaust A</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>FEB 4 Exhaust B</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 Exhaust A</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 Exhaust B</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 3 Exhaust A</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 3 Exhaust B</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 4 Exhaust A</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 4 Exhaust B</td>
<td>OK</td>
<td>30 degrees C / 86 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td>Front Top Tray Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Top Tray Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Top Tray Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Top Tray Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Top Tray Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Top Tray Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Top Tray Fan 7</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Top Tray Fan 8</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
### show chassis environment (M160 Router)

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>PEM 0</td>
<td>OK</td>
<td>Absent</td>
</tr>
<tr>
<td>Temp</td>
<td>PCG 0</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>PCG 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCS 0</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 0 SPP</td>
<td>OK</td>
<td>47 degrees C / 116 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 0 SPR</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 1 SPP</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 1 SPR</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 2 SPP</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 2 SPR</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 3 SPP</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>SFM 3 SPR</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 6</td>
<td>OK</td>
<td>43 degrees C / 109 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPM OMB</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPM Display</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td>Rear Bottom Blower</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Top Blower</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Front Bottom Blower</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Fan Tray Rear Left</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Fan Tray Rear Right</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Fan Tray Front Left</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Fan Tray Front Right</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Misc</td>
<td>CIP</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

### show chassis environment (M320 Router)

```
user@host> show chassis environment
```
<table>
<thead>
<tr>
<th>Class Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>Absent</td>
</tr>
<tr>
<td></td>
<td>PEM 1</td>
<td>Absent</td>
</tr>
<tr>
<td></td>
<td>PEM 2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>PEM 3</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>Absent</td>
</tr>
<tr>
<td></td>
<td>CB 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>CB 1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 3</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 2 Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 2 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 3 Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 3 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 6 Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 6 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 6 Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 6 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPM GBUS</td>
<td>OK</td>
</tr>
<tr>
<td>Fan</td>
<td>Top Left Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Top Right Rear fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Top Right Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Rear fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Rear fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Fan 1 (TOP)</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Fan 2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Fan 3</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Fan 4</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Fan 5</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Fan 6</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Fan 7 (Bottom)</td>
<td>OK</td>
</tr>
<tr>
<td>Misc</td>
<td>CIP</td>
<td>OK</td>
</tr>
</tbody>
</table>

show chassis environment (MX104 Router)
Fans  Fan 1                          OK         Spinning at normal speed
        Fan 2                          OK         Spinning at normal speed
        Fan 3                          OK         Spinning at normal speed
        Fan 4                          OK         Spinning at normal speed
        Fan 5                          OK         Spinning at normal speed

show chassis environment (MX240 Router)

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td></td>
<td>PEM 1</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>PEM 2</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PEM 3</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Intake</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Exhaust A</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Exhaust B</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 ACBC</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 SF A</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 SF B</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Intake</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Exhaust A</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Exhaust B</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 ACBC</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 SF A</td>
<td>OK</td>
<td>47 degrees C / 116 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 SF B</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Intake</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Exhaust A</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Exhaust B</td>
<td>OK</td>
<td>53 degrees C / 127 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 0 TSensor</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 0 Chip</td>
<td>OK</td>
<td>53 degrees C / 127 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 1 TSensor</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 1 Chip</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 2 TSensor</td>
<td>OK</td>
<td>47 degrees C / 116 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 2 Chip</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 3 TSensor</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 3 Chip</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 0 TSensor</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 0 Chip</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 1 TSensor</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 1 Chip</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 Intake</td>
<td>OK</td>
<td>52 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 Exhaust A</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 Exhaust B</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 0 TSensor</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 0 Chip</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 1 TSensor</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 1 Chip</td>
<td>OK</td>
<td>55 degrees C / 131 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 2 TSensor</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 2 Chip</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 3 TSensor</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 I3 3 Chip</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 IA 0 TSensor</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 IA 0 Chip</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 IA 1 TSensor</td>
<td>OK</td>
<td>47 degrees C / 116 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 2 IA 1 Chip</td>
<td>OK</td>
<td>53 degrees C / 127 degrees F</td>
</tr>
</tbody>
</table>

Fans  Front Fan                      OK         Spinning at normal speed
show chassis environment (MX240 Router with Enhanced MX SCB)

```
user@host>  show chassis environment

Class        Item                          Status     Measurement          
Temp  PEM 0                          OK         40 degrees C / 104 degrees F
      PEM 1                          OK         45 degrees C / 113 degrees F
      PEM 2                          Absent
      PEM 3                          Absent
Routing Engine 0               OK         39 degrees C / 102 degrees F
Routing Engine 1               OK         37 degrees C / 98 degrees F
CB 0 Intake                    OK         36 degrees C / 96 degrees F
CB 0 Exhaust A                 OK         34 degrees C / 93 degrees F
CB 0 Exhaust B                 OK         38 degrees C / 100 degrees F
CB 0 ACBC                      OK         37 degrees C / 98 degrees F
CB 0 XF A                      OK         49 degrees C / 120 degrees F
CB 0 XF B                      OK         41 degrees C / 105 degrees F
CB 1 Intake                    OK         37 degrees C / 98 degrees F
CB 1 Exhaust A                 OK         34 degrees C / 93 degrees F
CB 1 Exhaust B                 OK         39 degrees C / 102 degrees F
CB 1 ACBC                      OK         38 degrees C / 100 degrees F
CB 1 XF A                      OK         47 degrees C / 116 degrees F
CB 1 XF B                      OK         41 degrees C / 105 degrees F
FPC 1 Intake                   OK         33 degrees C / 91 degrees F
FPC 1 Exhaust A                OK         38 degrees C / 100 degrees F
FPC 1 Exhaust B                OK         53 degrees C / 127 degrees F
FPC 1 I3 0 TSensor             OK         50 degrees C / 122 degrees F
FPC 1 I3 0 Chip                OK         53 degrees C / 127 degrees F
FPC 1 I3 1 TSensor             OK         49 degrees C / 120 degrees F
FPC 1 I3 1 Chip                OK         52 degrees C / 125 degrees F
FPC 1 I3 2 TSensor             OK         47 degrees C / 116 degrees F
FPC 1 I3 2 Chip                OK         49 degrees C / 120 degrees F
FPC 1 I3 3 TSensor             OK         44 degrees C / 111 degrees F
FPC 1 I3 3 Chip                OK         46 degrees C / 114 degrees F
FPC 1 IA 0 TSensor             OK         45 degrees C / 113 degrees F
FPC 1 IA 0 Chip                OK         44 degrees C / 111 degrees F
FPC 1 IA 1 TSensor             OK         44 degrees C / 111 degrees F
FPC 1 IA 1 Chip                OK         48 degrees C / 118 degrees F
FPC 2 Intake                   OK         32 degrees C / 89 degrees F
FPC 2 Exhaust A                OK         40 degrees C / 104 degrees F
FPC 2 Exhaust B                OK         52 degrees C / 125 degrees F
FPC 2 I3 0 TSensor             OK         52 degrees C / 125 degrees F
FPC 2 I3 0 Chip                OK         56 degrees C / 132 degrees F
FPC 2 I3 1 TSensor             OK         52 degrees C / 125 degrees F
FPC 2 I3 1 Chip                OK         55 degrees C / 131 degrees F
FPC 2 I3 2 TSensor             OK         49 degrees C / 120 degrees F
FPC 2 I3 2 Chip                OK         52 degrees C / 125 degrees F
FPC 2 I3 3 TSensor             OK         44 degrees C / 111 degrees F
FPC 2 I3 3 Chip                OK         48 degrees C / 118 degrees F
FPC 2 IA 0 TSensor             OK         50 degrees C / 122 degrees F
FPC 2 IA 0 Chip                OK         48 degrees C / 118 degrees F
FPC 2 IA 1 TSensor             OK         47 degrees C / 116 degrees F
FPC 2 IA 1 Chip                OK         53 degrees C / 127 degrees F
Fans  Front Fan                  OK         Spinning at normal speed
        Middle Fan                 OK         Spinning at normal speed
        Rear Fan                   OK         Spinning at normal speed
```
### show chassis environment (MX480 Router)

```text
user@host> show chassis environment

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td></td>
<td>PEM 1</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td></td>
<td>PEM 2</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PEM 3</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Intake</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Exhaust A</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Exhaust B</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 ACBC</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 SF A</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 SF B</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Intake</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Exhaust A</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Exhaust B</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 ACBC</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 SF A</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 SF B</td>
<td>OK</td>
<td>43 degrees C / 109 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Intake</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Exhaust A</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Exhaust B</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 I3 0 TSensor</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 I3 1 TSensor</td>
<td>OK</td>
<td>47 degrees C / 116 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 I3 1 Chip</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 I3 2 TSensor</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 I3 2 Chip</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 I3 3 TSensor</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 I3 3 Chip</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 IA 0 TSensor</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 IA 0 Chip</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 IA 1 TSensor</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 IA 1 Chip</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Intake</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Exhaust A</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Exhaust B</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 0 TSensor</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 0 Chip</td>
<td>OK</td>
<td>57 degrees C / 134 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 1 TSensor</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 1 Chip</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 2 TSensor</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 3 TSensor</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 I3 3 Chip</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 0 TSensor</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 0 Chip</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 1 TSensor</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 IA 1 Chip</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td>Top Rear Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Rear Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Middle Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Middle Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Front Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Front Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
```
### show chassis environment (MX480 Router with Enhanced MX SCB)

```
user@host> show chassis environment

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td>PEM 1</td>
<td>OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PEM 2</td>
<td>Absent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PEM 3</td>
<td>Absent</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>CB 0</td>
<td>Intake</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>CB 0</td>
<td>Exhaust A</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>CB 0</td>
<td>Exhaust B</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>CB 0</td>
<td>ACBC</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td>CB 0</td>
<td>XF A</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>CB 0</td>
<td>XF B</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>CB 1</td>
<td>Intake</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>CB 1</td>
<td>Exhaust A</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>CB 1</td>
<td>Exhaust B</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td>CB 1</td>
<td>ACBC</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td>CB 1</td>
<td>XF A</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td>CB 1</td>
<td>XF B</td>
<td>OK</td>
<td>43 degrees C / 109 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>Intake</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>Exhaust A</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>Exhaust B</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>I3 0 TSensor</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>I3 0 Chip</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>I3 1 TSensor</td>
<td>OK</td>
<td>47 degrees C / 116 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>I3 1 Chip</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>I3 2 TSensor</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>I3 3 TSensor</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>I3 3 Chip</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>IA 0 TSensor</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>IA 0 Chip</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>IA 1 TSensor</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>FPC 0</td>
<td>IA 1 Chip</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>Intake</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>Exhaust A</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>Exhaust B</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>I3 0 TSensor</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>I3 0 Chip</td>
<td>OK</td>
<td>57 degrees C / 134 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>I3 1 TSensor</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>I3 1 Chip</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>I3 2 TSensor</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>I3 3 TSensor</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>I3 3 Chip</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>IA 0 TSensor</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>IA 0 Chip</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>IA 1 TSensor</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td>FPC 1</td>
<td>IA 1 Chip</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td>Top Rear Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Rear Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Middle Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Middle Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Front Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Front Fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

```

786  Copyright © 2013, Juniper Networks, Inc.
show chassis environment (MX960 Router)

```
user@host> show chassis environment
Class Item                           Status     Measurement
Temp  PEM 0                          Absent
PEM 1                          Absent
PEM 2                          Check
PEM 3                          OK         35 degrees C / 95 degrees F
Routing Engine 0               OK         37 degrees C / 98 degrees F
Routing Engine 1               Absent
CB 0 Intake                    OK         24 degrees C / 75 degrees F
CB 0 Exhaust A                 OK         30 degrees C / 86 degrees F
CB 0 Exhaust B                 OK         27 degrees C / 80 degrees F
CB 1 Intake                    Absent
CB 1 Exhaust A                 Absent
CB 1 Exhaust B                 Absent
CB 1 ACBC                      Absent
CB 1 SF A                       Absent
CB 1 SF B                       Absent
CB 2 Intake                    Absent
CB 2 Exhaust A                 Absent
CB 2 Exhaust B                 Absent
CB 2 ACBC                      Absent
CB 2 SF A                       Absent
CB 2 SF B                       Absent
FPC 4 Intake                   OK         24 degrees C / 75 degrees F
FPC 4 Exhaust A                OK         36 degrees C / 96 degrees F
FPC 4 Exhaust B                OK         38 degrees C / 100 degrees F
FPC 7 Intake                   OK         24 degrees C / 75 degrees F
FPC 7 Exhaust A                OK         36 degrees C / 96 degrees F
FPC 7 Exhaust B                OK         42 degrees C / 107 degrees F
Fans  Top Fan Tray Temp              Failed
Top Tray Fan 1                 OK         Spinning at normal speed
Top Tray Fan 2                 OK         Spinning at normal speed
Top Tray Fan 3                 OK         Spinning at normal speed
Top Tray Fan 4                 OK         Spinning at normal speed
Top Tray Fan 5                 OK         Spinning at normal speed
Top Tray Fan 6                 OK         Spinning at normal speed
Bottom Tray Fan Tray Temp         Failed
Bottom Tray Fan 1               OK         Spinning at normal speed
Bottom Tray Fan 2               OK         Spinning at normal speed
Bottom Tray Fan 3               OK         Spinning at normal speed
Bottom Tray Fan 4               OK         Spinning at normal speed
Bottom Tray Fan 5               OK         Spinning at normal speed
Bottom Tray Fan 6               OK         Spinning at normal speed
```
<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
<th>Temperature (°C/°F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CB 0 ACBC</td>
<td>OK</td>
<td>38 / 100</td>
</tr>
<tr>
<td>CB 0 XF A</td>
<td>OK</td>
<td>53 / 127</td>
</tr>
<tr>
<td>CB 0 XF B</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>CB 1 Intake</td>
<td>OK</td>
<td>35 / 95</td>
</tr>
<tr>
<td>CB 1 Exhaust A</td>
<td>OK</td>
<td>35 / 95</td>
</tr>
<tr>
<td>CB 1 Exhaust B</td>
<td>OK</td>
<td>41 / 105</td>
</tr>
<tr>
<td>CB 1 ACBC</td>
<td>OK</td>
<td>38 / 100</td>
</tr>
<tr>
<td>CB 1 XF A</td>
<td>OK</td>
<td>52 / 125</td>
</tr>
<tr>
<td>CB 1 XF B</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>CB 2 Intake</td>
<td>OK</td>
<td>32 / 89</td>
</tr>
<tr>
<td>CB 2 Exhaust A</td>
<td>OK</td>
<td>30 / 86</td>
</tr>
<tr>
<td>CB 2 Exhaust B</td>
<td>OK</td>
<td>35 / 95</td>
</tr>
<tr>
<td>CB 2 ACBC</td>
<td>OK</td>
<td>33 / 91</td>
</tr>
<tr>
<td>CB 2 XF A</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>CB 2 XF B</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 0 Intake</td>
<td>OK</td>
<td>35 / 95</td>
</tr>
<tr>
<td>FPC 0 Exhaust A</td>
<td>OK</td>
<td>39 / 102</td>
</tr>
<tr>
<td>FPC 0 Exhaust B</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 0 I3 0 TSensor</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 0 I3 0 Chip</td>
<td>OK</td>
<td>56 / 132</td>
</tr>
<tr>
<td>FPC 0 I3 1 TSensor</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 0 I3 1 Chip</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 0 I3 2 TSensor</td>
<td>OK</td>
<td>45 / 113</td>
</tr>
<tr>
<td>FPC 0 I3 2 Chip</td>
<td>OK</td>
<td>48 / 118</td>
</tr>
<tr>
<td>FPC 0 I3 3 TSensor</td>
<td>OK</td>
<td>41 / 105</td>
</tr>
<tr>
<td>FPC 0 I3 3 Chip</td>
<td>OK</td>
<td>44 / 111</td>
</tr>
<tr>
<td>FPC 0 IA 0 TSensor</td>
<td>OK</td>
<td>45 / 113</td>
</tr>
<tr>
<td>FPC 0 IA 0 Chip</td>
<td>OK</td>
<td>45 / 113</td>
</tr>
<tr>
<td>FPC 1 Intake</td>
<td>OK</td>
<td>36 / 96</td>
</tr>
<tr>
<td>FPC 1 Exhaust A</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 1 Exhaust B</td>
<td>OK</td>
<td>43 / 109</td>
</tr>
<tr>
<td>FPC 1 LU 0 TCAM TSensor</td>
<td>OK</td>
<td>53 / 127</td>
</tr>
<tr>
<td>FPC 1 LU 0 TCAM Chip</td>
<td>OK</td>
<td>57 / 134</td>
</tr>
<tr>
<td>FPC 1 LU 0 TSensor</td>
<td>OK</td>
<td>53 / 127</td>
</tr>
<tr>
<td>FPC 1 LU 0 Chip</td>
<td>OK</td>
<td>60 / 140</td>
</tr>
<tr>
<td>FPC 1 MQ 0 TSensor</td>
<td>OK</td>
<td>53 / 127</td>
</tr>
<tr>
<td>FPC 1 MQ 0 Chip</td>
<td>OK</td>
<td>56 / 132</td>
</tr>
<tr>
<td>FPC 1 LU 1 TCAM TSensor</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 1 LU 1 TCAM Chip</td>
<td>OK</td>
<td>52 / 125</td>
</tr>
<tr>
<td>FPC 1 LU 1 TSensor</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 1 LU 1 Chip</td>
<td>OK</td>
<td>53 / 127</td>
</tr>
<tr>
<td>FPC 1 MQ 1 TSensor</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 1 MQ 1 Chip</td>
<td>OK</td>
<td>58 / 136</td>
</tr>
<tr>
<td>FPC 2 Intake</td>
<td>OK</td>
<td>35 / 95</td>
</tr>
<tr>
<td>FPC 2 Exhaust A</td>
<td>OK</td>
<td>39 / 102</td>
</tr>
<tr>
<td>FPC 2 Exhaust B</td>
<td>OK</td>
<td>54 / 129</td>
</tr>
<tr>
<td>FPC 2 I3 0 TSensor</td>
<td>OK</td>
<td>52 / 125</td>
</tr>
<tr>
<td>FPC 2 I3 0 Chip</td>
<td>OK</td>
<td>59 / 138</td>
</tr>
<tr>
<td>FPC 2 I3 1 TSensor</td>
<td>OK</td>
<td>48 / 118</td>
</tr>
<tr>
<td>FPC 2 I3 1 Chip</td>
<td>OK</td>
<td>52 / 125</td>
</tr>
<tr>
<td>FPC 2 I3 2 TSensor</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 2 I3 2 Chip</td>
<td>OK</td>
<td>49 / 120</td>
</tr>
<tr>
<td>FPC 2 I3 3 TSensor</td>
<td>OK</td>
<td>41 / 105</td>
</tr>
<tr>
<td>FPC 2 I3 3 Chip</td>
<td>OK</td>
<td>44 / 111</td>
</tr>
<tr>
<td>FPC 2 IA 0 TSensor</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 2 IA 0 Chip</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 2 IA 1 TSensor</td>
<td>OK</td>
<td>45 / 113</td>
</tr>
<tr>
<td>FPC 2 IA 1 Chip</td>
<td>OK</td>
<td>49 / 120</td>
</tr>
<tr>
<td>FPC 3 Intake</td>
<td>OK</td>
<td>34 / 93</td>
</tr>
<tr>
<td>Component</td>
<td>Status</td>
<td>Temperature C</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------</td>
<td>---------------</td>
</tr>
<tr>
<td>FPC 3 Exhaust A</td>
<td>OK</td>
<td>34</td>
</tr>
<tr>
<td>FPC 3 Exhaust B</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 3 I3 0 TSensor</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 3 I3 0 Chip</td>
<td>OK</td>
<td>52</td>
</tr>
<tr>
<td>FPC 3 I3 1 TSensor</td>
<td>OK</td>
<td>46</td>
</tr>
<tr>
<td>FPC 3 I3 1 Chip</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 3 IA 0 TSensor</td>
<td>OK</td>
<td>41</td>
</tr>
<tr>
<td>FPC 3 IA 0 Chip</td>
<td>OK</td>
<td>40</td>
</tr>
<tr>
<td>FPC 5 Intake</td>
<td>OK</td>
<td>42</td>
</tr>
<tr>
<td>FPC 5 Exhaust A</td>
<td>OK</td>
<td>42</td>
</tr>
<tr>
<td>FPC 5 Exhaust B</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 5 LU 0 TSensor</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 5 LU 0 Chip</td>
<td>OK</td>
<td>54</td>
</tr>
<tr>
<td>FPC 5 LU 1 TSensor</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 5 LU 1 Chip</td>
<td>OK</td>
<td>61</td>
</tr>
<tr>
<td>FPC 5 LU 2 TSensor</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 5 LU 2 Chip</td>
<td>OK</td>
<td>51</td>
</tr>
<tr>
<td>FPC 5 LU 3 TSensor</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 5 LU 3 Chip</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 5 MQ 0 TSensor</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 5 MQ 0 Chip</td>
<td>OK</td>
<td>52</td>
</tr>
<tr>
<td>FPC 5 MQ 1 TSensor</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 5 MQ 1 Chip</td>
<td>OK</td>
<td>52</td>
</tr>
<tr>
<td>FPC 5 MQ 2 TSensor</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 5 MQ 2 Chip</td>
<td>OK</td>
<td>46</td>
</tr>
<tr>
<td>FPC 5 MQ 3 TSensor</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 5 MQ 3 Chip</td>
<td>OK</td>
<td>45</td>
</tr>
<tr>
<td>FPC 7 Intake</td>
<td>OK</td>
<td>36</td>
</tr>
<tr>
<td>FPC 7 Exhaust A</td>
<td>OK</td>
<td>35</td>
</tr>
<tr>
<td>FPC 7 Exhaust B</td>
<td>OK</td>
<td>33</td>
</tr>
<tr>
<td>FPC 7 LU 0 TSensor</td>
<td>OK</td>
<td>42</td>
</tr>
<tr>
<td>FPC 7 LU 0 Chip</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 7 MQ 0 TSensor</td>
<td>OK</td>
<td>42</td>
</tr>
<tr>
<td>FPC 7 MQ 0 Chip</td>
<td>OK</td>
<td>45</td>
</tr>
<tr>
<td>FPC 8 Intake</td>
<td>OK</td>
<td>33</td>
</tr>
<tr>
<td>FPC 8 Exhaust A</td>
<td>OK</td>
<td>36</td>
</tr>
<tr>
<td>FPC 8 Exhaust B</td>
<td>OK</td>
<td>36</td>
</tr>
<tr>
<td>FPC 8 I3 0 TSensor</td>
<td>OK</td>
<td>38</td>
</tr>
<tr>
<td>FPC 8 I3 0 Chip</td>
<td>OK</td>
<td>43</td>
</tr>
<tr>
<td>FPC 8 BDS 0 TSensor</td>
<td>OK</td>
<td>37</td>
</tr>
<tr>
<td>FPC 8 BDS 0 Chip</td>
<td>OK</td>
<td>36</td>
</tr>
<tr>
<td>FPC 8 IA 0 TSensor</td>
<td>OK</td>
<td>37</td>
</tr>
<tr>
<td>FPC 8 IA 0 Chip</td>
<td>OK</td>
<td>37</td>
</tr>
<tr>
<td>FPC 10 Intake</td>
<td>OK</td>
<td>38</td>
</tr>
<tr>
<td>FPC 10 Exhaust A</td>
<td>OK</td>
<td>36</td>
</tr>
<tr>
<td>FPC 10 Exhaust B</td>
<td>OK</td>
<td>41</td>
</tr>
<tr>
<td>FPC 10 I3 0 TSensor</td>
<td>OK</td>
<td>40</td>
</tr>
<tr>
<td>FPC 10 I3 0 Chip</td>
<td>OK</td>
<td>42</td>
</tr>
<tr>
<td>FPC 10 I3 1 TSensor</td>
<td>OK</td>
<td>40</td>
</tr>
<tr>
<td>FPC 10 I3 1 Chip</td>
<td>OK</td>
<td>44</td>
</tr>
<tr>
<td>FPC 10 I3 2 TSensor</td>
<td>OK</td>
<td>42</td>
</tr>
<tr>
<td>FPC 10 I3 2 Chip</td>
<td>OK</td>
<td>43</td>
</tr>
<tr>
<td>FPC 10 I3 3 TSensor</td>
<td>OK</td>
<td>39</td>
</tr>
<tr>
<td>FPC 10 I3 3 Chip</td>
<td>OK</td>
<td>44</td>
</tr>
<tr>
<td>FPC 10 IA 0 TSensor</td>
<td>OK</td>
<td>36</td>
</tr>
<tr>
<td>FPC 10 IA 0 Chip</td>
<td>OK</td>
<td>36</td>
</tr>
<tr>
<td>FPC 10 IA 1 TSensor</td>
<td>OK</td>
<td>43</td>
</tr>
</tbody>
</table>
### show chassis environment (MX2020 Router)

<table>
<thead>
<tr>
<th>Class Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSM 0</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>PSM 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>PSM 2</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>PSM 3</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>PSM 4</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>PSM 5</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>PSM 6</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>PSM 7</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>PSM 8</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td>PSM 9</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>PSM 10</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>PSM 11</td>
<td>OK</td>
<td>47 degrees C / 116 degrees F</td>
</tr>
<tr>
<td>PSM 12</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>PSM 13</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>PSM 14</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>PSM 15</td>
<td>OK</td>
<td>43 degrees C / 109 degrees F</td>
</tr>
<tr>
<td>PSM 16</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td>PSM 17</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>PDM 0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>PDM 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>PDM 2</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>PDM 3</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>CB 0 IntakeA-Zone0</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>CB 0 IntakeB-Zone1</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td>CB 0 IntakeC-Zone0</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td>CB 0 ExhaustA-Zone0</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>CB 0 ExhaustB-Zone1</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td>CB 0 TCBC-Zone0</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>CB 1 IntakeA-Zone0</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>CB 1 IntakeB-Zone1</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td>CB 1 IntakeC-Zone0</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>CB 1 ExhaustA-Zone0</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>CB 1 ExhaustB-Zone1</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>CB 1 TCBC-Zone0</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>SPMB 0 Intake</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td>SPMB 1 Intake</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td>Routing Engine 0</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td>Routing Engine 0 CPU</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td>Routing Engine 1</td>
<td>OK</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>Routing Engine 1 CPU</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td>SFB 0 Intake-Zone0</td>
<td>OK</td>
<td>55 degrees C / 131 degrees F</td>
</tr>
<tr>
<td>Device Type</td>
<td>Device ID</td>
<td>Status</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>SFB 7</td>
<td>SFB-XF1-Zone0</td>
<td>OK</td>
</tr>
<tr>
<td>SFB 7</td>
<td>SFB-XF0-Zone0</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>Intake</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>Exhaust A</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>Exhaust B</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 0 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 0 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 1 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 1 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 2 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 2 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 3 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>LU 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 0 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 0 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 1 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 1 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 2 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 2 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 3 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 0</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>Intake</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>Exhaust A</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>Exhaust B</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 0 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 0 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 1 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 1 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 2 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 2 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 3 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>LU 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 0 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 0 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 1 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 1 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 2 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 2 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 1</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>Intake</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>Exhaust A</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>Exhaust B</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 0 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 0 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 1 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 1 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 2 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 2 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 3 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>LU 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 0 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 0 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 1 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 1 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 2 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 2 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 3 TSen</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 2</td>
<td>MQ 3 Chip</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 3</td>
<td>Intake</td>
<td>OK</td>
</tr>
<tr>
<td>FPC 3</td>
<td>Exhaust A</td>
<td>OK</td>
</tr>
<tr>
<td>Device Type</td>
<td>Status</td>
<td>Temperature (°C)</td>
</tr>
<tr>
<td>-------------</td>
<td>--------</td>
<td>-----------------</td>
</tr>
<tr>
<td>FPC 3 Exhaust B</td>
<td>OK</td>
<td>61</td>
</tr>
<tr>
<td>FPC 3 LU 0 TSen</td>
<td>OK</td>
<td>58</td>
</tr>
<tr>
<td>FPC 3 LU 0 Chip</td>
<td>OK</td>
<td>61</td>
</tr>
<tr>
<td>FPC 3 LU 1 TSen</td>
<td>OK</td>
<td>58</td>
</tr>
<tr>
<td>FPC 3 LU 1 Chip</td>
<td>OK</td>
<td>62</td>
</tr>
<tr>
<td>FPC 3 LU 2 TSen</td>
<td>OK</td>
<td>58</td>
</tr>
<tr>
<td>FPC 3 LU 2 Chip</td>
<td>OK</td>
<td>51</td>
</tr>
<tr>
<td>FPC 3 LU 3 TSen</td>
<td>OK</td>
<td>58</td>
</tr>
<tr>
<td>FPC 3 LU 3 Chip</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 3 MQ 0 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 3 MQ 0 Chip</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 3 MQ 1 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 3 MQ 1 Chip</td>
<td>OK</td>
<td>54</td>
</tr>
<tr>
<td>FPC 3 MQ 2 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 3 MQ 2 Chip</td>
<td>OK</td>
<td>45</td>
</tr>
<tr>
<td>FPC 3 MQ 3 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 3 MQ 3 Chip</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 4 Intake</td>
<td>OK</td>
<td>40</td>
</tr>
<tr>
<td>FPC 4 Exhaust A</td>
<td>OK</td>
<td>49</td>
</tr>
<tr>
<td>FPC 4 Exhaust B</td>
<td>OK</td>
<td>62</td>
</tr>
<tr>
<td>FPC 4 LU 0 TSen</td>
<td>OK</td>
<td>59</td>
</tr>
<tr>
<td>FPC 4 LU 0 Chip</td>
<td>OK</td>
<td>62</td>
</tr>
<tr>
<td>FPC 4 LU 1 TSen</td>
<td>OK</td>
<td>59</td>
</tr>
<tr>
<td>FPC 4 LU 1 Chip</td>
<td>OK</td>
<td>65</td>
</tr>
<tr>
<td>FPC 4 LU 2 TSen</td>
<td>OK</td>
<td>59</td>
</tr>
<tr>
<td>FPC 4 LU 2 Chip</td>
<td>OK</td>
<td>51</td>
</tr>
<tr>
<td>FPC 4 LU 3 TSen</td>
<td>OK</td>
<td>59</td>
</tr>
<tr>
<td>FPC 4 LU 3 Chip</td>
<td>OK</td>
<td>65</td>
</tr>
<tr>
<td>FPC 4 MQ 0 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 4 MQ 0 Chip</td>
<td>OK</td>
<td>52</td>
</tr>
<tr>
<td>FPC 4 MQ 1 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 4 MQ 1 Chip</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 4 MQ 2 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 4 MQ 2 Chip</td>
<td>OK</td>
<td>46</td>
</tr>
<tr>
<td>FPC 4 MQ 3 TSen</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 4 MQ 3 Chip</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 5 Intake</td>
<td>OK</td>
<td>41</td>
</tr>
<tr>
<td>FPC 5 Exhaust A</td>
<td>OK</td>
<td>50</td>
</tr>
<tr>
<td>FPC 5 Exhaust B</td>
<td>OK</td>
<td>63</td>
</tr>
<tr>
<td>FPC 5 LU 0 TSen</td>
<td>OK</td>
<td>60</td>
</tr>
<tr>
<td>FPC 5 LU 0 Chip</td>
<td>OK</td>
<td>63</td>
</tr>
<tr>
<td>FPC 5 LU 1 TSen</td>
<td>OK</td>
<td>60</td>
</tr>
<tr>
<td>FPC 5 LU 1 Chip</td>
<td>OK</td>
<td>66</td>
</tr>
<tr>
<td>FPC 5 LU 2 TSen</td>
<td>OK</td>
<td>60</td>
</tr>
<tr>
<td>FPC 5 LU 2 Chip</td>
<td>OK</td>
<td>56</td>
</tr>
<tr>
<td>FPC 5 LU 3 TSen</td>
<td>OK</td>
<td>60</td>
</tr>
<tr>
<td>FPC 5 LU 3 Chip</td>
<td>OK</td>
<td>54</td>
</tr>
<tr>
<td>FPC 5 MQ 0 TSen</td>
<td>OK</td>
<td>49</td>
</tr>
<tr>
<td>FPC 5 MQ 0 Chip</td>
<td>OK</td>
<td>52</td>
</tr>
<tr>
<td>FPC 5 MQ 1 TSen</td>
<td>OK</td>
<td>49</td>
</tr>
<tr>
<td>FPC 5 MQ 1 Chip</td>
<td>OK</td>
<td>53</td>
</tr>
<tr>
<td>FPC 5 MQ 2 TSen</td>
<td>OK</td>
<td>49</td>
</tr>
<tr>
<td>FPC 5 MQ 2 Chip</td>
<td>OK</td>
<td>48</td>
</tr>
<tr>
<td>FPC 5 MQ 3 TSen</td>
<td>OK</td>
<td>49</td>
</tr>
<tr>
<td>FPC 5 MQ 3 Chip</td>
<td>OK</td>
<td>47</td>
</tr>
<tr>
<td>FPC 6 Intake</td>
<td>OK</td>
<td>42</td>
</tr>
<tr>
<td>FPC 6 Exhaust A</td>
<td>OK</td>
<td>51</td>
</tr>
<tr>
<td>FPC 6 Exhaust B</td>
<td>OK</td>
<td>63</td>
</tr>
<tr>
<td>FPC 6 LU 0 TSen</td>
<td>OK</td>
<td>61</td>
</tr>
<tr>
<td>FPC 6 LU 0 Chip</td>
<td>OK</td>
<td>64</td>
</tr>
<tr>
<td>FPC 6 LU 1 TSen</td>
<td>OK</td>
<td>61</td>
</tr>
</tbody>
</table>
FPC 6 LU 1 Chip   OK   66 degrees C / 150 degrees F
FPC 6 LU 2 TSen    OK   61 degrees C / 141 degrees F
FPC 6 LU 2 Chip    OK   56 degrees C / 132 degrees F
FPC 6 LU 3 TSen    OK   61 degrees C / 141 degrees F
FPC 6 LU 3 Chip    OK   56 degrees C / 132 degrees F
FPC 6 MQ 0 TSen    OK   50 degrees C / 122 degrees F
FPC 6 MQ 0 Chip    OK   56 degrees C / 132 degrees F
FPC 6 MQ 1 TSen    OK   50 degrees C / 122 degrees F
FPC 6 MQ 1 Chip    OK   59 degrees C / 138 degrees F
FPC 6 MQ 2 TSen    OK   50 degrees C / 122 degrees F
FPC 6 MQ 2 Chip    OK   49 degrees C / 120 degrees F
FPC 6 MQ 3 TSen    OK   49 degrees C / 120 degrees F
FPC 6 MQ 3 Chip    OK   49 degrees C / 120 degrees F
FPC 7 Intake       OK   41 degrees C / 105 degrees F
FPC 7 Exhaust A    OK   51 degrees C / 123 degrees F
FPC 7 Exhaust B    OK   63 degrees C / 145 degrees F
FPC 7 LU 0 TSen    OK   60 degrees C / 140 degrees F
FPC 7 LU 0 Chip    OK   61 degrees C / 141 degrees F
FPC 7 LU 1 TSen    OK   60 degrees C / 140 degrees F
FPC 7 LU 1 Chip    OK   65 degrees C / 149 degrees F
FPC 7 LU 2 TSen    OK   60 degrees C / 140 degrees F
FPC 7 LU 2 Chip    OK   54 degrees C / 129 degrees F
FPC 7 LU 3 TSen    OK   60 degrees C / 140 degrees F
FPC 7 LU 3 Chip    OK   53 degrees C / 127 degrees F
FPC 7 MQ 0 TSen    OK   50 degrees C / 122 degrees F
FPC 7 MQ 0 Chip    OK   53 degrees C / 127 degrees F
FPC 7 MQ 1 TSen    OK   50 degrees C / 122 degrees F
FPC 7 MQ 1 Chip    OK   54 degrees C / 129 degrees F
FPC 7 MQ 2 TSen    OK   50 degrees C / 122 degrees F
FPC 7 MQ 2 Chip    OK   47 degrees C / 116 degrees F
FPC 7 MQ 3 TSen    OK   50 degrees C / 122 degrees F
FPC 7 MQ 3 Chip    OK   47 degrees C / 116 degrees F
FPC 8 Intake       OK   41 degrees C / 105 degrees F
FPC 8 Exhaust A    OK   50 degrees C / 122 degrees F
FPC 8 Exhaust B    OK   62 degrees C / 143 degrees F
FPC 8 LU 0 TSen    OK   59 degrees C / 138 degrees F
FPC 8 LU 0 Chip    OK   62 degrees C / 143 degrees F
FPC 8 LU 1 TSen    OK   59 degrees C / 138 degrees F
FPC 8 LU 1 Chip    OK   64 degrees C / 147 degrees F
FPC 8 LU 2 TSen    OK   59 degrees C / 138 degrees F
FPC 8 LU 2 Chip    OK   55 degrees C / 131 degrees F
FPC 8 LU 3 TSen    OK   59 degrees C / 138 degrees F
FPC 8 LU 3 Chip    OK   54 degrees C / 129 degrees F
FPC 8 MQ 0 TSen    OK   49 degrees C / 120 degrees F
FPC 8 MQ 0 Chip    OK   51 degrees C / 123 degrees F
FPC 8 MQ 1 TSen    OK   49 degrees C / 120 degrees F
FPC 8 MQ 1 Chip    OK   52 degrees C / 125 degrees F
FPC 8 MQ 2 TSen    OK   49 degrees C / 120 degrees F
FPC 8 MQ 2 Chip    OK   46 degrees C / 114 degrees F
FPC 8 MQ 3 TSen    OK   49 degrees C / 120 degrees F
FPC 8 MQ 3 Chip    OK   47 degrees C / 116 degrees F
FPC 9 Intake       OK   42 degrees C / 107 degrees F
FPC 9 Exhaust A    OK   51 degrees C / 123 degrees F
FPC 9 Exhaust B    OK   63 degrees C / 145 degrees F
FPC 9 LU 0 TSen    OK   60 degrees C / 140 degrees F
FPC 9 LU 0 Chip    OK   65 degrees C / 149 degrees F
FPC 9 LU 1 TSen    OK   60 degrees C / 140 degrees F
FPC 9 LU 1 Chip    OK   67 degrees C / 152 degrees F
FPC 9 LU 2 TSen    OK   60 degrees C / 140 degrees F
FPC 9 LU 2 Chip    OK   54 degrees C / 129 degrees F
FPC 9 LU 3 TSen    OK   60 degrees C / 140 degrees F
FPC 9 LU 3 Chip    OK   53 degrees C / 127 degrees F
FPC 9 LU 3 Chip                OK         54 degrees C / 129 degrees F
FPC 9 MQ 0 TSen                OK         51 degrees C / 123 degrees F
FPC 9 MQ 0 Chip                OK         55 degrees C / 131 degrees F
FPC 9 MQ 1 TSen                OK         51 degrees C / 123 degrees F
FPC 9 MQ 1 Chip                OK         59 degrees C / 138 degrees F
FPC 9 MQ 2 TSen                OK         51 degrees C / 123 degrees F
FPC 9 MQ 2 Chip                OK         49 degrees C / 120 degrees F
FPC 9 MQ 3 TSen                OK         51 degrees C / 123 degrees F
FPC 9 MQ 3 Chip                OK         49 degrees C / 120 degrees F
FPC 9 MQ 4 TSen                OK         44 degrees C / 111 degrees F
FPC 9 MQ 4 Chip                OK         44 degrees C / 111 degrees F
FPC 9 MQ 5 TSen                OK         47 degrees C / 116 degrees F
FPC 9 MQ 5 Chip                OK         47 degrees C / 116 degrees F
FPC 9 MQ 6 TSen                OK         47 degrees C / 116 degrees F
FPC 9 MQ 6 Chip                OK         47 degrees C / 116 degrees F
FPC 9 MQ 7 TSen                OK         47 degrees C / 116 degrees F
FPC 9 MQ 7 Chip                OK         47 degrees C / 116 degrees F
FPC 9 MQ 8 TSen                OK         47 degrees C / 116 degrees F
FPC 9 MQ 8 Chip                OK         47 degrees C / 116 degrees F
FPC 9 MQ 9 TSen                OK         47 degrees C / 116 degrees F
FPC 9 MQ 9 Chip                OK         47 degrees C / 116 degrees F
FPC 9 MQ 10 TSen               OK         47 degrees C / 116 degrees F
FPC 9 MQ 10 Chip               OK         47 degrees C / 116 degrees F

FPC 10 Intake                  OK         44 degrees C / 111 degrees F
FPC 10 Exhaust A               OK         49 degrees C / 120 degrees F
FPC 10 Exhaust B               OK         55 degrees C / 131 degrees F
FPC 10 LU 0 TSen               OK         54 degrees C / 129 degrees F
FPC 10 LU 0 Chip               OK         55 degrees C / 131 degrees F
FPC 10 LU 1 TSen               OK         54 degrees C / 129 degrees F
FPC 10 LU 1 Chip               OK         59 degrees C / 138 degrees F
FPC 10 LU 2 TSen               OK         54 degrees C / 129 degrees F
FPC 10 LU 2 Chip               OK         52 degrees C / 125 degrees F
FPC 10 LU 3 TSen               OK         54 degrees C / 129 degrees F
FPC 10 LU 3 Chip               OK         51 degrees C / 123 degrees F
FPC 10 MQ 0 TSen               OK         48 degrees C / 118 degrees F
FPC 10 MQ 0 Chip               OK         49 degrees C / 120 degrees F
FPC 10 MQ 1 TSen               OK         48 degrees C / 118 degrees F
FPC 10 MQ 1 Chip               OK         52 degrees C / 125 degrees F
FPC 10 MQ 2 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 2 Chip               OK         48 degrees C / 118 degrees F
FPC 10 MQ 3 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 3 Chip               OK         47 degrees C / 116 degrees F
FPC 10 MQ 4 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 4 Chip               OK         47 degrees C / 116 degrees F
FPC 10 MQ 5 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 5 Chip               OK         47 degrees C / 116 degrees F
FPC 10 MQ 6 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 6 Chip               OK         47 degrees C / 116 degrees F
FPC 10 MQ 7 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 7 Chip               OK         47 degrees C / 116 degrees F
FPC 10 MQ 8 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 8 Chip               OK         47 degrees C / 116 degrees F
FPC 10 MQ 9 TSen               OK         47 degrees C / 116 degrees F
FPC 10 MQ 9 Chip               OK         47 degrees C / 116 degrees F
FPC 10 MQ 10 TSen              OK         47 degrees C / 116 degrees F
FPC 10 MQ 10 Chip              OK         47 degrees C / 116 degrees F

FPC 11 Intake                  OK         30 degrees C / 86 degrees F
FPC 11 Exhaust A               OK         35 degrees C / 95 degrees F
FPC 11 Exhaust B               OK         30 degrees C / 86 degrees F
FPC 11 LU 0 TSen               OK         57 degrees C / 134 degrees F
FPC 11 LU 0 Chip               OK         58 degrees C / 136 degrees F
FPC 11 LU 1 TSen               OK         57 degrees C / 134 degrees F
FPC 11 LU 1 Chip               OK         62 degrees C / 143 degrees F
FPC 11 LU 2 TSen               OK         57 degrees C / 134 degrees F
FPC 11 LU 2 Chip               OK         53 degrees C / 127 degrees F
FPC 11 LU 3 TSen               OK         57 degrees C / 134 degrees F
FPC 11 LU 3 Chip               OK         54 degrees C / 129 degrees F
FPC 11 MQ 0 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 0 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 1 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 1 Chip               OK         57 degrees C / 134 degrees F
FPC 11 MQ 2 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 2 Chip               OK         48 degrees C / 118 degrees F
FPC 11 MQ 3 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 3 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 4 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 4 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 5 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 5 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 6 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 6 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 7 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 7 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 8 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 8 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 9 TSen               OK         52 degrees C / 125 degrees F
FPC 11 MQ 9 Chip               OK         52 degrees C / 125 degrees F
FPC 11 MQ 10 TSen              OK         40 degrees C / 104 degrees F
FPC 11 MQ 10 Chip              OK         47 degrees C / 116 degrees F
FPC 11 MQ 0 TSen               OK         51 degrees C / 123 degrees F
FPC 11 MQ 0 Chip               OK         51 degrees C / 123 degrees F
FPC 11 MQ 1 TSen               OK         51 degrees C / 123 degrees F
FPC 11 MQ 1 Chip               OK         51 degrees C / 123 degrees F
FPC 11 MQ 2 TSen               OK         51 degrees C / 123 degrees F
FPC 11 MQ 2 Chip               OK         50 degrees C / 122 degrees F
FPC 11 MQ 3 TSen               OK         46 degrees C / 114 degrees F
FPC 11 MQ 3 Chip               OK         46 degrees C / 114 degrees F
FPC 11 MQ 4 TSen               OK         46 degrees C / 114 degrees F
FPC 11 MQ 4 Chip               OK         46 degrees C / 114 degrees F
FPC 11 MQ 5 TSen               OK         46 degrees C / 114 degrees F
FPC 11 MQ 5 Chip               OK         46 degrees C / 114 degrees F
<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
<th>Temperature (°C) / Temperature (°F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 12 MQ 1 Chip</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 12 MQ 2 TSen</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 12 MQ 2 Chip</td>
<td>OK</td>
<td>44 / 111</td>
</tr>
<tr>
<td>FPC 12 MQ 3 TSen</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 12 MQ 3 Chip</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 13 Intake</td>
<td>OK</td>
<td>52 / 125</td>
</tr>
<tr>
<td>FPC 13 Exhaust A</td>
<td>OK</td>
<td>48 / 118</td>
</tr>
<tr>
<td>FPC 13 Exhaust B</td>
<td>OK</td>
<td>52 / 125</td>
</tr>
<tr>
<td>FPC 13 LU 0 TSen</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 13 LU 0 Chip</td>
<td>OK</td>
<td>52 / 125</td>
</tr>
<tr>
<td>FPC 13 LU 1 TSen</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 13 LU 1 Chip</td>
<td>OK</td>
<td>55 / 131</td>
</tr>
<tr>
<td>FPC 13 LU 2 TSen</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 13 LU 2 Chip</td>
<td>OK</td>
<td>48 / 118</td>
</tr>
<tr>
<td>FPC 13 LU 3 TSen</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 13 LU 3 Chip</td>
<td>OK</td>
<td>48 / 118</td>
</tr>
<tr>
<td>FPC 13 MQ 0 TSen</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 13 MQ 0 Chip</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 13 MQ 1 TSen</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 13 MQ 1 Chip</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 13 MQ 2 TSen</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 13 MQ 2 Chip</td>
<td>OK</td>
<td>44 / 111</td>
</tr>
<tr>
<td>FPC 13 MQ 3 TSen</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 13 MQ 3 Chip</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 14 Intake</td>
<td>OK</td>
<td>40 / 104</td>
</tr>
<tr>
<td>FPC 14 Exhaust A</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 14 Exhaust B</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 14 LU 0 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 14 LU 0 Chip</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 14 LU 1 TSen</td>
<td>OK</td>
<td>54 / 129</td>
</tr>
<tr>
<td>FPC 14 LU 1 Chip</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 14 LU 2 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 14 LU 2 Chip</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 14 LU 3 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 14 LU 3 Chip</td>
<td>OK</td>
<td>49 / 120</td>
</tr>
<tr>
<td>FPC 14 MQ 0 TSen</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 14 MQ 0 Chip</td>
<td>OK</td>
<td>46 / 114</td>
</tr>
<tr>
<td>FPC 14 MQ 1 TSen</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 14 MQ 1 Chip</td>
<td>OK</td>
<td>51 / 123</td>
</tr>
<tr>
<td>FPC 14 MQ 2 TSen</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 14 MQ 2 Chip</td>
<td>OK</td>
<td>45 / 113</td>
</tr>
<tr>
<td>FPC 14 MQ 3 TSen</td>
<td>OK</td>
<td>47 / 116</td>
</tr>
<tr>
<td>FPC 14 MQ 3 Chip</td>
<td>OK</td>
<td>48 / 118</td>
</tr>
<tr>
<td>FPC 15 Intake</td>
<td>OK</td>
<td>44 / 111</td>
</tr>
<tr>
<td>FPC 15 Exhaust A</td>
<td>OK</td>
<td>49 / 120</td>
</tr>
<tr>
<td>FPC 15 Exhaust B</td>
<td>OK</td>
<td>60 / 140</td>
</tr>
<tr>
<td>FPC 15 LU 0 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 LU 0 Chip</td>
<td>OK</td>
<td>56 / 132</td>
</tr>
<tr>
<td>FPC 15 LU 1 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 LU 1 Chip</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 LU 2 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 LU 2 Chip</td>
<td>OK</td>
<td>58 / 136</td>
</tr>
<tr>
<td>FPC 15 LU 3 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 LU 3 Chip</td>
<td>OK</td>
<td>63 / 145</td>
</tr>
<tr>
<td>FPC 15 XM 0 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 XM 0 Chip</td>
<td>OK</td>
<td>56 / 132</td>
</tr>
<tr>
<td>FPC 15 XF 0 TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 XF 0 Chip</td>
<td>OK</td>
<td>68 / 154</td>
</tr>
<tr>
<td>FPC 15 PLX Switch TSen</td>
<td>OK</td>
<td>50 / 122</td>
</tr>
<tr>
<td>FPC 15 PLX Switch Chip</td>
<td>OK</td>
<td>56 / 132</td>
</tr>
<tr>
<td>FPC 16 Intake</td>
<td>OK</td>
<td>42 / 107</td>
</tr>
</tbody>
</table>
FPC 16 Exhaust A       OK         51 degrees C / 123 degrees F
FPC 16 Exhaust B       OK         53 degrees C / 127 degrees F
FPC 16 LU 0 TSen       OK         51 degrees C / 123 degrees F
FPC 16 LU 0 Chip       OK         52 degrees C / 125 degrees F
FPC 16 LU 1 TSen       OK         51 degrees C / 123 degrees F
FPC 16 LU 1 Chip       OK         55 degrees C / 131 degrees F
FPC 16 LU 2 TSen       OK         51 degrees C / 123 degrees F
FPC 16 LU 2 Chip       OK         48 degrees C / 118 degrees F
FPC 16 LU 3 TSen       OK         51 degrees C / 123 degrees F
FPC 16 LU 3 Chip       OK         49 degrees C / 120 degrees F
FPC 16 MQ 0 TSen       OK         49 degrees C / 120 degrees F
FPC 16 MQ 0 Chip       OK         48 degrees C / 118 degrees F
FPC 16 MQ 1 TSen       OK         53 degrees C / 127 degrees F
FPC 16 MQ 1 Chip       OK         49 degrees C / 120 degrees F
FPC 16 MQ 2 TSen       OK         49 degrees C / 120 degrees F
FPC 16 MQ 2 Chip       OK         46 degrees C / 114 degrees F
FPC 16 MQ 3 TSen       OK         49 degrees C / 120 degrees F
FPC 16 MQ 3 Chip       OK         49 degrees C / 120 degrees F
FPC 17 Intake          OK         43 degrees C / 109 degrees F
FPC 17 Exhaust A       OK         51 degrees C / 123 degrees F
FPC 17 Exhaust B       OK         55 degrees C / 131 degrees F
FPC 17 LU 0 TSen       OK         54 degrees C / 129 degrees F
FPC 17 LU 0 Chip       OK         57 degrees C / 134 degrees F
FPC 17 LU 1 TSen       OK         54 degrees C / 129 degrees F
FPC 17 LU 1 Chip       OK         60 degrees C / 140 degrees F
FPC 17 LU 2 TSen       OK         54 degrees C / 129 degrees F
FPC 17 LU 2 Chip       OK         53 degrees C / 127 degrees F
FPC 17 LU 3 TSen       OK         54 degrees C / 129 degrees F
FPC 17 LU 3 Chip       OK         53 degrees C / 127 degrees F
FPC 17 MQ 0 TSen       OK         49 degrees C / 120 degrees F
FPC 17 MQ 0 Chip       OK         50 degrees C / 122 degrees F
FPC 17 MQ 1 TSen       OK         49 degrees C / 120 degrees F
FPC 17 MQ 1 Chip       OK         54 degrees C / 129 degrees F
FPC 17 MQ 2 TSen       OK         49 degrees C / 120 degrees F
FPC 17 MQ 2 Chip       OK         47 degrees C / 116 degrees F
FPC 17 MQ 3 TSen       OK         49 degrees C / 120 degrees F
FPC 17 MQ 3 Chip       OK         51 degrees C / 123 degrees F
FPC 18 Intake          OK         44 degrees C / 111 degrees F
FPC 18 Exhaust A       OK         53 degrees C / 127 degrees F
FPC 18 Exhaust B       OK         57 degrees C / 134 degrees F
FPC 18 LU 0 TSen       OK         56 degrees C / 132 degrees F
FPC 18 LU 0 Chip       OK         57 degrees C / 134 degrees F
FPC 18 LU 1 TSen       OK         56 degrees C / 132 degrees F
FPC 18 LU 1 Chip       OK         62 degrees C / 143 degrees F
FPC 18 LU 2 TSen       OK         56 degrees C / 132 degrees F
FPC 18 LU 2 Chip       OK         53 degrees C / 127 degrees F
FPC 18 LU 3 TSen       OK         56 degrees C / 132 degrees F
FPC 18 LU 3 Chip       OK         55 degrees C / 131 degrees F
FPC 18 MQ 0 TSen       OK         51 degrees C / 123 degrees F
FPC 18 MQ 0 Chip       OK         54 degrees C / 129 degrees F
FPC 18 MQ 1 TSen       OK         51 degrees C / 123 degrees F
FPC 18 MQ 1 Chip       OK         58 degrees C / 136 degrees F
FPC 18 MQ 2 TSen       OK         51 degrees C / 123 degrees F
FPC 18 MQ 2 Chip       OK         50 degrees C / 122 degrees F
FPC 18 MQ 3 TSen       OK         51 degrees C / 123 degrees F
FPC 18 MQ 3 Chip       OK         53 degrees C / 127 degrees F
FPC 19 Intake          OK         48 degrees C / 118 degrees F
FPC 19 Exhaust A       OK         56 degrees C / 132 degrees F
FPC 19 Exhaust B       OK         64 degrees C / 147 degrees F
FPC 19 LU 0 TSen       OK         63 degrees C / 145 degrees F
FPC 19 LU 0 Chip       OK         64 degrees C / 147 degrees F

Chapter 24: Administration
<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 19 LU 1 TSen</td>
<td>OK</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>FPC 19 LU 1 Chip</td>
<td>OK</td>
<td>70 degrees C / 158 degrees F</td>
</tr>
<tr>
<td>FPC 19 LU 2 TSen</td>
<td>OK</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>FPC 19 LU 2 Chip</td>
<td>OK</td>
<td>61 degrees C / 141 degrees F</td>
</tr>
<tr>
<td>FPC 19 LU 3 TSen</td>
<td>OK</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>FPC 19 LU 3 Chip</td>
<td>OK</td>
<td>62 degrees C / 143 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 0 TSen</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 0 Chip</td>
<td>OK</td>
<td>60 degrees C / 140 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 1 TSen</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 1 Chip</td>
<td>OK</td>
<td>62 degrees C / 143 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 2 TSen</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 2 Chip</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 3 TSen</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td>FPC 19 MQ 3 Chip</td>
<td>OK</td>
<td>57 degrees C / 134 degrees F</td>
</tr>
<tr>
<td>ADC 0 Intake</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td>ADC 0 Exhaust</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td>ADC 0 ADC-XF1</td>
<td>OK</td>
<td>59 degrees C / 138 degrees F</td>
</tr>
<tr>
<td>ADC 0 ADC-XF0</td>
<td>OK</td>
<td>66 degrees C / 150 degrees F</td>
</tr>
<tr>
<td>ADC 1 Intake</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>ADC 1 Exhaust</td>
<td>OK</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td>ADC 1 ADC-XF1</td>
<td>OK</td>
<td>59 degrees C / 138 degrees F</td>
</tr>
<tr>
<td>ADC 1 ADC-XF0</td>
<td>OK</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>ADC 2 Intake</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td>ADC 2 Exhaust</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td>ADC 2 ADC-XF1</td>
<td>OK</td>
<td>53 degrees C / 127 degrees F</td>
</tr>
<tr>
<td>ADC 2 ADC-XF0</td>
<td>OK</td>
<td>61 degrees C / 141 degrees F</td>
</tr>
<tr>
<td>ADC 3 Intake</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td>ADC 3 Exhaust</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>ADC 3 ADC-XF1</td>
<td>OK</td>
<td>61 degrees C / 141 degrees F</td>
</tr>
<tr>
<td>ADC 3 ADC-XF0</td>
<td>OK</td>
<td>64 degrees C / 147 degrees F</td>
</tr>
<tr>
<td>ADC 4 Intake</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>ADC 4 Exhaust</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>ADC 4 ADC-XF1</td>
<td>OK</td>
<td>60 degrees C / 140 degrees F</td>
</tr>
<tr>
<td>ADC 4 ADC-XF0</td>
<td>OK</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>ADC 5 Intake</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>ADC 5 Exhaust</td>
<td>OK</td>
<td>54 degrees C / 129 degrees F</td>
</tr>
<tr>
<td>ADC 5 ADC-XF1</td>
<td>OK</td>
<td>56 degrees C / 132 degrees F</td>
</tr>
<tr>
<td>ADC 5 ADC-XF0</td>
<td>OK</td>
<td>67 degrees C / 152 degrees F</td>
</tr>
<tr>
<td>ADC 6 Intake</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>ADC 6 Exhaust</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td>ADC 6 ADC-XF1</td>
<td>OK</td>
<td>59 degrees C / 138 degrees F</td>
</tr>
<tr>
<td>ADC 6 ADC-XF0</td>
<td>OK</td>
<td>66 degrees C / 150 degrees F</td>
</tr>
<tr>
<td>ADC 7 Intake</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>ADC 7 Exhaust</td>
<td>OK</td>
<td>54 degrees C / 129 degrees F</td>
</tr>
<tr>
<td>ADC 7 ADC-XF1</td>
<td>OK</td>
<td>62 degrees C / 143 degrees F</td>
</tr>
<tr>
<td>ADC 7 ADC-XF0</td>
<td>OK</td>
<td>70 degrees C / 158 degrees F</td>
</tr>
<tr>
<td>ADC 8 Intake</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td>ADC 8 Exhaust</td>
<td>OK</td>
<td>52 degrees C / 125 degrees F</td>
</tr>
<tr>
<td>ADC 8 ADC-XF1</td>
<td>OK</td>
<td>61 degrees C / 141 degrees F</td>
</tr>
<tr>
<td>ADC 8 ADC-XF0</td>
<td>OK</td>
<td>65 degrees C / 149 degrees F</td>
</tr>
<tr>
<td>ADC 9 Intake</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>ADC 9 Exhaust</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>ADC 9 ADC-XF1</td>
<td>OK</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>ADC 9 ADC-XF0</td>
<td>OK</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>ADC 10 Intake</td>
<td>OK</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td>ADC 10 Exhaust</td>
<td>OK</td>
<td>53 degrees C / 127 degrees F</td>
</tr>
<tr>
<td>ADC 10 ADC-XF1</td>
<td>OK</td>
<td>67 degrees C / 152 degrees F</td>
</tr>
<tr>
<td>ADC 10 ADC-XF0</td>
<td>OK</td>
<td>66 degrees C / 150 degrees F</td>
</tr>
<tr>
<td>ADC 12 Intake</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>ADC 12 Exhaust</td>
<td>OK</td>
<td>54 degrees C / 129 degrees F</td>
</tr>
<tr>
<td>ADC 12 ADC-XF1</td>
<td>OK</td>
<td>67 degrees C / 152 degrees F</td>
</tr>
</tbody>
</table>
ADC 12 ADC-XF0          OK         67 degrees C / 152 degrees F
ADC 13 Intake            OK         49 degrees C / 120 degrees F
ADC 13 Exhaust           OK         57 degrees C / 134 degrees F
ADC 13 ADC-XF1           OK         66 degrees C / 150 degrees F
ADC 13 ADC-XF0           OK         69 degrees C / 156 degrees F
ADC 14 Intake            OK         51 degrees C / 123 degrees F
ADC 14 Exhaust           OK         59 degrees C / 138 degrees F
ADC 14 ADC-XF1           OK         69 degrees C / 156 degrees F
ADC 14 ADC-XF0           OK         74 degrees C / 165 degrees F
ADC 15 Intake            OK         50 degrees C / 122 degrees F
ADC 15 Exhaust           OK         59 degrees C / 138 degrees F
ADC 15 ADC-XF1           OK         68 degrees C / 154 degrees F
ADC 15 ADC-XF0           OK         69 degrees C / 156 degrees F
ADC 16 Intake            OK         52 degrees C / 125 degrees F
ADC 16 Exhaust           OK         58 degrees C / 136 degrees F
ADC 16 ADC-XF1           OK         68 degrees C / 154 degrees F
ADC 16 ADC-XF0           OK         70 degrees C / 158 degrees F
ADC 17 Intake            OK         52 degrees C / 125 degrees F
ADC 17 Exhaust           OK         59 degrees C / 138 degrees F
ADC 17 ADC-XF1           OK         69 degrees C / 156 degrees F
ADC 17 ADC-XF0           OK         71 degrees C / 159 degrees F
ADC 18 Intake            OK         53 degrees C / 127 degrees F
ADC 18 Exhaust           OK         59 degrees C / 138 degrees F
ADC 18 ADC-XF1           OK         68 degrees C / 154 degrees F
ADC 18 ADC-XF0           OK         73 degrees C / 163 degrees F
ADC 19 Intake            OK         50 degrees C / 122 degrees F
ADC 19 Exhaust           OK         59 degrees C / 138 degrees F
ADC 19 ADC-XF1           OK         68 degrees C / 154 degrees F
ADC 19 ADC-XF0           OK         72 degrees C / 161 degrees F

Fans
Fan Tray 0 Fan 1          OK         7440 RPM
Fan Tray 0 Fan 2          OK         7200 RPM
Fan Tray 0 Fan 3          OK         6960 RPM
Fan Tray 0 Fan 4          OK         7200 RPM
Fan Tray 0 Fan 5          OK         7080 RPM
Fan Tray 0 Fan 6          OK         6840 RPM
Fan Tray 1 Fan 1          OK         6840 RPM
Fan Tray 1 Fan 2          OK         6960 RPM
Fan Tray 1 Fan 3          OK         6960 RPM
Fan Tray 1 Fan 4          OK         7080 RPM
Fan Tray 1 Fan 5          OK         6960 RPM
Fan Tray 1 Fan 6          OK         6960 RPM
Fan Tray 2 Fan 1          OK         8640 RPM
Fan Tray 2 Fan 2          OK         8640 RPM
Fan Tray 2 Fan 3          OK         8760 RPM
Fan Tray 2 Fan 4          OK         8760 RPM
Fan Tray 2 Fan 5          OK         8640 RPM
Fan Tray 2 Fan 6          OK         8640 RPM
Fan Tray 3 Fan 1          OK         8520 RPM
Fan Tray 3 Fan 2          OK         8520 RPM
Fan Tray 3 Fan 3          OK         8640 RPM
Fan Tray 3 Fan 4          OK         8640 RPM
Fan Tray 3 Fan 5          OK         8520 RPM
Fan Tray 3 Fan 6          OK         8520 RPM

show chassis environment (MX2010 Router)

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PSM 0</td>
<td>OK</td>
<td>7 degrees C / 44 degrees F</td>
</tr>
<tr>
<td></td>
<td>PSM 1</td>
<td>OK</td>
<td>7 degrees C / 44 degrees F</td>
</tr>
<tr>
<td></td>
<td>PSM 2</td>
<td>OK</td>
<td>7 degrees C / 44 degrees F</td>
</tr>
<tr>
<td>Component</td>
<td>Status</td>
<td>Temperature</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>PSM 3</td>
<td>OK</td>
<td>6 degrees C / 42 degrees F</td>
<td></td>
</tr>
<tr>
<td>PSM 4</td>
<td>OK</td>
<td>6 degrees C / 42 degrees F</td>
<td></td>
</tr>
<tr>
<td>PSM 5</td>
<td>OK</td>
<td>6 degrees C / 42 degrees F</td>
<td></td>
</tr>
<tr>
<td>PSM 6</td>
<td>OK</td>
<td>6 degrees C / 42 degrees F</td>
<td></td>
</tr>
<tr>
<td>PSM 7</td>
<td>OK</td>
<td>7 degrees C / 44 degrees F</td>
<td></td>
</tr>
<tr>
<td>PSM 8</td>
<td>OK</td>
<td>7 degrees C / 44 degrees F</td>
<td></td>
</tr>
<tr>
<td>PDM 0</td>
<td>OK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDM 1</td>
<td>Absent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CB 0 IntakeA-Zone0</td>
<td>OK</td>
<td>14 degrees C / 57 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 0 IntakeB-Zone0</td>
<td>OK</td>
<td>7 degrees C / 44 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 0 IntakeC-Zone0</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 0 ExhaustA-Zone0</td>
<td>OK</td>
<td>14 degrees C / 57 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 0 ExhaustB-Zone1</td>
<td>OK</td>
<td>9 degrees C / 48 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 0 TCBC-Zone0</td>
<td>OK</td>
<td>11 degrees C / 51 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 1 IntakeA-Zone0</td>
<td>OK</td>
<td>9 degrees C / 48 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 1 IntakeB-Zone1</td>
<td>OK</td>
<td>5 degrees C / 41 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 1 IntakeC-Zone0</td>
<td>OK</td>
<td>20 degrees C / 68 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 1 ExhaustA-Zone0</td>
<td>OK</td>
<td>12 degrees C / 53 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 1 ExhaustB-Zone1</td>
<td>OK</td>
<td>7 degrees C / 44 degrees F</td>
<td></td>
</tr>
<tr>
<td>CB 1 TCBC-Zone0</td>
<td>OK</td>
<td>10 degrees C / 53 degrees F</td>
<td></td>
</tr>
<tr>
<td>SPMB 0 Intake</td>
<td>OK</td>
<td>5 degrees C / 41 degrees F</td>
<td></td>
</tr>
<tr>
<td>SPMB 1 Intake</td>
<td>OK</td>
<td>4 degrees C / 39 degrees F</td>
<td></td>
</tr>
<tr>
<td>Routing Engine 0</td>
<td>OK</td>
<td>9 degrees C / 48 degrees F</td>
<td></td>
</tr>
<tr>
<td>Routing Engine 0 CPU</td>
<td>OK</td>
<td>9 degrees C / 48 degrees F</td>
<td></td>
</tr>
<tr>
<td>Routing Engine 1</td>
<td>OK</td>
<td>6 degrees C / 42 degrees F</td>
<td></td>
</tr>
<tr>
<td>Routing Engine 1 CPU</td>
<td>OK</td>
<td>6 degrees C / 42 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 Intake-Zone0</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 Exhaust-Zone0</td>
<td>OK</td>
<td>17 degrees C / 62 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 IntakeA-Zone0</td>
<td>OK</td>
<td>16 degrees C / 60 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 IntakeB-Zone1</td>
<td>OK</td>
<td>11 degrees C / 51 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 Exhaust-Zone0</td>
<td>OK</td>
<td>18 degrees C / 64 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 SFB-XF2-Zone1</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 SFB-XF1-Zone0</td>
<td>OK</td>
<td>23 degrees C / 73 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 0 SFB-XF0-Zone0</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 Intake-Zone0</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 Exhaust-Zone0</td>
<td>OK</td>
<td>15 degrees C / 59 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 IntakeA-Zone0</td>
<td>OK</td>
<td>20 degrees C / 68 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 IntakeB-Zone1</td>
<td>OK</td>
<td>10 degrees C / 50 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 Exhaust-Zone0</td>
<td>OK</td>
<td>19 degrees C / 66 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 SFB-XF2-Zone1</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 SFB-XF1-Zone0</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 1 SFB-XF0-Zone0</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 2 Intake-Zone0</td>
<td>OK</td>
<td>18 degrees C / 64 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 2 IntakeB-Zone1</td>
<td>OK</td>
<td>9 degrees C / 48 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 2 Exhaust-Zone0</td>
<td>OK</td>
<td>16 degrees C / 60 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 2 SFB-XF2-Zone1</td>
<td>OK</td>
<td>24 degrees C / 75 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 2 SFB-XF1-Zone0</td>
<td>OK</td>
<td>21 degrees C / 69 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 2 SFB-XF0-Zone0</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 Intake-Zone0</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 Exhaust-Zone1</td>
<td>OK</td>
<td>16 degrees C / 60 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 IntakeA-Zone0</td>
<td>OK</td>
<td>18 degrees C / 64 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 IntakeB-Zone1</td>
<td>OK</td>
<td>11 degrees C / 51 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 Exhaust-Zone0</td>
<td>OK</td>
<td>19 degrees C / 66 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 SFB-XF2-Zone1</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 SFB-XF1-Zone0</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 4 SFB-XF0-Zone0</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 5 Intake-Zone0</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 5 Exhaust-Zone1</td>
<td>OK</td>
<td>14 degrees C / 57 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 5 IntakeA-Zone0</td>
<td>OK</td>
<td>18 degrees C / 64 degrees F</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Status</td>
<td>Temperature [°C / °F]</td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>SFB 5 Intake B-Zone 1</td>
<td>OK</td>
<td>10 degrees C / 50 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 5 Exhaust-Zone 0</td>
<td>OK</td>
<td>17 degrees C / 62 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 5 SFB-XF2-Zone 1</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 5 SFB-XF1-Zone 0</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 5 SFB-XF0-Zone 0</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 6 Intake-Zone 0</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 6 Exhaust-Zone 1</td>
<td>OK</td>
<td>13 degrees C / 55 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 6 Intake A-Zone 0</td>
<td>OK</td>
<td>10 degrees C / 50 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 6 Exhaust-Zone 0</td>
<td>OK</td>
<td>20 degrees C / 68 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 6 SFB-XF2-Zone 1</td>
<td>OK</td>
<td>10 degrees C / 50 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 6 SFB-XF1-Zone 0</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 6 SFB-XF0-Zone 0</td>
<td>OK</td>
<td>19 degrees C / 66 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 7 Intake-Zone 0</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 7 Exhaust-Zone 1</td>
<td>OK</td>
<td>13 degrees C / 55 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 7 Intake A-Zone 0</td>
<td>OK</td>
<td>19 degrees C / 66 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 7 Exhaust-Zone 0</td>
<td>OK</td>
<td>24 degrees C / 75 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 7 SFB-XF2-Zone 1</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 7 SFB-XF1-Zone 0</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
<td></td>
</tr>
<tr>
<td>SFB 7 SFB-XF0-Zone 0</td>
<td>OK</td>
<td>14 degrees C / 57 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 Intake</td>
<td>OK</td>
<td>17 degrees C / 62 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 Exhaust A</td>
<td>OK</td>
<td>20 degrees C / 68 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 Exhaust B</td>
<td>OK</td>
<td>19 degrees C / 66 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 0 TSen</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 0 Chip</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 1 TSen</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 1 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 2 TSen</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 2 Chip</td>
<td>OK</td>
<td>19 degrees C / 66 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 3 TSen</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 LU 3 Chip</td>
<td>OK</td>
<td>23 degrees C / 73 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 XM 0 TSen</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 XM 0 Chip</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 XM 1 TSen</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 XM 1 Chip</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 PLX Switch TSen</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 0 PLX Switch Chip</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 Intake</td>
<td>OK</td>
<td>10 degrees C / 50 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 Exhaust A</td>
<td>OK</td>
<td>24 degrees C / 75 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 Exhaust B</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 0 TSen</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 0 Chip</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 1 TSen</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 1 Chip</td>
<td>OK</td>
<td>21 degrees C / 69 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 2 TSen</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 2 Chip</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 3 TSen</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 LU 3 Chip</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 XM 0 TSen</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 XM 0 Chip</td>
<td>OK</td>
<td>30 degrees C / 86 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 XM 1 TSen</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 XM 1 Chip</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 PLX Switch TSen</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 1 PLX Switch Chip</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 Intake</td>
<td>OK</td>
<td>9 degrees C / 48 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 Exhaust A</td>
<td>OK</td>
<td>10 degrees C / 50 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 Exhaust B</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 0 TSen</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 0 Chip</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 1 TSen</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Status</td>
<td>Temperature</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 1 Chip</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 2 TSen</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 2 Chip</td>
<td>OK</td>
<td>17 degrees C / 62 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 3 TSen</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 LU 3 Chip</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 XM 1 TSen</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 XM 1 Chip</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 PLX Switch TSen</td>
<td>OK</td>
<td>20 degrees C / 68 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 2 PLX Switch Chip</td>
<td>OK</td>
<td>20 degrees C / 68 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 3 Intake</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 3 Exhaust A</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 3 Exhaust B</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 3 LU 0 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 3 LU 0 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 3 MQ 0 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 3 MQ 0 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 Intake</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 Exhaust A</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 Exhaust B</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 LU 0 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 LU 0 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 LU 1 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 LU 1 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 LU 2 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 4 LU 2 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 Intake</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 Exhaust A</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 0 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 0 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 1 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 1 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 2 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 2 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 3 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 LU 3 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 XM 0 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 XM 0 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 XM 1 TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 XM 1 Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 PLX Switch TSen</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 PLX Switch Chip</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Status</td>
<td>Temperature °C / °F</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>FPC 5 XM 1 Chip</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 PLX Switch TSen</td>
<td>OK</td>
<td>27 °C / 80 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 5 PLX Switch Chip</td>
<td>OK</td>
<td>24 °C / 75 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 Intake</td>
<td>OK</td>
<td>12 °C / 53 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 Exhaust A</td>
<td>OK</td>
<td>17 °C / 62 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 Exhaust B</td>
<td>OK</td>
<td>28 °C / 82 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 0 TSen</td>
<td>OK</td>
<td>24 °C / 75 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 0 Chip</td>
<td>OK</td>
<td>29 °C / 84 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 1 TSen</td>
<td>OK</td>
<td>24 °C / 75 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 1 Chip</td>
<td>OK</td>
<td>30 °C / 86 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 2 TSen</td>
<td>OK</td>
<td>24 °C / 75 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 2 Chip</td>
<td>OK</td>
<td>24 °C / 75 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 3 TSen</td>
<td>OK</td>
<td>24 °C / 75 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 LU 3 Chip</td>
<td>OK</td>
<td>22 °C / 71 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 0 TSen</td>
<td>OK</td>
<td>16 °C / 60 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 0 Chip</td>
<td>OK</td>
<td>19 °C / 66 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 1 TSen</td>
<td>OK</td>
<td>16 °C / 60 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 1 Chip</td>
<td>OK</td>
<td>20 °C / 68 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 2 TSen</td>
<td>OK</td>
<td>16 °C / 60 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 2 Chip</td>
<td>OK</td>
<td>17 °C / 62 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 3 TSen</td>
<td>OK</td>
<td>16 °C / 60 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 3 Chip</td>
<td>OK</td>
<td>16 °C / 60 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 4 TSen</td>
<td>OK</td>
<td>16 °C / 60 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 MQ 4 Chip</td>
<td>OK</td>
<td>32 °C / 89 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 PLX Switch TSen</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 6 PLX Switch Chip</td>
<td>OK</td>
<td>22 °C / 71 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 Intake</td>
<td>OK</td>
<td>10 °C / 50 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 Exhaust A</td>
<td>OK</td>
<td>10 °C / 50 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 Exhaust B</td>
<td>OK</td>
<td>11 °C / 53 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 0 TSen</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 0 Chip</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 1 TSen</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 1 Chip</td>
<td>OK</td>
<td>29 °C / 84 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 2 TSen</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 2 Chip</td>
<td>OK</td>
<td>19 °C / 66 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 3 TSen</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 3 Chip</td>
<td>OK</td>
<td>24 °C / 75 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 4 TSen</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 LU 4 Chip</td>
<td>OK</td>
<td>32 °C / 89 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 PLX Switch TSen</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 7 PLX Switch Chip</td>
<td>OK</td>
<td>22 °C / 71 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 Intake</td>
<td>OK</td>
<td>10 °C / 50 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 Exhaust A</td>
<td>OK</td>
<td>22 °C / 71 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 Exhaust B</td>
<td>OK</td>
<td>28 °C / 82 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 0 TSen</td>
<td>OK</td>
<td>20 °C / 68 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 0 Chip</td>
<td>OK</td>
<td>33 °C / 91 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 1 TSen</td>
<td>OK</td>
<td>20 °C / 68 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 1 Chip</td>
<td>OK</td>
<td>33 °C / 91 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 2 TSen</td>
<td>OK</td>
<td>20 °C / 68 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 2 Chip</td>
<td>OK</td>
<td>26 °C / 78 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 3 TSen</td>
<td>OK</td>
<td>33 °C / 91 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 LU 3 Chip</td>
<td>OK</td>
<td>29 °C / 84 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 XM 0 TSen</td>
<td>OK</td>
<td>20 °C / 68 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 XM 0 Chip</td>
<td>OK</td>
<td>20 °C / 68 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 XF 0 TSen</td>
<td>OK</td>
<td>38 °C / 100 °F</td>
<td></td>
</tr>
<tr>
<td>FPC 8 XF 0 Chip</td>
<td>OK</td>
<td>20 °C / 68 °F</td>
<td></td>
</tr>
<tr>
<td>Component ID</td>
<td>Status</td>
<td>Temperature (°C / °F)</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>-----------------------</td>
<td></td>
</tr>
<tr>
<td>FPC 9 LU 1 TSen</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 LU 1 Chip</td>
<td>OK</td>
<td>26 / 78</td>
<td></td>
</tr>
<tr>
<td>FPC 9 LU 2 TSen</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 LU 2 Chip</td>
<td>OK</td>
<td>16 / 60</td>
<td></td>
</tr>
<tr>
<td>FPC 9 LU 3 TSen</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 LU 3 Chip</td>
<td>OK</td>
<td>21 / 69</td>
<td></td>
</tr>
<tr>
<td>FPC 9 XM 0 TSen</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 XM 0 Chip</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 XM 1 TSen</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 XM 1 Chip</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 PLX Switch TSen</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>FPC 9 PLX Switch Chip</td>
<td>OK</td>
<td>25 / 77</td>
<td></td>
</tr>
<tr>
<td>ADC 0 Intake</td>
<td>OK</td>
<td>12 / 53</td>
<td></td>
</tr>
<tr>
<td>ADC 0 Exhaust</td>
<td>OK</td>
<td>20 / 68</td>
<td></td>
</tr>
<tr>
<td>ADC 0 ADC-XF1</td>
<td>OK</td>
<td>26 / 78</td>
<td></td>
</tr>
<tr>
<td>ADC 0 ADC-XF0</td>
<td>OK</td>
<td>32 / 89</td>
<td></td>
</tr>
<tr>
<td>ADC 1 Intake</td>
<td>OK</td>
<td>11 / 51</td>
<td></td>
</tr>
<tr>
<td>ADC 1 Exhaust</td>
<td>OK</td>
<td>21 / 69</td>
<td></td>
</tr>
<tr>
<td>ADC 1 ADC-XF1</td>
<td>OK</td>
<td>24 / 75</td>
<td></td>
</tr>
<tr>
<td>ADC 1 ADC-XF0</td>
<td>OK</td>
<td>31 / 87</td>
<td></td>
</tr>
<tr>
<td>ADC 2 Intake</td>
<td>OK</td>
<td>14 / 57</td>
<td></td>
</tr>
<tr>
<td>ADC 2 Exhaust</td>
<td>OK</td>
<td>21 / 69</td>
<td></td>
</tr>
<tr>
<td>ADC 2 ADC-XF1</td>
<td>OK</td>
<td>28 / 82</td>
<td></td>
</tr>
<tr>
<td>ADC 2 ADC-XF0</td>
<td>OK</td>
<td>34 / 93</td>
<td></td>
</tr>
<tr>
<td>ADC 3 Intake</td>
<td>OK</td>
<td>13 / 55</td>
<td></td>
</tr>
<tr>
<td>ADC 3 Exhaust</td>
<td>OK</td>
<td>19 / 66</td>
<td></td>
</tr>
<tr>
<td>ADC 3 ADC-XF1</td>
<td>OK</td>
<td>24 / 75</td>
<td></td>
</tr>
<tr>
<td>ADC 3 ADC-XF0</td>
<td>OK</td>
<td>31 / 87</td>
<td></td>
</tr>
<tr>
<td>ADC 4 Intake</td>
<td>OK</td>
<td>9 / 48</td>
<td></td>
</tr>
<tr>
<td>ADC 4 Exhaust</td>
<td>OK</td>
<td>22 / 71</td>
<td></td>
</tr>
<tr>
<td>ADC 4 ADC-XF1</td>
<td>OK</td>
<td>28 / 82</td>
<td></td>
</tr>
<tr>
<td>ADC 4 ADC-XF0</td>
<td>OK</td>
<td>35 / 95</td>
<td></td>
</tr>
<tr>
<td>ADC 5 Intake</td>
<td>OK</td>
<td>12 / 53</td>
<td></td>
</tr>
<tr>
<td>ADC 5 Exhaust</td>
<td>OK</td>
<td>22 / 71</td>
<td></td>
</tr>
<tr>
<td>ADC 5 ADC-XF1</td>
<td>OK</td>
<td>28 / 82</td>
<td></td>
</tr>
<tr>
<td>ADC 5 ADC-XF0</td>
<td>OK</td>
<td>34 / 93</td>
<td></td>
</tr>
<tr>
<td>ADC 6 Intake</td>
<td>OK</td>
<td>11 / 51</td>
<td></td>
</tr>
<tr>
<td>ADC 6 Exhaust</td>
<td>OK</td>
<td>21 / 69</td>
<td></td>
</tr>
<tr>
<td>ADC 6 ADC-XF1</td>
<td>OK</td>
<td>26 / 78</td>
<td></td>
</tr>
<tr>
<td>ADC 6 ADC-XF0</td>
<td>OK</td>
<td>35 / 95</td>
<td></td>
</tr>
<tr>
<td>Fans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan Tray 0 Fan 1</td>
<td>OK</td>
<td>3480</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 0 Fan 2</td>
<td>OK</td>
<td>3480</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 0 Fan 3</td>
<td>OK</td>
<td>3480</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 0 Fan 4</td>
<td>OK</td>
<td>3360</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 0 Fan 5</td>
<td>OK</td>
<td>3360</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 0 Fan 6</td>
<td>OK</td>
<td>3480</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 1 Fan 1</td>
<td>OK</td>
<td>3360</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 1 Fan 2</td>
<td>OK</td>
<td>3360</td>
<td></td>
</tr>
<tr>
<td>Fan Tray 1 Fan 3</td>
<td>OK</td>
<td>3360</td>
<td></td>
</tr>
</tbody>
</table>
### show chassis environment (T320 Router)

<table>
<thead>
<tr>
<th>Class Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power PEM 0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Power PEM 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>Temp SCG 0</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
</tr>
<tr>
<td>Temp SCG 1</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
</tr>
<tr>
<td>Routing Engine 0</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td>Routing Engine 1</td>
<td>OK</td>
<td>30 degrees C / 86 degrees F</td>
</tr>
<tr>
<td>CB 0</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td>CB 1</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td>SIB 0</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td>SIB 1</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td>SIB 2</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td>FPC 0 Top</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>FPC 0 Bottom</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td>FPC 1 Top</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>FPC 1 Bottom</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td>FPC 2 Top</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>FPC 2 Bottom</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td>FPM GBUS</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
</tr>
<tr>
<td>FPM Display</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td>Fans Top Left Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Top Left Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Top Left Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Top Right Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Top Right Middle fanOK</td>
<td></td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Top Right Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Bottom Left Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Bottom Left Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Bottom Left Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Bottom Right Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Bottom Right Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans Bottom Right Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Misc CIP</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Misc SPMB 0</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>
show chassis environment (T640 Router)

```
user@host> show chassis environment
Class    Item                           Status   Measurement
Temp     PEM 0                          Absent
         PEM 1                          OK       22 degrees C / 71 degrees F
         SCG 0                          OK       30 degrees C / 86 degrees F
         SCG 1                          OK       30 degrees C / 86 degrees F
Routing Engine 0   Present
Routing Engine 1   OK       27 degrees C / 80 degrees F
CB 0              Present
CB 1              OK       33 degrees C / 91 degrees F
SIB 0              Absent
SIB 1              Absent
SIB 2              Absent
SIB 3              Absent
SIB 4              Absent
FPC 4 Top          Testing
FPC 4 Bottom       Testing
FPC 5 Top          Testing
FPC 5 Bottom       Testing
FPC 6 Top          Testing
FPC 6 Bottom       Testing
FPM GBUS            OK       23 degrees C / 73 degrees F
FPM Display        Absent
Fans    Top Left Front fan              OK       Spinning at normal speed
        Top Left Middle fan           OK       Spinning at normal speed
        Top Left Rear fan             OK       Spinning at normal speed
        Top Right Front fan           OK       Spinning at normal speed
        Top Right Middle fan          OK       Spinning at normal speed
        Top Right Rear fan            OK       Spinning at normal speed
        Bottom Left Front fan         OK       Spinning at normal speed
        Bottom Left Middle fan        OK       Spinning at normal speed
        Bottom Left Rear fan          OK       Spinning at normal speed
        Bottom Right Front fan        OK       Spinning at normal speed
        Bottom Right Middle fan       OK       Spinning at normal speed
        Bottom Right Rear fan         OK       Spinning at normal speed
        Fourth Blower from top        OK       Spinning at normal speed
        Bottom Blower                 OK       Spinning at normal speed
        Middle Blower                 OK       Spinning at normal speed
        Top Blower                    OK       Spinning at normal speed
        Second Blower from top        OK       Spinning at normal speed
Misc     CIP                            OK
         SPMB 0                        OK
         SPMB 1                        OK
```
Routing Engine 1 CPU OK 46 degrees C / 114 degrees F
CB 0 OK 32 degrees C / 89 degrees F
CB 1 OK 33 degrees C / 91 degrees F
SIB 0 OK 42 degrees C / 107 degrees F
SIB 1 OK 42 degrees C / 107 degrees F
SIB 2 OK 42 degrees C / 107 degrees F
SIB 3 OK 43 degrees C / 109 degrees F
SIB 4 OK 45 degrees C / 113 degrees F
FPC 0 Fan Intake OK 34 degrees C / 93 degrees F
FPC 0 Fan Exhaust OK 48 degrees C / 118 degrees F
FPC 0 PMB OK 47 degrees C / 116 degrees F
FPC 0 LMB0 OK 50 degrees C / 122 degrees F
FPC 0 LMB1 OK 41 degrees C / 105 degrees F
FPC 0 LMB2 OK 35 degrees C / 95 degrees F
FPC 0 PFE1 LU2 OK 46 degrees C / 114 degrees F
FPC 0 PFE1 LU0 OK 41 degrees C / 105 degrees F
FPC 0 PFE0 LU0 OK 57 degrees C / 134 degrees F
FPC 0 XF1 OK 46 degrees C / 114 degrees F
FPC 0 XF0 OK 52 degrees C / 125 degrees F
FPC 0 XM1 OK 41 degrees C / 105 degrees F
FPC 0 XM0 OK 50 degrees C / 122 degrees F
FPC 0 PFE0 LU1 OK 56 degrees C / 132 degrees F
FPC 0 PFE0 LU2 OK 45 degrees C / 113 degrees F
FPC 0 PFE1 LU1 OK 37 degrees C / 98 degrees F
FPC 3 Fan Intake OK 36 degrees C / 96 degrees F
FPC 3 Fan Exhaust OK 51 degrees C / 123 degrees F
FPC 3 PMB OK 43 degrees C / 109 degrees F
FPC 3 LMB0 OK 57 degrees C / 134 degrees F
FPC 3 LMB1 OK 54 degrees C / 129 degrees F
FPC 3 LMB2 OK 38 degrees C / 100 degrees F
FPC 3 PFE1 LU2 OK 63 degrees C / 145 degrees F
FPC 3 PFE1 LU0 OK 45 degrees C / 113 degrees F
FPC 3 PFE0 LU0 OK 69 degrees C / 156 degrees F
FPC 3 XF1 OK 62 degrees C / 143 degrees F
FPC 3 XF0 OK 63 degrees C / 145 degrees F
FPC 3 XM1 OK 43 degrees C / 109 degrees F
FPC 3 XM0 OK 67 degrees C / 152 degrees F
FPC 3 PFE0 LU1 OK 63 degrees C / 145 degrees F
FPC 3 PFE0 LU2 OK 66 degrees C / 150 degrees F
FPC 3 PFE1 LU1 OK 41 degrees C / 105 degrees F
FPC 5 Top OK 39 degrees C / 102 degrees F
FPC 5 Bottom OK 38 degrees C / 100 degrees F
FPC 6 Fan Intake OK 33 degrees C / 91 degrees F
FPC 6 Fan Exhaust OK 49 degrees C / 120 degrees F
FPC 6 PMB OK 40 degrees C / 104 degrees F
FPC 6 LMB0 OK 60 degrees C / 140 degrees F
FPC 6 LMB1 OK 58 degrees C / 136 degrees F
FPC 6 LMB2 OK 40 degrees C / 104 degrees F
FPC 6 PFE1 LU2 OK 69 degrees C / 156 degrees F
FPC 6 PFE1 LU0 OK 45 degrees C / 113 degrees F
FPC 6 PFE0 LU0 OK 71 degrees C / 159 degrees F
FPC 6 XF1 OK 58 degrees C / 136 degrees F
FPC 6 XF0 OK 65 degrees C / 149 degrees F
FPC 6 XM1 OK 39 degrees C / 102 degrees F
FPC 6 XM0 OK 66 degrees C / 150 degrees F
FPC 6 PFE0 LU1 OK 69 degrees C / 156 degrees F
FPC 6 PFE0 LU2 OK 69 degrees C / 156 degrees F
FPC 6 PFE1 LU1 OK 42 degrees C / 107 degrees F
FPM GBUS OK 24 degrees C / 75 degrees F
FPM Display OK 27 degrees C / 80 degrees F
Fans Top Left Front fan OK Spinning at high speed
### show chassis environment (TX Matrix Router)

```
user@host> show chassis environment

Class Item                         Status     Measurement
Temp PEM 0                         Absent
  PEM 1 OK                         29 degrees C / 84 degrees F
  Routing Engine 0 OK              34 degrees C / 93 degrees F
  Routing Engine 1 OK              34 degrees C / 93 degrees F
  CB 0 OK                          32 degrees C / 89 degrees F
  CB 1 OK                          32 degrees C / 89 degrees F
  SIB 0 OK                         44 degrees C / 111 degrees F
  SIB 0 (B) OK                     44 degrees C / 111 degrees F
  FPM GBUS OK                      27 degrees C / 80 degrees F
  FPM Display OK                   32 degrees C / 89 degrees F
Fans Top Left Front fan OK         Spinning at normal speed
  Top Left Middle fan OK           Spinning at normal speed
  Top Left Rear fan OK             Spinning at normal speed
  Top Right Front fan OK           Spinning at normal speed
  Top Right Middle fan OK          Spinning at normal speed
  Top Right Rear fan OK            Spinning at normal speed
  Bottom Left Front fan OK         Spinning at normal speed
  Bottom Left Middle fan OK        Spinning at normal speed
  Bottom Left Rear fan OK          Spinning at normal speed
  Bottom Right Front fan OK        Spinning at normal speed
  Bottom Right Middle fan OK       Spinning at normal speed
  Bottom Right Rear fan OK         Spinning at normal speed
  Rear Tray Top fan OK             Spinning at normal speed
  Rear Tray Second fan OK          Spinning at normal speed
  Rear Tray Third fan OK           Spinning at normal speed
  Rear Tray Fourth fan OK          Spinning at normal speed
  Rear Tray Fifth fan OK           Spinning at normal speed
  Rear Tray Sixth fan OK           Spinning at normal speed
  Rear Tray Seventh fan OK         Spinning at normal speed
Misc CIP 0 OK                      OK
  SPMB 0 OK                        OK
  SPMB 1 OK                        OK
```
### lcc0-re0:

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td></td>
<td>PEM 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCG 0</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td></td>
<td>SCG 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
<td>39 degrees C / 102 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>OK</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 0</td>
<td>OK</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 0 (B)</td>
<td>OK</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Top</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Top</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Bottom</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Bottom</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC Display</td>
<td>OK</td>
<td>30 degrees C / 86 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPM GBUS</td>
<td>OK</td>
<td>30 degrees C / 86 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td>Top Left Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Left Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Right Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Right Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Right Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Rear fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Top fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Second fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Third fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Fourth fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Fifth fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Sixth fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Seventh fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Rear Tray Bottom fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Misc</td>
<td>CIP</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SPMB 0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SPMB 1</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

### lcc2-re0:

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td></td>
<td>PEM 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCG 0</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>SCG 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>OK</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0</td>
<td>OK</td>
<td>30 degrees C / 86 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 0</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 0 (B)</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Top</td>
<td>OK</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Bottom</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 1 Top</td>
<td>OK</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
</tbody>
</table>
show chassis environment (T1600 Router)

<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 1 Bottom</td>
<td>OK</td>
<td>33 degrees C / 91 degrees F</td>
</tr>
<tr>
<td>FPM GBUS</td>
<td>OK</td>
<td>30 degrees C / 86 degrees F</td>
</tr>
<tr>
<td>FPM Display</td>
<td>OK</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Left Front fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Top Left Middle fan</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

```
user@host> show chassis environment

Class    Item                           Status     Measurement
Temp  PEM 0                          OK         27 degrees C / 80 degrees F
PEM 1    Absent                      
SCG 0                          OK         31 degrees C / 87 degrees F
SCG 1                          OK         35 degrees C / 95 degrees F
Routing Engine 0               OK         30 degrees C / 86 degrees F
Routing Engine 1               OK         30 degrees C / 86 degrees F
CB 0                          OK         31 degrees C / 87 degrees F
CB 1                          OK         31 degrees C / 87 degrees F
SIB 0                          OK         41 degrees C / 105 degrees F
SIB 0 (B)                      OK         34 degrees C / 93 degrees F
SIB 1                          OK         0 degrees C / 32 degrees F
SIB 1 (B)                      OK         0 degrees C / 32 degrees F
SIB 2                          OK         0 degrees C / 32 degrees F
SIB 2 (B)                      OK         0 degrees C / 32 degrees F
SIB 3                          OK         0 degrees C / 32 degrees F
SIB 3 (B)                      OK         0 degrees C / 32 degrees F
SIB 4                          OK         0 degrees C / 32 degrees F
SIB 4 (B)                      OK         0 degrees C / 32 degrees F
FPC 0 Top                      OK         49 degrees C / 120 degrees F
FPC 0 Bottom                   OK         50 degrees C / 122 degrees F
FPC 1 Top                      OK         48 degrees C / 118 degrees F
FPC 1 Bottom                   OK         49 degrees C / 120 degrees F
FPM GBUS                       OK         27 degrees C / 80 degrees F
FPM Display                    OK         30 degrees C / 86 degrees F
Fans    Top Left Front fan           OK         Spinning at normal speed
         Top Left Middle fan          OK         Spinning at normal speed
         Top Left Rear fan           OK         Spinning at normal speed
         Top Right Front fan         OK         Spinning at normal speed
         Top Right Middle fan        OK         Spinning at normal speed
         Top Right Rear fan          OK         Spinning at normal speed
         Bottom Left Front fan       OK         Spinning at normal speed
         Bottom Left Middle fan      OK         Spinning at normal speed
         Bottom Left Rear fan        OK         Spinning at normal speed
         Bottom Right Front fan      OK         Spinning at normal speed
         Bottom Right Middle fan     OK         Spinning at normal speed
         Bottom Right Rear fan       OK         Spinning at normal speed
         Rear Tray Top fan           OK         Spinning at normal speed
         Rear Tray Second fan        OK         Spinning at normal speed
         Rear Tray Third fan         OK         Spinning at normal speed
         Rear Tray Fourth fan        OK         Spinning at normal speed
         Rear Tray Fifth fan         OK         Spinning at normal speed
         Rear Tray Sixth fan         OK         Spinning at normal speed
         Rear Tray Seventh fan       OK         Spinning at normal speed
         Rear Tray Bottom fan        OK         Spinning at normal speed
Misc    CIP                            OK
        SPMB 0                         OK
        SPMB 1                         OK
```
show chassis environment (TX Matrix Plus Router)

```
user@host> show chassis environment
sfc0-re0:
--------------------------------------------------------------------------
Class             Item                          Status    Measurement
--------------------------------------------------------------------------
Temp              PEM 0                          OK         28 degrees C / 82 degrees F
PEM 1                          Absent
Routing Engine 0               OK         27 degrees C / 80 degrees F
Routing Engine 1               OK         29 degrees C / 84 degrees F
CB 0 Intake                   OK         25 degrees C / 77 degrees F
CB 0 Exhaust A                OK         25 degrees C / 77 degrees F
CB 0 Exhaust B                OK         25 degrees C / 77 degrees F
CB 1 Intake                   OK         26 degrees C / 78 degrees F
CB 1 Exhaust A                OK         26 degrees C / 78 degrees F
CB 1 Exhaust B                OK         26 degrees C / 78 degrees F
SIB F13 0                      OK         47 degrees C / 116 degrees F
SIB F13 0 (B)                  OK         48 degrees C / 118 degrees F
SIB F13 1                      OK         38 degrees C / 100 degrees F
SIB F13 1 (B)                  OK         37 degrees C / 98 degrees F
SIB F2S 0/0                    OK         27 degrees C / 80 degrees F
SIB F2S 0/2                    OK         28 degrees C / 82 degrees F
SIB F2S 0/4                    OK         27 degrees C / 80 degrees F
SIB F2S 0/6                    OK         28 degrees C / 82 degrees F
SIB F2S 1/0                    OK         26 degrees C / 78 degrees F
SIB F2S 1/2                    OK         26 degrees C / 78 degrees F
SIB F2S 1/4                    OK         26 degrees C / 78 degrees F
SIB F2S 1/6                    OK         26 degrees C / 78 degrees F
SIB F2S 2/0                    OK         25 degrees C / 77 degrees F
SIB F2S 2/2                    OK         25 degrees C / 77 degrees F
SIB F2S 2/4                    OK         23 degrees C / 73 degrees F
CIP 0 Intake                   OK         23 degrees C / 73 degrees F
CIP 0 Exhaust A                OK         24 degrees C / 75 degrees F
CIP 0 Exhaust B                OK         24 degrees C / 75 degrees F
CIP 1 Intake                   OK         24 degrees C / 75 degrees F
CIP 1 Exhaust A                OK         25 degrees C / 77 degrees F
CIP 1 Exhaust B                OK         25 degrees C / 77 degrees F
Fans             Fan Tray 0 Fan 1               OK         Spinning at normal speed
Fan Tray 0 Fan 2               OK         Spinning at normal speed
Fan Tray 0 Fan 3               OK         Spinning at normal speed
Fan Tray 0 Fan 4               OK         Spinning at normal speed
Fan Tray 0 Fan 5               OK         Spinning at normal speed
Fan Tray 0 Fan 6               OK         Spinning at normal speed
Fan Tray 1 Fan 1               OK         Spinning at normal speed
Fan Tray 1 Fan 2               OK         Spinning at normal speed
Fan Tray 1 Fan 3               OK         Spinning at normal speed
Fan Tray 1 Fan 4               OK         Spinning at normal speed
Fan Tray 1 Fan 5               OK         Spinning at normal speed
Fan Tray 1 Fan 6               OK         Spinning at normal speed
Fan Tray 2 Fan 1               OK         Spinning at normal speed
Fan Tray 2 Fan 2               OK         Spinning at normal speed
Fan Tray 2 Fan 3               OK         Spinning at normal speed
Fan Tray 2 Fan 4               OK         Spinning at normal speed
Fan Tray 2 Fan 5               OK         Spinning at normal speed
Fan Tray 2 Fan 6               OK         Spinning at normal speed
Fan Tray 2 Fan 7               OK         Spinning at normal speed
Fan Tray 2 Fan 8               OK         Spinning at normal speed
Fan Tray 2 Fan 9               OK         Spinning at normal speed
Fan Tray 3 Fan 1               OK         Spinning at normal speed
Fan Tray 3 Fan 2               OK         Spinning at normal speed
Fan Tray 3 Fan 3               OK         Spinning at normal speed
```
Fan Tray 3 Fan 4               OK         Spinning at normal speed
Fan Tray 3 Fan 5               OK         Spinning at normal speed
Fan Tray 3 Fan 6               OK         Spinning at normal speed
Fan Tray 3 Fan 7               OK         Spinning at normal speed
Fan Tray 3 Fan 8               OK         Spinning at normal speed
Fan Tray 3 Fan 9               OK         Spinning at normal speed
Fan Tray 4 Fan 1               OK         Spinning at normal speed
Fan Tray 4 Fan 2               OK         Spinning at normal speed
Fan Tray 4 Fan 3               OK         Spinning at normal speed
Fan Tray 4 Fan 4               OK         Spinning at normal speed
Fan Tray 4 Fan 5               OK         Spinning at normal speed
Fan Tray 4 Fan 6               OK         Spinning at normal speed
Fan Tray 4 Fan 7               OK         Spinning at normal speed
Fan Tray 4 Fan 8               OK         Spinning at normal speed
Fan Tray 4 Fan 9               OK         Spinning at normal speed
Fan Tray 5 Fan 1               OK         Spinning at normal speed
Fan Tray 5 Fan 2               OK         Spinning at normal speed
Fan Tray 5 Fan 3               OK         Spinning at normal speed
Fan Tray 5 Fan 4               OK         Spinning at normal speed
Fan Tray 5 Fan 5               OK         Spinning at normal speed
Fan Tray 5 Fan 6               OK         Spinning at normal speed
Fan Tray 5 Fan 7               OK         Spinning at normal speed
Fan Tray 5 Fan 8               OK         Spinning at normal speed
Fan Tray 5 Fan 9               OK         Spinning at normal speed
Misc  SPMB 0                     OK
SPMB 1                         OK

lcc0-re0:-----------------------------------------------------------------------
Class Item                           Status     Measurement
Temp  PEM 0                          OK         27 degrees C / 80 degrees F
PEM 1                          Absent
SCG 0                          OK         31 degrees C / 87 degrees F
SCG 1                          OK         35 degrees C / 95 degrees F
Routing Engine 0               OK         30 degrees C / 86 degrees F
Routing Engine 1               OK         30 degrees C / 86 degrees F
CB 0                           OK         31 degrees C / 87 degrees F
CB 1                           OK         31 degrees C / 87 degrees F
SIB 0                          OK         41 degrees C / 105 degrees F
SIB 0 (B)                      OK         34 degrees C / 93 degrees F
SIB 1                          OK         0 degrees C / 32 degrees F
SIB 1 (B)                      OK         0 degrees C / 32 degrees F
SIB 2                          OK         0 degrees C / 32 degrees F
SIB 2 (B)                      OK         0 degrees C / 32 degrees F
SIB 3                          OK         0 degrees C / 32 degrees F
SIB 3 (B)                      OK         0 degrees C / 32 degrees F
SIB 4                          OK         0 degrees C / 32 degrees F
SIB 4 (B)                      OK         0 degrees C / 32 degrees F
FPC 0 Top                      OK         49 degrees C / 120 degrees F
FPC 0 Bottom                   OK         50 degrees C / 122 degrees F
FPC 1 Top                      OK         48 degrees C / 118 degrees F
FPC 1 Bottom                   OK         49 degrees C / 120 degrees F
FPM GBUS                       OK         27 degrees C / 80 degrees F
FPM Display                    OK         30 degrees C / 86 degrees F
Fans  Top Left Front fan         OK         Spinning at normal speed
Top Left Middle fan            OK         Spinning at normal speed
Top Left Rear fan              OK         Spinning at normal speed
Top Right Front fan            OK         Spinning at normal speed
Top Right Middle fan           OK         Spinning at normal speed
Top Right Rear fan             OK         Spinning at normal speed
Bottom Left Front fan          OK         Spinning at normal speed
Bottom Left Middle fan   OK   Spinning at normal speed
Bottom Left Rear fan     OK   Spinning at normal speed
Bottom Right Front fan   OK   Spinning at normal speed
Bottom Right Middle fan  OK   Spinning at normal speed
Bottom Right Rear fan    OK   Spinning at normal speed
Rear Tray Top fan        OK   Spinning at normal speed
Rear Tray Second fan     OK   Spinning at normal speed
Rear Tray Third fan      OK   Spinning at normal speed
Rear Tray Fourth fan     OK   Spinning at normal speed
Rear Tray Fifth fan      OK   Spinning at normal speed
Rear Tray Sixth fan      OK   Spinning at normal speed
Rear Tray Seventh fan    OK   Spinning at normal speed
Rear Tray Bottom fan     OK   Spinning at normal speed

Misc
CIP   OK
SPMB 0  OK
SPMB 1  OK

showchassisenvironment (TX Matrix Plus router with 3D SIBs)

user@host> show chassis environment
sfc0-re0:

Class Item                           Status     Measurement
--------------------------------------------------------------------------
Temp  PEM 0                          Check      30 degrees C / 86 degrees F
PEM 1                          OK         33 degrees C / 91 degrees F
Routing Engine 0               OK         28 degrees C / 82 degrees F
Routing Engine 0 CPU           OK         42 degrees C / 107 degrees F
Routing Engine 1               OK         29 degrees C / 84 degrees F
Routing Engine 1 CPU           OK         44 degrees C / 111 degrees F
CB 0 Intake                    OK         30 degrees C / 86 degrees F
CB 0 Exhaust A                 OK         28 degrees C / 82 degrees F
CB 0 Exhaust B                 OK         30 degrees C / 86 degrees F
CB 1 Intake                    OK         31 degrees C / 87 degrees F
CB 1 Exhaust A                 OK         27 degrees C / 80 degrees F
CB 1 Exhaust B                 OK         31 degrees C / 87 degrees F
SIB F13 0 Board                OK         44 degrees C / 111 degrees F
SIB F13 0 XF Junction          OK         62 degrees C / 143 degrees F
SIB F13 3 Board                OK         45 degrees C / 113 degrees F
SIB F13 3 XF Junction          OK         60 degrees C / 140 degrees F
SIB F13 6 Board                OK         47 degrees C / 116 degrees F
SIB F13 6 XF Junction          OK         62 degrees C / 143 degrees F
SIB F2S 0/0 Board              OK         32 degrees C / 89 degrees F
SIB F2S 0/0 XF Junction        OK         42 degrees C / 107 degrees F
SIB F2S 0/2 Board              OK         31 degrees C / 87 degrees F
SIB F2S 0/2 XF Junction        OK         41 degrees C / 105 degrees F
SIB F2S 0/4 Board              OK         31 degrees C / 87 degrees F
SIB F2S 0/4 XF Junction        OK         42 degrees C / 107 degrees F
SIB F2S 0/6 Board              OK         31 degrees C / 87 degrees F
SIB F2S 0/6 XF Junction        OK         41 degrees C / 105 degrees F
SIB F2S 1/0 Board              OK         31 degrees C / 87 degrees F
SIB F2S 1/0 XF Junction        OK         41 degrees C / 105 degrees F
SIB F2S 1/2 Board              OK         29 degrees C / 84 degrees F
SIB F2S 1/2 XF Junction        OK         39 degrees C / 102 degrees F
SIB F2S 1/4 Board              OK         29 degrees C / 84 degrees F
SIB F2S 1/4 XF Junction        OK         35 degrees C / 95 degrees F
SIB F2S 1/6 Board              OK         30 degrees C / 86 degrees F
SIB F2S 1/6 XF Junction        OK         41 degrees C / 105 degrees F
SIB F2S 2/0 Board              OK         30 degrees C / 86 degrees F
SIB F2S 2/0 XF Junction        OK         42 degrees C / 107 degrees F
SIB F2S 2/2 Board              OK         28 degrees C / 82 degrees F
SIB F2S 2/2 XF Junction        OK         39 degrees C / 102 degrees F
<table>
<thead>
<tr>
<th>Component</th>
<th>Status</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIB F2S 2/4 Board</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td>SIB F2S 2/4 XF Junction</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td>SIB F2S 2/6 Board</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td>SIB F2S 2/6 XF Junction</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>CIP 0 Intake</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
</tr>
<tr>
<td>CIP 0 Exhaust A</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
</tr>
<tr>
<td>CIP 0 Exhaust B</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
</tr>
<tr>
<td>CIP 1 Intake</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
</tr>
<tr>
<td>CIP 1 Exhaust A</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
</tr>
<tr>
<td>CIP 1 Exhaust B</td>
<td>OK</td>
<td>27 degrees C / 80 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan Tray 0 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 0 Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 1 Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 7</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 8</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 2 Fan 9</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 7</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 8</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 3 Fan 9</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 7</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 8</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 4 Fan 9</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 7</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 8</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fan Tray 5 Fan 9</td>
<td>Check</td>
<td></td>
</tr>
<tr>
<td>Misc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPMB 0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>SPMB 1</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td>Class</td>
<td>Item</td>
<td>Status</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Temp</td>
<td>PEM 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>PEM 1</td>
<td>Check</td>
</tr>
<tr>
<td></td>
<td>SCG 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SCG 1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 0 CPU</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Routing Engine 1 CPU</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>CB 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>CB 1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 0 (B)</td>
<td>Absent</td>
</tr>
<tr>
<td></td>
<td>SIB 1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 1 (B)</td>
<td>Absent</td>
</tr>
<tr>
<td></td>
<td>SIB 2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>SIB 2 (B)</td>
<td>Absent</td>
</tr>
<tr>
<td></td>
<td>FPC 4 Top</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 4 Bottom</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 Fan Intake</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 Fan Exhaust</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 PMB</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 LMB0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 LMB1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 LMB2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 PFE1 LU2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 PFE1 LU0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 PFE0 LU0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 XF1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 XF0</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 XM1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 XMO</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 PFE0 LU1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 PFE0 LU2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPC 7 PFE1 LU1</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPM GBUS</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>FPM Display</td>
<td>OK</td>
</tr>
<tr>
<td>Fans</td>
<td>Top Left Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Top Left Middle fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Top Left Rear fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Top Right Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Top Right Middle Fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Top Right Rear fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Middle fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Left Rear fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Front fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Middle fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Bottom Right Rear fan</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray 1 (Top)</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 2</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 3</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 4</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 5</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 6</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 7</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 8</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 9</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Rear Tray fan 10</td>
<td>OK</td>
</tr>
</tbody>
</table>
show chassis environment (EX4200 Standalone Switch)

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>FPC 0 Power Supply 0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FPC 0 Power Supply 1</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>Temp</td>
<td>FPC 0 CPU</td>
<td>OK</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 EX-PFE1</td>
<td>OK</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 EX-PFE2</td>
<td>OK</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 GEPHY Front Left</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 GEPHY Front Right</td>
<td>OK</td>
<td>27 degrees C / 82 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Uplink Conn</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td>FPC 0 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>FPC 0 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>

show chassis environment (EX8216 Switch)

<table>
<thead>
<tr>
<th>Class</th>
<th>Item</th>
<th>Status</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>PSU 0</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSU 1</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSU 2</td>
<td>OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSU 3</td>
<td>Check</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSU 4</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PSU 5</td>
<td>Absent</td>
<td></td>
</tr>
<tr>
<td>Temp</td>
<td>CB 0 Intake</td>
<td>OK</td>
<td>23 degrees C / 73 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 0 Exhaust</td>
<td>OK</td>
<td>26 degrees C / 78 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Intake</td>
<td>OK</td>
<td>22 degrees C / 71 degrees F</td>
</tr>
<tr>
<td></td>
<td>CB 1 Exhaust</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 4 Intake</td>
<td>OK</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td></td>
<td>FPC 4 Exhaust</td>
<td>OK</td>
<td>59 degrees C / 138 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 5 Intake</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 5 Exhaust</td>
<td>OK</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 6 Intake</td>
<td>OK</td>
<td>25 degrees C / 77 degrees F</td>
</tr>
<tr>
<td></td>
<td>SIB 6 Exhaust</td>
<td>OK</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>Fans</td>
<td>Top Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 7</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 8</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Top Fan 9</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td></td>
<td>Bottom Fan 6</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
Bottom Fan 7                  OK         Spinning at normal speed  
Bottom Fan 8                  OK         Spinning at normal speed  
Bottom Fan 9                  OK         Spinning at normal speed

show chassis environment (QFX Series)

```
user@switch> show chassis environment
Class  Item                           Status     Measurement
Power  FPC 0 Power Supply 0           OK
FPC 0 Power Supply 1           OK
Temp   FPC 0 Sensor TopLeft I         OK         26 degrees C / 78 degrees F
FPC 0 Sensor TopRight I        OK         24 degrees C / 75 degrees F
FPC 0 Sensor TopLeft E         OK         30 degrees C / 86 degrees F
FPC 0 Sensor TopRight E        OK         30 degrees C / 86 degrees F
FPC 0 Sensor TopMiddle I       OK         30 degrees C / 86 degrees F
FPC 0 Sensor TopMiddle E       OK         38 degrees C / 100 degrees F
FPC 0 Sensor Bottom I          OK         38 degrees C / 100 degrees F
FPC 0 Sensor Bottom E          OK         38 degrees C / 100 degrees F
FPC 0 Sensor Die Temp          OK         38 degrees C / 100 degrees F
FPC 0 Sensor Mgmnt Brd I       OK         24 degrees C / 75 degrees F
FPC 0 Sensor Switch I          OK         28 degrees C / 82 degrees F
Fans  FPC 0 Fan 1 (left)             Failed
FPC 0 Fan 2 (right)            OK         Spinning at normal speed
FPC 0 Fan 3 (middle)           OK         Spinning at normal speed
```

show chassis environment interconnect-device (QFabric System)

```
user@switch> show chassis environment interconnect-device IC-A0004
Class  Item                          Status     Measurement
CB 0                               OK     30 degrees C / 86 degrees F
CB 0 L Intake                      OK     31 degrees C / 87 degrees F
CB 0 L Exhaust                     OK     32 degrees C / 89 degrees F
CB 0 R Exhaust                     OK     33 degrees C / 91 degrees F
Routing Engine 0 CPU temp          OK     51 degrees C / 123 degrees F
CB 1                               OK     27 degrees C / 80 degrees F
CB 1 L Intake                      OK     29 degrees C / 84 degrees F
CB 1 L Exhaust                     OK     31 degrees C / 87 degrees F
CB 1 R Exhaust                     OK     32 degrees C / 89 degrees F
Routing Engine 1 CPU temp          OK     40 degrees C / 104 degrees F
FC 0 FPC 0                         OK     25 degrees C / 77 degrees F
FC 0 L Intake                      OK     28 degrees C / 82 degrees F
FC 0 L Exhaust                     OK     28 degrees C / 82 degrees F
FC 0 R Exhaust                     OK     29 degrees C / 84 degrees F
FC 7 FPC 7                         OK     25 degrees C / 77 degrees F
FC 7 L Intake                      OK     26 degrees C / 78 degrees F
FC 7 L Exhaust                     OK     28 degrees C / 82 degrees F
FC 7 R Exhaust                     OK     29 degrees C / 84 degrees F
RC 0 FPC 8                         OK     25 degrees C / 77 degrees F
FC 8 L Intake                      OK     26 degrees C / 78 degrees F
FC 8 L Exhaust                     OK     32 degrees C / 89 degrees F
FC 8 R Exhaust                     OK     30 degrees C / 86 degrees F
RC 7 FPC 15                        OK     24 degrees C / 75 degrees F
FPC 15 L Intake                    OK     25 degrees C / 77 degrees F
FPC 15 R Intake                    OK     25 degrees C / 77 degrees F
FPC 15 L Exhaust                   OK     33 degrees C / 91 degrees F
FPC 15 R Exhaust                   OK     31 degrees C / 87 degrees F
```
<table>
<thead>
<tr>
<th>Fans</th>
<th>TFT 0 Fan 0</th>
<th>OK</th>
<th>Spinning at normal speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fans</td>
<td>TFT 0 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>TFT 0 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>TFT 0 Fan 3</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>TFT 0 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>TFT 0 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>BFT 1 Fan 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>BFT 1 Fan 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>BFT 1 Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>BFT 1 Fan 3</td>
<td>Check</td>
<td></td>
</tr>
<tr>
<td>Fans</td>
<td>BFT 1 Fan 4</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>BFT 1 Fan 5</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 0 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 0 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 1 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 1 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 2 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 2 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 3 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 0 Fan 3 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 0 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 0 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 1 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 1 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 2 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 2 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 3 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 1 Fan 3 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 0 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 0 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 1 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 1 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 2 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 2 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 3 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 2 Fan 3 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 0 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 0 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 1 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 1 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 2 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 2 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 3 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 3 Fan 3 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 0 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 0 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 1 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 1 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 2 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 2 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 3 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 4 Fan 3 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 0 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 0 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 1 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 1 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 2 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 2 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 3 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 5 Fan 3 Rotor 1</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
<tr>
<td>Fans</td>
<td>SFT 6 Fan 0 Rotor 0</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
Fans  SFT 6 Fan 0 Rotor 1            OK         Spinning at normal speed
Fans  SFT 6 Fan 1 Rotor 0            OK         Spinning at normal speed
Fans  SFT 6 Fan 1 Rotor 1            OK         Spinning at normal speed
Fans  SFT 6 Fan 2 Rotor 0            OK         Spinning at normal speed
Fans  SFT 6 Fan 2 Rotor 1            OK         Spinning at normal speed
Fans  SFT 6 Fan 3 Rotor 0            OK         Spinning at normal speed
Fans  SFT 6 Fan 3 Rotor 1            OK         Spinning at normal speed
Fans  SFT 7 Fan 0 Rotor 0            OK         Spinning at normal speed
Fans  SFT 7 Fan 0 Rotor 1            OK         Spinning at normal speed
Fans  SFT 7 Fan 1 Rotor 0            OK         Spinning at normal speed
Fans  SFT 7 Fan 1 Rotor 1            OK         Spinning at normal speed
Fans  SFT 7 Fan 2 Rotor 0            OK         Spinning at normal speed
Fans  SFT 7 Fan 2 Rotor 1            OK         Spinning at normal speed
Fans  SFT 7 Fan 3 Rotor 0            OK         Spinning at normal speed
Fans  SFT 7 Fan 3 Rotor 1            OK         Spinning at normal speed
Power PEM 0                          OK         30 degrees C / 86 degrees F
Power PEM 1                          OK         30 degrees C / 86 degrees F
Power PEM 2                          OK         30 degrees C / 86 degrees F
Power PEM 3                          Absent
Power PEM 4                          Absent
Power PEM 5                          Absent

show chassis environment node-device (QFabric System)

user@switch>  show chassis environment node-device node1

Class Item                           Status     Measurement
Power node1 Power Supply 0            Absent
node1 Power Supply 1            Absent
Fans  node1 Fan Tray 0                Testing
node1 Fan Tray 1                Testing
node1 Fan Tray 2                Testing

show chassis environment pem node-device (QFabric System)

user@switch>  show chassis environment pem node-device node1

FPC 0 PEM 0 status:
State                      Check
Airflow                    Front to Back
Temperature                OK
AC Input:                  OK
DC Output           Voltage(V) Current(A)  Power(W)  Load(%)
12        10            120      18

FPC 0 PEM 1 status:
State                      Online
Airflow                    Back to Front
Temperature                OK
AC Input:                  OK
DC Output           Voltage(V) Current(A)  Power(W)  Load(%)
11        10           110      17

show chassis environment (PTX5000 Packet Transport Router)

user@switch>  show chassis environment

Class Item                           Status     Measurement
Temp  PDU 0                          OK         36 degrees C / 96 degrees F
PDU 0 PSM 0                    OK         38 degrees C / 100 degrees F
PDU 0 PSM 1                    OK         38 degrees C / 100 degrees F
PDU 0 PSM 2                    OK         37 degrees C / 98 degrees F
PDU 0 PSM 3                    OK         Absent
PDU 1                          OK         44 degrees C / 111 degrees F
CCG 0                          OK         44 degrees C / 111 degrees F
FPC 3 TL2                      OK         56 degrees C / 132 degrees F
FPC 3 TQ2                      OK         59 degrees C / 138 degrees F
FPC 3 TL3                      OK         62 degrees C / 143 degrees F
FPC 3 TQ3                      OK         63 degrees C / 145 degrees F
PIC 3/1                       Absent
FPC 5 PMB                      OK         35 degrees C / 95 degrees F
FPC 5 Intake                   OK         34 degrees C / 93 degrees F
FPC 5 Exhaust A                OK         51 degrees C / 123 degrees F
FPC 5 Exhaust B                OK         53 degrees C / 127 degrees F
FPC 5 TL0                      OK         54 degrees C / 129 degrees F
FPC 5 TQ0                      OK         52 degrees C / 125 degrees F
FPC 5 TL1                      OK         61 degrees C / 141 degrees F
FPC 5 TQ1                      OK         60 degrees C / 140 degrees F
FPC 5 TL2                      OK         55 degrees C / 131 degrees F
FPC 5 TQ2                      OK         55 degrees C / 131 degrees F
FPC 5 TL3                      OK         59 degrees C / 138 degrees F
FPC 5 TQ3                      OK         58 degrees C / 136 degrees F
PIC 5/0 Ambient                OK         51 degrees C / 123 degrees F
PIC 5/1 Ambient                OK         34 degrees C / 93 degrees F
PIC 5/1 cfp-5/1/0              OK         34 degrees C / 93 degrees F
PIC 5/1 cfp-5/1/1              OK         36 degrees C / 96 degrees F
FPC 6 PMB                      OK         36 degrees C / 96 degrees F
FPC 6 Intake                   OK         33 degrees C / 91 degrees F
FPC 6 Exhaust A                OK         51 degrees C / 123 degrees F
FPC 6 Exhaust B                OK         39 degrees C / 102 degrees F
FPC 6 TL0                      OK         44 degrees C / 111 degrees F
FPC 6 TQ0                      OK         54 degrees C / 129 degrees F
FPC 6 TL1                      OK         59 degrees C / 138 degrees F
FPC 6 TQ1                      OK         58 degrees C / 136 degrees F
FPC 6 TL2                      OK         60 degrees C / 140 degrees F
FPC 6 TQ2                      OK         57 degrees C / 134 degrees F
FPC 6 TL3                      OK         65 degrees C / 149 degrees F
FPC 6 TQ3                      OK         60 degrees C / 140 degrees F
FPC 7 PMB                      OK         35 degrees C / 95 degrees F
FPC 7 Intake                   OK         33 degrees C / 91 degrees F
FPC 7 Exhaust A                OK         53 degrees C / 127 degrees F
FPC 7 Exhaust B                OK         40 degrees C / 104 degrees F
FPC 7 TL0                      OK         46 degrees C / 114 degrees F
FPC 7 TQ0                      OK         58 degrees C / 136 degrees F
FPC 7 TL1                      OK         53 degrees C / 127 degrees F
FPC 7 TQ1                      OK         59 degrees C / 138 degrees F
FPC 7 TL2                      OK         56 degrees C / 132 degrees F
FPC 7 TQ2                      OK         61 degrees C / 141 degrees F
FPC 7 TL3                      OK         63 degrees C / 145 degrees F
FPC 7 TQ3                      OK         63 degrees C / 145 degrees F
FPM I2CS                       OK         37 degrees C / 98 degrees F

Fans
Fan Tray 0 Fan 1              OK         3042 RPM
Fan Tray 0 Fan 2              OK         3042 RPM
Fan Tray 0 Fan 3              OK         3000 RPM
Fan Tray 0 Fan 4              OK         3042 RPM
Fan Tray 0 Fan 5              OK         3000 RPM
Fan Tray 0 Fan 6              OK         3042 RPM
Fan Tray 0 Fan 7              OK         3085 RPM
Fan Tray 0 Fan 8              OK         3042 RPM
Fan Tray 0 Fan 9              OK         3042 RPM
Fan Tray 0 Fan 10             OK         3085 RPM
Fan Tray 0 Fan 11             OK         3085 RPM
Fan Tray 0 Fan 12             OK         3128 RPM
Fan Tray 0 Fan 13             OK         3128 RPM
Fan Tray 0 Fan 14             OK         3042 RPM
Fan Tray 1 Fan 1              OK         2299 RPM
Fan Tray 1 Fan 2               OK         2399 RPM
Fan Tray 1 Fan 3               OK         2299 RPM
Fan Tray 1 Fan 4               OK         2266 RPM
Fan Tray 1 Fan 5               OK         2266 RPM
Fan Tray 1 Fan 6               OK         2366 RPM
Fan Tray 2 Fan 1               OK         2199 RPM
Fan Tray 2 Fan 2               OK         2133 RPM
Fan Tray 2 Fan 3               OK         2366 RPM
Fan Tray 2 Fan 4               OK         2233 RPM
Fan Tray 2 Fan 5               OK         2399 RPM
Fan Tray 2 Fan 6               OK         2233 RPM
Misc SPMB 0 Intake                  OK         50 degrees C / 122 degrees F
SPMB 1 Intake                  OK         40 degrees C / 104 degrees F

show chassis environment (ACX2000 Universal Access Router)

user@host> show chassis environment

Class       Item               Status     Measurement
PCB Left    OK         44 degrees C / 111 degrees F
SFP+ Xcvr   OK         50 degrees C / 122 degrees F
FEB         OK         70 degrees C / 158 degrees F
PCB Up      OK         63 degrees C / 145 degrees F
PCB Mid     OK         66 degrees C / 150 degrees F
Telecom Mod OK         65 degrees C / 149 degrees F
Routing Engine OK         54 degrees C / 129 degrees F
Heater off

show chassis environment (ACX4000 Universal Access Router)

On the ACX4000 router, the MIC output of the show chassis environment command varies depending on the number of temperature channels present in the installed MIC.

user@host> show chassis environment

Class       Item               Status     Measurement
Temp PEM 0   OK         33 degrees C / 91 degrees F
PEM 1        Absent
PCB Bottom   OK         30 degrees C / 86 degrees F
PCB Middle   OK         34 degrees C / 93 degrees F
BCM56445     OK         33 degrees C / 91 degrees F
SFP+ Xcvr     OK         32 degrees C / 89 degrees F
Fan tray inlet OK         39 degrees C / 102 degrees F
Exhaust      OK         30 degrees C / 86 degrees F
Routing Engine OK         32 degrees C / 89 degrees F
Heater off
Pic PIC 0/0 Channel 0     OK         28 degrees C / 82 degrees F
PIC 0/0 Channel 1     OK         29 degrees C / 84 degrees F
PIC 0/0 Channel 2     OK         0 degrees C / 32 degrees F
PIC 0/0 Channel 3     OK         0 degrees C / 32 degrees F
PIC 0/0 Channel 4     OK         0 degrees C / 32 degrees F
PIC 0/0 Channel 5     OK         0 degrees C / 32 degrees F
PIC 0/0 Channel 6     OK         0 degrees C / 32 degrees F
PIC 0/0 Channel 7     OK         0 degrees C / 32 degrees F
PIC 0/0 Channel 8     OK         0 degrees C / 32 degrees F
PIC 0/0 Channel 9     OK         0 degrees C / 32 degrees F
PIC 1/0 Channel 0     OK         33 degrees C / 91 degrees F
PIC 1/0 Channel 1     OK         31 degrees C / 87 degrees F
PIC 1/0 Channel 2     OK         30 degrees C / 86 degrees F
PIC 1/0 Channel 3     OK         0 degrees C / 32 degrees F
PIC 1/0 Channel 4     OK         0 degrees C / 32 degrees F
PIC 1/0 Channel 5     OK         0 degrees C / 32 degrees F

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>PIC 1/0 Channel 6</th>
<th>OK</th>
<th>0 degrees C / 32 degrees F</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIC 1/0 Channel 7</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>PIC 1/0 Channel 8</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 0</td>
<td>OK</td>
<td>31 degrees C / 87 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 1</td>
<td>OK</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 2</td>
<td>OK</td>
<td>28 degrees C / 82 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 3</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 4</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 5</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 6</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 7</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>PIC 1/1 Channel 8</td>
<td>OK</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
</tbody>
</table>

**Fans**

<table>
<thead>
<tr>
<th>Fan 1</th>
<th>OK</th>
<th>Spinning at normal speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan 2</td>
<td>OK</td>
<td>Spinning at normal speed</td>
</tr>
</tbody>
</table>
show chassis environment cb

Syntax

show chassis environment cb
<slot>

Syntax (TX Matrix Routers)

show chassis environment cb
<lcc number | scc>
<slot>

Syntax (TX Matrix Plus Routers)

show chassis environment cb
<lcc number | sfc number>
<slot>

Syntax (MX Series Routers)

show chassis environment cb
<slot>
<all-members>
<local>
<member member-id>

Syntax (MX104 3D Universal Edge Routers)

show chassis environment cb

Syntax (MX2010 and MX2020 3D Universal Edge Routers)

show chassis environment cb
<slot>

Syntax (QFabric System)

show chassis environment cb
<slot interconnect-device interconnect-device-name>
<interconnect-device interconnect-device-name slot>

Release Information

Command introduced before Junos Release 7.4.
Command introduced in Junos OS Release 9.4 for EX Series switches.
Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
Command introduced in Junos OS Release 12.1 for T4000 Core Routers.
sfc option introduced for the TX Matrix Plus router in Junos Release 9.6.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

Description

(M120, M320, MX Series, and T Series routers, EX8200 switches, and PTX Series Packet Transport Routers only) Display environmental information about the Control Boards (CBs). For information about the meaning of “CBs” on the switches, see “EX Series Switches Hardware and CLI Terminology Mapping” on page 389.

Options

none—Display environmental information about all CBs. For a TX Matrix router, display environmental information about all CBs on the TX Matrix router and its attached T640 routers. For a TX Matrix Plus router, display environmental information about all CBs on the TX Matrix Plus router and its attached T1600 or T4000 routers.
all-members—(MX Series routers only) (Optional) Display environmental information about the CBs on all the members of the Virtual Chassis configuration.

interconnect-device—(QFabric systems only) Display environmental information about CBs on the Interconnect device.

lcc number—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.
Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers only) (Optional) Display environmental information about the CBs on the local Virtual Chassis member.

member member-id—(MX Series routers only) (Optional) Display environmental information about the CBs on the specified member of the Virtual Chassis configuration. Replace member-id with a value of 0 or 1.

scc—(TX Matrix router only) (Optional) Display environmental information about the CBs in the TX Matrix router (switch-card chassis).

sfc number—(TX Matrix Plus router only) (Optional) Display environmental information about the CBs in the TX Matrix Plus router (or switch-fabric chassis).

slot—(Optional) Display environmental information about the specified CB. On routers and PTX Series Packet Transport Routers, replace slot with 0 or 1. On EX Series switches replace slot with 0, 1, or 2. On QFX Series switches, replace slot with 0 or 1.

Required Privilege Level

view

Related Documentation

- request chassis cb on page 744
- Switching Control Board Redundancy
- Routing Engine and Switching Control Board Redundancy Configuration Statements

List of Sample Output

show chassis environment cb (M120 Router) on page 827
show chassis environment cb (M320 Router) on page 827
show chassis environment cb (MX80 Router) on page 828
show chassis environment cb (MX104 Router) on page 828
show chassis environment cb (MX240 Router) on page 828
show chassis environment cb (MX240 Router with Enhanced MX SCB) on page 829
show chassis environment cb (MX480 Router) on page 829
show chassis environment cb (MX480 Router with Enhanced MX SCB) on page 830
show chassis environment cb (MX960 Router) on page 830
show chassis environment cb (MX960 Router with Enhanced MX SCB) on page 831
show chassis environment cb (MX2020 Router) on page 831
show chassis environment cb (MX2010 Router) on page 832
show chassis environment cb (T4000 Core Router) on page 833
show chassis environment cb (TX Matrix Router) on page 833
show chassis environment cb (TX Matrix Plus Router) on page 834
show chassis environment cb (EX8200 Switch) on page 837
show chassis environment cb (EX8208 Switch) on page 839
show chassis environment cb (PTX5000 Packet Transport Router) on page 840
show chassis environment cb (QFabric System) on page 841

**Output Fields**

Table 140 on page 826 lists the output fields for the `show chassis environment cb` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Status of the CB. If two CBs are installed and online, one is functioning as the master, and the other is the standby.</td>
</tr>
</tbody>
</table>
|                | • **Online**—CB is online and running.  
|                | • **Offline**—CB is powered down.                                                                                                                                                                                                                                                                                                                 |
| **NOTE:**      | On the EX8208 switch, the installation can include three CBs. See “EX Series Switches Hardware and CLI Terminology Mapping” on page 389.                                                                                                                                                                                                                  |
| **Temperature**| Temperature in Celsius (C) and Fahrenheit (F) of the air flowing past the CB.                                                                                                                                                                                                                                                                                                                            |
|                | • **Temperature Intake**—Measures the temperature of the air intake to cool the power supplies.  
|                | • **Temperature Exhaust**—Measures the temperature of the hot air exhaust.                                                                                                                                                                                                                                                                                                                             |
| **NOTE:**      | On the MX2010 and MX2020 routers, the intake temperature measures the temperature of the air intake to cool the Control Board (CB). The MX2010 and MX2020 routers include intake and exhaust temperatures for multiple zones (Intake A, Intake B, Intake C, Exhaust A, Exhaust B, and TCBC). |
| **Power**      | Power required and measured on the CB. The left column displays the required power, in volts. The right column displays the measured power, in millivolts.                                                                                                                                                                                               |
|                | **BUS Revision**—Revision level of the generic bus device. (Not on switches.)                                                                                                                                                                                                                                                                                                                                 |
| **FPGA Revision**| Revision level of the field-programmable gate array (FPGA). (Not on switches.)                                                                                                                                                                                                                                                                                                                               |
Table 140: show chassis environment cb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMBus device (on MX240, MX480, and MX960 routers with Enhanced MX SCB)</td>
<td>Enhanced SCB on MX 240, MX480, and MX960 routers allows the system to save power by supplying only the amount of voltage that is required. Configurable PMBus devices are used to provide the voltage for each individual device. There is one PMBus device for each XF ASIC so that the output can be customized to each device. The following PMBus device information is displayed for routers with Enhanced MX SCB:</td>
</tr>
<tr>
<td>Expected voltage</td>
<td></td>
</tr>
<tr>
<td>Measured voltage</td>
<td></td>
</tr>
<tr>
<td>Measured current</td>
<td></td>
</tr>
<tr>
<td>Calculated power</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show chassis environment cb (M120 Router)

```
user@host> show chassis environment cb
CB 0 status:
  State                      Online Master
  Temperature                33 degrees C / 91 degrees F
  Power:
  1.2 V                     1214 mV
  1.5 V                     1495 mV
  2.5 V                     2494 mV
  3.3 V                     3319 mV
  5.0 V                     5085 mV
  3.3 V bias                3296 mV
  Bus Revision               12
  FPGA Revision              17
CB 1 status:
  State                      Online Standby
  Temperature                34 degrees C / 93 degrees F
  Power:
  1.2 V                     1195 mV
  1.5 V                     1495 mV
  2.5 V                     2504 mV
  3.3 V                     3312 mV
  5.0 V                     5111 mV
  3.3 V bias                3296 mV
  Bus Revision               12
  FPGA Revision              17
```

show chassis environment cb (M320 Router)

```
user@host> show chassis environment cb
CB 0 status:
  State                      Online Master
  Temperature                29 degrees C / 84 degrees F
  Power:
  1.8 V                    1805 mV
  2.5 V                    2501 mV
  3.3 V                    3293 mV
  4.6 V                    4725 mV
  5.0 V                    5032 mV
  12.0 V                   11975 mV
  3.3 V bias               3286 mV
```

Copyright © 2013, Juniper Networks, Inc.
show chassis environment cb (MX80 Router)

user@host> show chassis environment cb
CB 0 status:
  State                      Online Master
  Temperature                36 degrees C / 96 degrees F
  Power 1
    1.0 V                     1034 mV
    1.0 V MQ                  1037 mV
    1.0 V LU                  1005 mV
    1.2 V                     1218 mV
    1.5 V                     1524 mV
    1.8 V                     1814 mV
    2.5 V                     2558 mV
    3.3 V                     3296 mV
    5.0 V                     5233 mV
    5.0 V bias                5207 mV
    12.0 V                   12162 mV

show chassis environment cb (MX104 Router)

user@host > show chassis environment cb
CB 0 status:
  State                      Online Master
  Temperature                33 degrees C / 91 degrees F
  Power 1
    0.75 V                   751 mV
    1.0 V                     1005 mV
    1.1 V                     1113 mV
    1.5 V                     1494 mV
    2.5 V                     2518 mV
    3.3 V                     3338 mV
    5.0 V                     4960 mV
    12.0 V                   12006 mV
  FPGA Revision              25
CB 1 status:
  State                      Empty

show chassis environment cb (MX240 Router)

user@host> show chassis environment cb
CB 0 status:
  State                      Online Standby
  Temperature                37 degrees C / 98 degrees F
### Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Measured Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 V</td>
<td>1208 mV</td>
</tr>
<tr>
<td>1.5 V</td>
<td>1521 mV</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1811 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2513 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3332 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>5059 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>12162 mV</td>
</tr>
<tr>
<td>1.25 V</td>
<td>1260 mV</td>
</tr>
<tr>
<td>3.3 V SM3</td>
<td>3306 mV</td>
</tr>
<tr>
<td>5.0 V RE</td>
<td>5085 mV</td>
</tr>
<tr>
<td>12.0 V RE</td>
<td>11872 mV</td>
</tr>
</tbody>
</table>

### Power 2

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Measured Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 V bias PEM</td>
<td>11272 mV</td>
</tr>
<tr>
<td>4.6 V bias MidPlane</td>
<td>4827 mV</td>
</tr>
<tr>
<td>11.3 V bias FPD</td>
<td>11272 mV</td>
</tr>
<tr>
<td>11.3 V bias POE 0</td>
<td>11292 mV</td>
</tr>
<tr>
<td>11.3 V bias POE 1</td>
<td>11253 mV</td>
</tr>
</tbody>
</table>

**Bus Revision** 42

**FPGA Revision** 1

### show chassis environment cb (MX240 Router with Enhanced MX SCB)

**user@host> show chassis environment cb**

**CB 0 status:**

- **State** Online Standby
- **Temperature** 37 degrees C / 98 degrees F

**Power 1**

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Measured Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 V</td>
<td>1208 mV</td>
</tr>
<tr>
<td>1.5 V</td>
<td>1521 mV</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1811 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2513 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3332 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>5059 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>12162 mV</td>
</tr>
<tr>
<td>1.25 V</td>
<td>1260 mV</td>
</tr>
<tr>
<td>3.3 V SM3</td>
<td>3306 mV</td>
</tr>
<tr>
<td>5.0 V RE</td>
<td>5085 mV</td>
</tr>
<tr>
<td>12.0 V RE</td>
<td>11872 mV</td>
</tr>
</tbody>
</table>

**Power 2**

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Measured Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 V bias PEM</td>
<td>11272 mV</td>
</tr>
<tr>
<td>4.6 V bias MidPlane</td>
<td>4827 mV</td>
</tr>
<tr>
<td>11.3 V bias FPD</td>
<td>11272 mV</td>
</tr>
<tr>
<td>11.3 V bias POE 0</td>
<td>11292 mV</td>
</tr>
<tr>
<td>11.3 V bias POE 1</td>
<td>11253 mV</td>
</tr>
</tbody>
</table>

- **Bus Revision** 42
- **FPGA Revision** 1

### show chassis environment cb (MX480 Router)

**user@host> show chassis environment cb**

**CB 0 status:**

- **State** Online Master
- **Temperature** 41 degrees C / 105 degrees F

**Power 1**

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Measured Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 V</td>
<td>1202 mV</td>
</tr>
<tr>
<td>1.5 V</td>
<td>1511 mV</td>
</tr>
</tbody>
</table>

---

Copyright © 2013, Juniper Networks, Inc.
show chassis environment cb (MX480 Router with Enhanced MX SCB)

user@host> show chassis environment cb
CB 0 status:
  State                      Online Master
  Temperature                41 degrees C / 105 degrees F

Power 1
  1.2 V                     1202 mV
  1.5 V                     1511 mV
  1.8 V                     1798 mV
  2.5 V                     2507 mV
  3.3 V                     3312 mV
  5.0 V                     5027 mV
  12.0 V                   12200 mV
  1.25 V                    1260 mV
  3.3 V SM3                 3293 mV
  5 V RE                    5040 mV
  12 V RE                   11910 mV

Power 2
  11.3 V bias PEM           11156 mV
  4.6 V bias MidPlane       4801 mV
  11.3 V bias FPD           11214 mV
  11.3 V bias POE 0         11098 mV
  11.3 V bias POE 1         11330 mV
  Bus Revision              42
  FPGA Revision             1

show chassis environment cb (MX960 Router)

user@host> show chassis environment cb
CB 0 status:
  State                      Online Master
  Temperature                24 degrees C / 75 degrees F

Power 1
  1.2 V                     1965 mV
  1.5 V                     2465 mV
  1.8 V                     2990 mV
  2.5 V                     3296 mV
  3.3 V                     3296 mV

show chassis environment cb (MX960 Router)
show chassis environment cb (MX960 Router with Enhanced MX SCB)

user@host> show chassis environment cb
CB 0 status:
State                      Online Master
Temperature                24 degrees C / 75 degrees F
Power 1
 1.2 V                     1965 mV
 1.5 V                     2465 mV
 1.8 V                     2990 mV
 2.5 V                     3296 mV
 3.3 V                     3296 mV
 5.0 V                     6593 mV
12.0 V                   13187 mV
3.3 V bias                3296 mV
1.25 V                    1994 mV
3.3 V SM3                 3296 mV
5 V RE                    6593 mV
12 V RE                  13174 mV
Power 2                    Sensor failure
Bus Revision               4
FPGA Revision              3

show chassis environment cb (MX2020 Router)

user@host> show chassis environment cb
CB 0 status:
State                      Online Master
IntakeA-Zone0 Temperature  44 degrees C / 111 degrees F
IntakeB-Zone1 Temperature  34 degrees C / 93 degrees F
IntakeC-Zone0 Temperature  45 degrees C / 113 degrees F
ExhaustA-Zone0 Temperature 43 degrees C / 109 degrees F
ExhaustB-Zone1 Temperature 36 degrees C / 96 degrees F
TCBC-Zone0 Temperature     39 degrees C / 102 degrees F
Power 1
 1.0 V                     1011 mV
 1.2 V                     1208 mV
 1.8 V                     1801 mV
 2.5 V                     2552 mV
 3.3 V                     3312 mV
 5.0 V                     5040 mV
 5.0 V RE                  4988 mV
12.0 V                   12065 mV
12.0 V RE                12046 mV
Bus Revision               99
FPGA Revision              270
CB 1 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online Standby</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntakeA-Zone0 Temp.</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>IntakeB-Zone1 Temp.</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>IntakeC-Zone0 Temp.</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>ExhaustA-Zone0 Temp.</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>ExhaustB-Zone1 Temp.</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>TCBC-Zone0 Temp.</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
</tbody>
</table>

Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V</td>
<td>1008</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1208</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1798</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2539</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3325</td>
</tr>
<tr>
<td>5.0 V</td>
<td>5033</td>
</tr>
<tr>
<td>5.0 V RE</td>
<td>4950</td>
</tr>
<tr>
<td>12.0 V</td>
<td>12046</td>
</tr>
<tr>
<td>12.0 V RE</td>
<td>11968</td>
</tr>
</tbody>
</table>

Bus Revision: 99
FPGA Revision: 0

show chassis environment cb (MX2010 Router)

user@host> show chassis environment cb

CB 0 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntakeA-Zone0 Temp.</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>IntakeB-Zone1 Temp.</td>
<td>30 degrees C / 86 degrees F</td>
</tr>
<tr>
<td>IntakeC-Zone0 Temp.</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>ExhaustA-Zone0 Temp.</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>ExhaustB-Zone1 Temp.</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
<tr>
<td>TCBC-Zone0 Temp.</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
</tbody>
</table>

Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V</td>
<td>1015</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1205</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1804</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2552</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3325</td>
</tr>
<tr>
<td>5.0 V</td>
<td>5020</td>
</tr>
<tr>
<td>5.0 V RE</td>
<td>4988</td>
</tr>
<tr>
<td>12.0 V</td>
<td>12104</td>
</tr>
<tr>
<td>12.0 V RE</td>
<td>12026</td>
</tr>
</tbody>
</table>

Bus Revision: 100
FPGA Revision: 270

CB 1 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntakeA-Zone0 Temp.</td>
<td>35 degrees C / 95 degrees F</td>
</tr>
<tr>
<td>IntakeB-Zone1 Temp.</td>
<td>28 degrees C / 82 degrees F</td>
</tr>
<tr>
<td>IntakeC-Zone0 Temp.</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
<tr>
<td>ExhaustA-Zone0 Temp.</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td>ExhaustB-Zone1 Temp.</td>
<td>29 degrees C / 84 degrees F</td>
</tr>
<tr>
<td>TCBC-Zone0 Temp.</td>
<td>32 degrees C / 89 degrees F</td>
</tr>
</tbody>
</table>

Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V</td>
<td>1011</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1208</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1788</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2526</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3319</td>
</tr>
<tr>
<td>5.0 V</td>
<td>5046</td>
</tr>
<tr>
<td>5.0 V RE</td>
<td>4975</td>
</tr>
<tr>
<td>12.0 V</td>
<td>12046</td>
</tr>
</tbody>
</table>
show chassis environment cb (T4000 Core Router)

user@host> show chassis environment cb
CB 0 status:
  State                   Online Master
  Temperature          33 degrees C / 91 degrees F
Power 1
  1.8 V               1805 mV
  2.5 V               2523 mV
  3.3 V               3324 mV
  3.3 V bias          3296 mV
  4.6 V               4680 mV
  5.0 V               4893 mV
  8.0 V bias          7572 mV
  12.0 V              11916 mV
Power 2
  1.0 V              993 mV
  1.2 V              1210 mV
  3.3 V RE           3330 mV
  Bus Revision       51
  FPGA Revision      5
CB 1 status:
  State               Online Standby
  Temperature         33 degrees C / 91 degrees F
Power 1
  1.8 V              1810 mV
  2.5 V              2496 mV
  3.3 V              3308 mV
  3.3 V bias         3286 mV
  4.6 V              4692 mV
  5.0 V              4954 mV
  8.0 V bias         7282 mV
  12.0 V             11926 mV
Power 2
  1.0 V              993 mV
  1.2 V              1185 mV
  3.3 V RE           3316 mV
  Bus Revision       51
  FPGA Revision      5

show chassis environment cb (TX Matrix Router)

user@host> show chassis environment cb
------------------------------------------------------------------------
CB 0 status:
  State                   Online Master
  Temperature          32 degrees C / 89 degrees F
Power:
  1.8 V                1797 mV
  2.5 V                2477 mV
  3.3 V                3311 mV
  4.6 V                4727 mV
  5.0 V                5015 mV
  12.0 V              12185 mV
  3.3 V bias          3304 mV
  8.0 V bias          7870 mV
  BUS Revision        40
show chassis environment cb (TX Matrix Plus Router)

user@host> show chassis environment cb
sfc0-re0:

CB 0 status:
State                      Online Master
Temperature                38 degrees C / 100 degrees F
Power 1
  1.0 V                     1005 mV
  1.1 V                     1108 mV
  1.2 V                     1205 mV
  1.25 V                    1269 mV
  1.5 V                     1508 mV
  1.8 V                     1814 mV
  2.5 V                     2507 mV
  3.3 V                     3306 mV
  3.3 V bias                3300 mV
  9.0 V                     9058 mV
  9.0 V RE                  9107 mV
Power 2
  3.9 V                     3963 mV
  5.0 V                     5020 mV
  9.0 V                     9087 mV
Bus Revision               79
FPGA Revision 23

CB 1 status:
State Online Standby
Temperature 39 degrees C / 102 degrees F

<table>
<thead>
<tr>
<th>Power 1</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V</td>
<td>1002 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 V</td>
<td>1105 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 V</td>
<td>1198 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.25 V</td>
<td>1276 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5 V</td>
<td>1504 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.8 V</td>
<td>1804 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 V</td>
<td>2507 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3 V</td>
<td>3300 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3293 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.0 V</td>
<td>9039 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.0 V RE</td>
<td>9049 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Power 2   |            |            |            |            |            |
| 3.9 V     | 3892 mV    |            |            |            |            |
| 5.0 V     | 5040 mV    |            |            |            |            |
| 9.0 V     | 9058 mV    |            |            |            |            |

Bus Revision 79
FPGA Revision 23

1cc0-re0:

CB 0 status:
State Online Master
Temperature 39 degrees C / 102 degrees F

<table>
<thead>
<tr>
<th>Power 1</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.8 V</td>
<td>1799 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 V</td>
<td>2499 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3 V</td>
<td>3327 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3299 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.6 V</td>
<td>4673 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.0 V</td>
<td>4918 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.0 V bias</td>
<td>7308 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.0 V</td>
<td>11887 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Power 2   |            |            |            |            |            |
| 1.0 V     | 996 mV     |            |            |            |            |
| 1.2 V     | 1199 mV    |            |            |            |            |
| 3.3 V RE  | 3319 mV    |            |            |            |            |

Bus Revision 51
FPGA Revision 3

CB 1 status:
State Online Standby
Temperature 40 degrees C / 104 degrees F

<table>
<thead>
<tr>
<th>Power 1</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.8 V</td>
<td>1800 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5 V</td>
<td>2496 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3 V</td>
<td>3322 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3284 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.6 V</td>
<td>4680 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.0 V</td>
<td>4954 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.0 V bias</td>
<td>7284 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.0 V</td>
<td>11902 mV</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Power 2   |            |            |            |            |            |
| 1.0 V     | 998 mV     |            |            |            |            |
| 1.2 V     | 1205 mV    |            |            |            |            |
| 3.3 V RE  | 3327 mV    |            |            |            |            |

Bus Revision 51
FPGA Revision 3
### lcc1-re0:

<table>
<thead>
<tr>
<th>CB 0 status:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Online Master</td>
</tr>
<tr>
<td>Temperature</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td><strong>Power 1</strong></td>
<td></td>
</tr>
<tr>
<td>1.8 V</td>
<td>1804 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2517 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3300 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3284 mV</td>
</tr>
<tr>
<td>4.6 V</td>
<td>4681 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>4927 mV</td>
</tr>
<tr>
<td>8.0 V bias</td>
<td>7357 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11907 mV</td>
</tr>
<tr>
<td><strong>Power 2</strong></td>
<td></td>
</tr>
<tr>
<td>1.0 V</td>
<td>991 mV</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1202 mV</td>
</tr>
<tr>
<td>3.3 V RE</td>
<td>3301 mV</td>
</tr>
<tr>
<td><strong>Bus Revision</strong></td>
<td>51</td>
</tr>
<tr>
<td><strong>FPGA Revision</strong></td>
<td>3</td>
</tr>
</tbody>
</table>

### CB 1 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online Standby</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td><strong>Power 1</strong></td>
<td></td>
</tr>
<tr>
<td>1.8 V</td>
<td>1805 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2528 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3324 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3289 mV</td>
</tr>
<tr>
<td>4.6 V</td>
<td>4694 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>4959 mV</td>
</tr>
<tr>
<td>8.0 V bias</td>
<td>7311 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11926 mV</td>
</tr>
<tr>
<td><strong>Power 2</strong></td>
<td></td>
</tr>
<tr>
<td>1.0 V</td>
<td>998 mV</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1200 mV</td>
</tr>
<tr>
<td>3.3 V RE</td>
<td>3313 mV</td>
</tr>
<tr>
<td><strong>Bus Revision</strong></td>
<td>51</td>
</tr>
<tr>
<td><strong>FPGA Revision</strong></td>
<td>3</td>
</tr>
</tbody>
</table>

### lcc2-re0:

<table>
<thead>
<tr>
<th>CB 0 status:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Online Master</td>
</tr>
<tr>
<td>Temperature</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td><strong>Power 1</strong></td>
<td></td>
</tr>
<tr>
<td>1.8 V</td>
<td>1805 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2494 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3333 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3296 mV</td>
</tr>
<tr>
<td>4.6 V</td>
<td>4673 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>4901 mV</td>
</tr>
<tr>
<td>8.0 V bias</td>
<td>7343 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11916 mV</td>
</tr>
<tr>
<td><strong>Power 2</strong></td>
<td></td>
</tr>
<tr>
<td>1.0 V</td>
<td>993 mV</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1213 mV</td>
</tr>
<tr>
<td>3.3 V RE</td>
<td>3328 mV</td>
</tr>
<tr>
<td><strong>Bus Revision</strong></td>
<td>51</td>
</tr>
<tr>
<td><strong>FPGA Revision</strong></td>
<td>3</td>
</tr>
</tbody>
</table>

### CB 1 status:
### CB 0 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>37 degrees C / 98 degrees F</td>
</tr>
</tbody>
</table>

### Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.8 V</td>
<td>1809 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2510 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3296 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3291 mV</td>
</tr>
<tr>
<td>4.6 V</td>
<td>4670 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>4905 mV</td>
</tr>
<tr>
<td>8.0 V bias</td>
<td>7211 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11882 mV</td>
</tr>
</tbody>
</table>

### Power 2

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V</td>
<td>996 mV</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1188 mV</td>
</tr>
<tr>
<td>3.3 V RE</td>
<td>3326 mV</td>
</tr>
</tbody>
</table>

**Bus Revision**: 51  
**FPGA Revision**: 5

### CB 1 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online Standby</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
</tbody>
</table>

### Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.8 V</td>
<td>1813 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2510 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3322 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3289 mV</td>
</tr>
<tr>
<td>4.6 V</td>
<td>4692 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>4967 mV</td>
</tr>
<tr>
<td>8.0 V bias</td>
<td>7194 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11916 mV</td>
</tr>
</tbody>
</table>

### Power 2

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V</td>
<td>996 mV</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1205 mV</td>
</tr>
<tr>
<td>3.3 V RE</td>
<td>3273 mV</td>
</tr>
</tbody>
</table>

**Bus Revision**: 51  
**FPGARevision**: 5

---

**show chassis environment cb (EX8200 Switch)**

```
user@host> show chassis environment cb
```
<table>
<thead>
<tr>
<th>CB 0 status:</th>
<th>Online Master</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Online Master</td>
</tr>
<tr>
<td><strong>Temperature Intake</strong></td>
<td>20 degrees C / 68 degrees F</td>
</tr>
<tr>
<td><strong>Temperature Exhaust</strong></td>
<td>24 degrees C / 75 degrees F</td>
</tr>
</tbody>
</table>

### Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 V</td>
<td>1086 mV</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1179 mV</td>
</tr>
<tr>
<td>1.2 V *</td>
<td>1182 mV</td>
</tr>
<tr>
<td>1.2 V *</td>
<td>1182 mV</td>
</tr>
<tr>
<td>1.25 V</td>
<td>1211 mV</td>
</tr>
<tr>
<td>1.5 V</td>
<td>1472 mV</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1756 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2449 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3254 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3300 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>4911 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11891 mV</td>
</tr>
</tbody>
</table>

### Power 2

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3 V bias</td>
<td>3615 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3615 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3567 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3664 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4224 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4215 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4224 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4205 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4195 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4215 mV</td>
</tr>
<tr>
<td>5.0 V bias</td>
<td>4920 mV</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CB 1 status:</th>
<th>Online Standby</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Online Standby</td>
</tr>
<tr>
<td><strong>Temperature Intake</strong></td>
<td>19 degrees C / 66 degrees F</td>
</tr>
<tr>
<td><strong>Temperature Exhaust</strong></td>
<td>23 degrees C / 73 degrees F</td>
</tr>
</tbody>
</table>

### Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 V</td>
<td>1082 mV</td>
</tr>
<tr>
<td>1.2 V</td>
<td>1169 mV</td>
</tr>
<tr>
<td>1.2 V *</td>
<td>1179 mV</td>
</tr>
<tr>
<td>1.2 V *</td>
<td>1179 mV</td>
</tr>
<tr>
<td>1.25 V</td>
<td>1214 mV</td>
</tr>
<tr>
<td>1.5 V</td>
<td>1482 mV</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1759 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2481 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3248 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3306 mV</td>
</tr>
<tr>
<td>5.0 V</td>
<td>4911 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11910 mV</td>
</tr>
</tbody>
</table>

### Power 2

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3 V bias</td>
<td>3644 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3664 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3586 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3654 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4224 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4215 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4224 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4205 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4244 mV</td>
</tr>
<tr>
<td>4.3 V bias</td>
<td>4215 mV</td>
</tr>
<tr>
<td>5.0 V bias</td>
<td>4930 mV</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CB 2 status:</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Online</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Temperature Intake 19 degrees C / 66 degrees F  
Temperature Exhaust 23 degrees C / 73 degrees F  

Power 1  
1.2 V 1195 mV  
1.5 V 1511 mV  
1.8 V 1804 mV  
2.5 V 2526 mV  
3.3 V 3300 mV  
3.3 V bias 3306 mV  
12.0 V 12220 mV  

Power 2  
3.3 V bias * 3606 mV  
3.3 V bias * 3615 mV  
3.3 V bias * 3567 mV  
3.3 V bias * 3673 mV  
4.3 V bias * 4224 mV  
4.3 V bias * 4215 mV  
4.3 V bias * 4234 mV  
4.3 V bias * 4205 mV  
4.3 V bias * 4186 mV  
4.3 V bias * 4215 mV  
5.0 V bias 4940 mV  

show chassis environment cb (EX8208 Switch)  
user@host> show chassis environment cb  
CB 0 status:  
State Online Master  
Temperature Intake 20 degrees C / 68 degrees F  
Temperature Exhaust 24 degrees C / 75 degrees F  
Power 1  
1.1 V 1086 mV  
1.2 V 1179 mV  
1.2 V * 1182 mV  
1.2 V * 1182 mV  
1.25 V 1211 mV  
1.5 V 1466 mV  
1.8 V 1759 mV  
2.5 V 2455 mV  
3.3 V 3261 mV  
3.3 V bias 3300 mV  
5.0 V 4930 mV  
12.0 V 11891 mV  

Power 2  
3.3 V bias * 3606 mV  
3.3 V bias * 3615 mV  
3.3 V bias * 3567 mV  
3.3 V bias * 3673 mV  
4.3 V bias * 4224 mV  
4.3 V bias * 4215 mV  
4.3 V bias * 4234 mV  
4.3 V bias * 4205 mV  
4.3 V bias * 4186 mV  
4.3 V bias * 4215 mV  
5.0 V bias 4940 mV  

CB 1 status:  
State Online Standby  
Temperature Intake 19 degrees C / 66 degrees F  
Temperature Exhaust 23 degrees C / 73 degrees F  
Power 1  
1.1 V 1086 mV  
1.2 V 1169 mV  
1.2 V * 1179 mV  
1.2 V * 1179 mV  
1.25 V 1211 mV  
1.5 V 1479 mV  
1.8 V 1759 mV  
2.5 V 2475 mV  
3.3 V 3235 mV  
3.3 V bias 3306 mV  
5.0 V 4930 mV  
12.0 V 11891 mV  

Power 2
3.3 V bias *    3644 mV
3.3 V bias *    3664 mV
3.3 V bias *    3586 mV
3.3 V bias *    3654 mV
4.3 V bias *    4215 mV
4.3 V bias *    4224 mV
4.3 V bias *    4215 mV
4.3 V bias *    4215 mV
4.3 V bias *    4234 mV
4.3 V bias *    4224 mV
5.0 V bias      4920 mV

CB 2 status:
State          Online
Temperature Intake         20 degrees C / 68 degrees F
Temperature Exhaust        24 degrees C / 75 degrees F
Power 1
1.2 V           1202 mV
1.5 V           1508 mV
1.8 V           1804 mV
2.5 V           2520 mV
3.3 V           3300 mV
3.3 V bias      3300 mV
12.0 V          12200 mV

show chassis environment cb (PTX5000 Packet Transport Router)

user@host> show chassis environment cb

CB 0 status:
State          Online Master
Intake Temperature         38 degrees C / 100 degrees F
Exhaust A Temperature      45 degrees C / 113 degrees F
Exhaust B Temperature      42 degrees C / 107 degrees F
Power 1
1.2 V           1200 mV
1.25 V          1250 mV
2.5 V           2500 mV
3.3 V           3300 mV
Power 2
1.0 V           1000 mV
3.3 V bias      3293 mV
3.9 V           3921 mV
Bus Revision      132
FPGA Revision     27

CB 1 status:
State          Online Standby
Intake Temperature         34 degrees C / 93 degrees F
Exhaust A Temperature      39 degrees C / 102 degrees F
Exhaust B Temperature      36 degrees C / 96 degrees F
Power 1
1.2 V           1199 mV
1.25 V          1250 mV
2.5 V           2499 mV
3.3 V           3299 mV
Power 2
1.0 V           1000 mV
3.3 V bias      3312 mV
3.9 V           3961 mV
Bus Revision      132
FPGA Revision     28
show chassis environment cb (QFabric System)

user@switch> show chassis environment cb interconnect-device IC-123 0
CB 0 status:

State                      Online Master
Left Intake Temperature    33 degrees C / 91 degrees F
Right Intake Temperature   33 degrees C / 91 degrees F
Left Exhaust Temperature   36 degrees C / 96 degrees F
Right Exhaust Temperature  35 degrees C / 95 degrees F
Power                      OK
VDD 3V3                    3294 mV
VDD 2V5                    2436 mV
VDD 1V8                    1746 mV
VDD 1V5                    1460 mV
VDD 1V25                   1210 mV
VDD 1V2                    1164 mV
CPU CORE 1V2               1120 mV
VDD 1V0                    968 mV
VDD 5V0                    5088 mV
CPU MP BIAS 4V3            4050 mV
BIAS 3V3                   3180 mV
VTT 0V9                    866 mV
**show chassis environment fpc**

**Syntax**

```
show chassis environment fpc
<slot>
```

**Syntax (TX Matrix and TX Matrix Plus Routers)**

```
show chassis environment fpc
<lcc number>
<slot>
```

**Syntax (MX Series Routers)**

```
show chassis environment fpc
<slot>
<all-members>
<local>
<member member-id>
```

**Syntax (MX2010 3D Universal Edge Routers)**

```
show chassis environment fpc
<slot>
```

**Syntax (MX2020 3D Universal Edge Routers)**

```
show chassis environment fpc
<slot>
```

**Syntax (QFX Series)**

```
show chassis environment fpc
<fpc-slot>
interconnect-device name
```

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for QFX Series.  
Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.  
Command introduced in Junos OS Release 12.1 for T4000 Core Routers.  
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.  
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

**Description**

(M40e, M120, M160, M320, MX Series, T Series routers, EX Series, QFX Series, and PTX Series routers only) Display environmental information about Flexible PIC Concentrators (FPCs).

**Options**

- **none**—Display environmental information about all FPCs. On a TX Matrix router, display environmental information about all FPCs on the TX Matrix router and its attached T640 routers. On a TX Matrix Plus router, display environmental information about all FPCs on the TX Matrix Plus router and its attached routers.

- **all-members**—(MX Series routers only) (Optional) Display environmental information for the FPCs in all the members of the Virtual Chassis configuration.

- **interconnect-device name**—(QFabric systems only) (Optional) Display chassis environmental information for the Interconnect device.
**lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.
Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(MX Series routers only) (Optional) Display environmental information for the FPCs in the local Virtual Chassis member.

**member member-id**—(MX Series routers only) (Optional) Display environmental information for the FPCs in the specified member of the Virtual Chassis configuration. Replace member-id with a value of 0 or 1.

**slot or fpc-slot**—(Optional) Display environmental information about an individual FPC:

- (TX Matrix and TX Matrix Plus routers only) On a TX Matrix router, if you specify the number of the T640 router by using only the lcc number option (the recommended method), replace slot with a value from 0 through 7. Similarly, on a TX Matrix Plus router, if you specify the number of the router by using only the lcc number option (the recommended method), replace slot with a value from 0 through 7. Otherwise, replace slot with a value from 0 through 31. For example, the following commands have the same result:

  ```
  user@host> show chassis environment fpc 1 lcc 1
  user@host> show chassis environment fpc 9
  ```

- M120 router—Replace slot with a value from 0 through 5.
- MX240 router—Replace slot with a value from 0 through 2.
- MX480 router—Replace slot with a value from 0 through 5.
- MX960 router—Replace slot with a value from 0 through 11.
- MX2010 router—Replace slot with a value from 0 through 9.
- MX2020 router—Replace slot with a value from 0 through 19.
- Other routers—Replace slot with a value from 0 through 7.
- EX Series switches:
  - EX3200 switches and EX4200 standalone switches—Replace slot with 0.
  - EX4200 switches in a Virtual Chassis configuration—Replace slot with a value from 0 through 9 (switch's member ID).
• EX6210 switches—Replace slot with a value from 0 through 3 (line card only), 4 or 5 (line card or Switch Fabric and Routing Engine (SRE) module), or 6 through 9 (line card only).

• EX8208 switches—Replace slot with a value from 0 through 7 (line card).

• EX8216 switches—Replace slot with a value from 0 through 15 (line card).

• QFX3500 switches —Replace fpc-slot with 0 through 15.

• PTX5000 Packet Transport Router—Replace fpc-slot with 0 through 7.

### Required Privilege
view

### Related Documentation
- request chassis fpc on page 749
- show chassis fpc on page 1011
- show chassis fpc-feb-connectivity
- Configuring the Junos OS to Resynchronize FPC Sequence Numbers with Active FPCs when an FPC Comes Online
- MX960 Flexible PIC Concentrator Description

### List of Sample Output
- show chassis environment fpc (M120 Router) on page 846
- show chassis environment fpc (M160 Router) on page 847
- show chassis environment fpc (M320 Router) on page 847
- show chassis environment fpc (MX2020 Router) on page 848
- show chassis environment fpc (MX2010 Router) on page 851
- show chassis environment fpc (MX240 Router) on page 853
- show chassis environment fpc (MX480 Router) on page 854
- show chassis environment fpc (MX960 Router) on page 855
- show chassis environment fpc (MX480 Router with 100-Gigabit Ethernet CFP) on page 856
- show chassis environment fpc (MX240, MX480, MX960 with Application Services Modular Line Card on page 857
- show chassis environment fpc (T320, T640, and T1600 Routers) on page 857
- show chassis environment fpc (T4000 Router) on page 858
- show chassis environment fpc lcc (TX Matrix Router) on page 863
- show chassis environment fpc lcc (TX Matrix Plus Router) on page 864
- show chassis environment fpc (QFX Series) on page 865
- show chassis environment fpc interconnect-device (QFabric Systems) on page 865
- show chassis environment fpc 0 (PTX5000 Packet Transport Router) on page 865
- show chassis environment FPC 1 (MX Routers with Media Services Blade [MSB]) on page 866

### Output Fields
Table 141 on page 845 lists the output fields for the show chassis environment fpc command. Output fields are listed in the approximate order in which they appear.
Table 141: show chassis environment fpc Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>Status of the FPC:</td>
</tr>
<tr>
<td>• Unknown</td>
<td>FPC is not detected by the router.</td>
</tr>
<tr>
<td>• Empty</td>
<td>No FPC is present.</td>
</tr>
<tr>
<td>• Present</td>
<td>FPC is detected by the chassis daemon but is either not supported by the current version of the Junos OS, or the FPC is coming up but not yet online.</td>
</tr>
<tr>
<td>• Ready</td>
<td>FPC is in intermediate or transition state.</td>
</tr>
<tr>
<td>• Announce online</td>
<td>Intermediate state during which the FPC is coming up but not yet online, and the chassis manager acknowledges the chassisd FPC online initiative.</td>
</tr>
<tr>
<td>• Online</td>
<td>FPC is online and running.</td>
</tr>
<tr>
<td>• Offline</td>
<td>FPC is powered down.</td>
</tr>
<tr>
<td>• Diagnostics</td>
<td>FPC is set to operate in diagnostics mode.</td>
</tr>
<tr>
<td><strong>Temperature</strong></td>
<td>(M40e and M160 routers and QFX Series only) Temperature of the air flowing past the FPC.</td>
</tr>
<tr>
<td><strong>PMB Temperature</strong></td>
<td>(PTX Series only) Temperature of the air flowing past the PMB (bottom of the FPC).</td>
</tr>
<tr>
<td><strong>Temperature Intake</strong></td>
<td>(M320 routers, MX2010 routers, MX2020 routers, and PTX Series only) Temperature of the air flowing into the chassis.</td>
</tr>
<tr>
<td><strong>Temperature Top</strong></td>
<td>(T Series routers only) Temperature of the air flowing past the top of the FPC.</td>
</tr>
<tr>
<td><strong>Temperature Exhaust</strong></td>
<td>(M120 and M320 routers, MX2010 routers, MX2020 routers, and PTX Series only) Temperature of the air flowing out of the chassis. The PTX Series Packet Transport Routers, and the MX2010 and MX2020 routers include exhaust temperatures for multiple zones (Exhaust A and Exhaust B).</td>
</tr>
<tr>
<td><strong>Temperature Bottom</strong></td>
<td>(T Series routers only) Temperature of the air flowing past the bottom of the FPC.</td>
</tr>
<tr>
<td><strong>TL n Temperature</strong></td>
<td>(PTX Series only) Temperature of the air flowing past the specified TL area of the packet forwarding engine (PFE) on the FPC.</td>
</tr>
<tr>
<td><strong>TQ n Temperature</strong></td>
<td>(PTX Series only) Temperature of the air flowing past the specified TQ area of the packet forwarding engine (PFE) on the FPC.</td>
</tr>
<tr>
<td><strong>Temperature MMBO</strong></td>
<td>(T640 router only) Temperature of the air flowing past the type 3 FPC.</td>
</tr>
<tr>
<td><strong>Temperature MMB1</strong></td>
<td>(M320 and T Series routers only) Temperature of the air flowing past the type 1, type 2, and type 3 FPC.</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td>Information about the voltage supplied to the FPC. The left column displays the required power, in volts. The right column displays the measured power, in millivolts.</td>
</tr>
<tr>
<td><strong>CMB Revision or BUS revision</strong></td>
<td>Revision level of the chassis management bus device (M Series router) or bus (T Series routers).</td>
</tr>
</tbody>
</table>
Sample Output

show chassis environment fpc (M120 Router)

```
user@host> show chassis environment fpc
FPC 2 status:
  State                      Online
  Temperature Exhaust A      32 degrees C / 89 degrees F
  Temperature Exhaust B      31 degrees C / 87 degrees F
  Power A-Board
    1.2 V                     1202 mV
    1.5 V                     1508 mV
    1.8 V                     1798 mV
    2.5 V                     2507 mV
    3.3 V                     3351 mV
    5.0 V                     4995 mV
    3.3 V bias                3296 mV
    1.2 V Rocket IO           1205 mV
    1.5 V Rocket IO           1501 mV
    I2C Slave Revision        12

FPC 3 status:
  State                      Online
  Temperature Exhaust A      31 degrees C / 87 degrees F
  Temperature Exhaust B      33 degrees C / 91 degrees F
  Power A-Board
    1.2 V                     1211 mV
    1.5 V                     1501 mV
    1.8 V                     1798 mV
    2.5 V                     2471 mV
    3.3 V                     3293 mV
    5.0 V                     4930 mV
    3.3 V bias                3296 mV
    1.2 V Rocket IO           1205 mV
    1.5 V Rocket IO           1501 mV
  Power B-Board
    1.2 V                     1214 mV
    1.5 V                     1501 mV
    2.5 V                     2471 mV
    3.3 V                     3300 mV
    5.0 V                     4943 mV
    3.3 V bias                3296 mV
    1.2 V Rocket IO           1205 mV
    1.5 V Rocket IO           1501 mV
    I2C Slave Revision        12

FPC 4 status:
  State                      Online
  Temperature Exhaust A      32 degrees C / 89 degrees F
  Temperature Exhaust B      30 degrees C / 86 degrees F
  Power A-Board
    1.2 V                     1195 mV
    1.5 V                     1504 mV
    1.8 V                     1801 mV
    2.5 V                     2504 mV
    3.3 V                     3293 mV
    5.0 V                     4917 mV
    3.3 V bias                3296 mV
    1.2 V Rocket IO           1202 mV
    1.5 V Rocket IO           1492 mV
    I2C Slave Revision        12
```
show chassis environment fpc (M160 Router)

user@host> show chassis environment fpc
FPC 0 status:
  State              Online
  Temperature       42 degrees C / 107 degrees F
  Power:
    1.5 V            1500 mV
    2.5 V            2509 mV
    3.3 V            3308 mV
    5.0 V            4991 mV
    5.0 V bias       4952 mV
    8.0 V bias       8307 mV
  CMB Revision      12
FPC 1 status:
  State              Online
  Temperature       45 degrees C / 113 degrees F
  Power:
    1.5 V            1498 mV
    2.5 V            2501 mV
    3.3 V            3319 mV
    5.0 V            5020 mV
    5.0 V bias       5025 mV
    8.0 V bias       8307 mV
  CMB Revision      12

show chassis environment fpc (M320 Router)

user@host> show chassis environment fpc
FPC 0 status:
  State              Online
  Temperature Intake 27 degrees C / 80 degrees F
  Temperature Exhaust 38 degrees C / 100 degrees F
  Temperature MMB1   31 degrees C / 87 degrees F
  Power:
    1.5 V            1487 mV
    1.5 V *          1494 mV
    1.8 V            1821 mV
    2.5 V            2533 mV
    3.3 V            3323 mV
    5.0 V            5028 mV
    3.3 V bias       3296 mV
    5.0 V bias       4984 mV
  CMB Revision      16
FPC 1 status:
  State              Online
  Temperature Intake 27 degrees C / 80 degrees F
  Temperature Exhaust 37 degrees C / 98 degrees F
  Temperature MMB1   32 degrees C / 89 degrees F
  Power:
    1.5 V            1504 mV
    1.5 V *          1499 mV
    1.8 V            1820 mV
    2.5 V            2529 mV
    3.3 V            3328 mV
    5.0 V            5013 mV
    3.3 V bias       3294 mV
    5.0 V bias       4984 mV
  CMB Revision      16
FPC 2 status:
  State              Online
Temperature Intake           28 degrees C / 82 degrees F
Temperature Exhaust          38 degrees C / 100 degrees F
Temperature MMB1             32 degrees C / 89 degrees F

Power:
1.5 V                    1498 mV
1.5 V bias                1487 mV
1.8 V                    1816 mV
2.5 V                    2531 mV
3.3 V                    3324 mV
5.0 V                    5023 mV
3.3 V bias               3277 mV
5.0 V bias               5013 mV
CMB Revision                 17

FPC 3 status:

show chassis environment fpc (MX2020 Router)

user@host> show chassis environment fpc
FPC 0 status:

State                      Online
Temperature Intake         41 degrees C / 105 degrees F
Temperature Exhaust A      48 degrees C / 118 degrees F
Temperature Exhaust B      60 degrees C / 140 degrees F
Temperature LU 0 TSen      56 degrees C / 132 degrees F
Temperature LU 0 Chip      59 degrees C / 138 degrees F
Temperature LU 1 TSen      56 degrees C / 132 degrees F
Temperature LU 1 Chip      61 degrees C / 141 degrees F
Temperature LU 2 TSen      56 degrees C / 132 degrees F
Temperature LU 2 Chip      52 degrees C / 125 degrees F
Temperature LU 3 TSen      56 degrees C / 132 degrees F
Temperature LU 3 Chip      52 degrees C / 125 degrees F
Temperature MQ 0 TSen      49 degrees C / 120 degrees F
Temperature MQ 0 Chip      49 degrees C / 120 degrees F
Temperature MQ 1 TSen      49 degrees C / 120 degrees F
Temperature MQ 1 Chip      52 degrees C / 125 degrees F
Temperature MQ 2 TSen      49 degrees C / 120 degrees F
Temperature MQ 2 Chip      45 degrees C / 113 degrees F
Temperature MQ 3 TSen      49 degrees C / 120 degrees F
Temperature MQ 3 Chip      46 degrees C / 114 degrees F

Power
AS-BIAS3V3-zl2105         3299 mV
AS-VDD1V8-zl2006          1807 mV
AS-VDD2V5-zl2006          2512 mV
AS-AVDD1V0-zl2004         997 mV
AS-PCIE_1V0-zl2004        996 mV
AS-VDD3V3-zl2004          3294 mV
AS-VDD_1V5A-zl2004        1501 mV
AS-VDD_1V5B-zl2004        1498 mV
AS-LU0_1V0-zl2004         998 mV
AS-LU1_1V0-zl2004         1002 mV
AS-MQ0_1V0-zl2004         999 mV
AS-MQ1_1V0-zl2004         994 mV
AS-LU2_1V0-zl2004         1000 mV
AS-LU3_1V0-zl2004         998 mV
AS-MQ2_1V0-zl2004         1002 mV
AS-MQ3_1V0-zl2004         999 mV
AS-PMB_1VL-zl2006         1096 mV

I2C Slave Revision         68

FPC 1 status:

State                      Online
Temperature Intake         39 degrees C / 102 degrees F
Temperature Exhaust A      48 degrees C / 118 degrees F
Temperature Exhaust B      55 degrees C / 131 degrees F
Temperature LU 0 TSen      52 degrees C / 125 degrees F
Temperature LU 0 Chip      54 degrees C / 129 degrees F
Temperature LU 1 TSen      52 degrees C / 125 degrees F
Temperature LU 1 Chip      56 degrees C / 132 degrees F
Temperature LU 2 TSen      52 degrees C / 125 degrees F
Temperature LU 2 Chip      49 degrees C / 120 degrees F
Temperature LU 3 TSen      52 degrees C / 125 degrees F
Temperature LU 3 Chip      50 degrees C / 122 degrees F
Temperature MQ 0 TSen      48 degrees C / 118 degrees F
Temperature MQ 0 Chip      48 degrees C / 118 degrees F
Temperature MQ 1 TSen      48 degrees C / 118 degrees F
Temperature MQ 1 Chip      51 degrees C / 123 degrees F
Temperature MQ 2 TSen      48 degrees C / 118 degrees F
Temperature MQ 2 Chip      45 degrees C / 113 degrees F
Temperature MQ 3 TSen      48 degrees C / 118 degrees F
Temperature MQ 3 Chip      45 degrees C / 113 degrees F

Power
AS-BIAS3V3-zl2105         3299 mV
AS-VDDV18-zl2006          1786 mV
AS-VDD2V5-zl2006          2496 mV
AS-AVD1V0-zl2004          1000 mV
AS-PCIE1V0-zl2004         1000 mV
AS-VDD3V3-zl2004          3294 mV
AS-VDD1V5A-zl2004         1500 mV
AS-VDD1V5B-zl2004         1500 mV
AS-LU0_1V0-zl2004         1003 mV
AS-LU1_1V0-zl2004         1000 mV
AS-MQ0_1V0-zl2004         1000 mV
AS-MQ1_1V0-zl2004         995 mV
AS-LU2_1V0-zl2004         1002 mV
AS-LU3_1V0-zl2004         997 mV
AS-MQ2_1V0-zl2004         1000 mV
AS-MQ3_1V0-zl2004         998 mV
AS-PMB1V1-zl2006          1096 mV

I2C Slave Revision         68

FPC 2 status:
State                      Online
Temperature Intake         39 degrees C / 102 degrees F
Temperature Exhaust A      48 degrees C / 118 degrees F
Temperature Exhaust B      58 degrees C / 136 degrees F
Temperature LU 0 TSen      55 degrees C / 131 degrees F
Temperature LU 1 TSen      55 degrees C / 131 degrees F
Temperature LU 1 Chip      63 degrees C / 145 degrees F
Temperature LU 2 TSen      55 degrees C / 131 degrees F
Temperature LU 2 Chip      51 degrees C / 123 degrees F
Temperature LU 3 TSen      55 degrees C / 131 degrees F
Temperature LU 3 Chip      52 degrees C / 125 degrees F
Temperature MQ 0 TSen      48 degrees C / 118 degrees F
Temperature MQ 0 Chip      50 degrees C / 122 degrees F
Temperature MQ 1 TSen      48 degrees C / 118 degrees F
Temperature MQ 1 Chip      52 degrees C / 125 degrees F
Temperature MQ 2 TSen      48 degrees C / 118 degrees F
Temperature MQ 2 Chip      47 degrees C / 116 degrees F
Temperature MQ 3 TSen      48 degrees C / 118 degrees F
Temperature MQ 3 Chip      47 degrees C / 116 degrees F

Power
AS-BIAS3V3-zl2105         3299 mV
AS-VDD1V8-zl2006  1805 mV
AS-VDD2V5-zl2006  2510 mV
AS-AVDD1V0-zl2004  999 mV
AS-PCIE_1V0-zl2004  998 mV
AS-VDD3V3-zl2004  3296 mV
AS-VDD_1V5A-zl2004  1492 mV
AS-VDD_1V5B-zl2004  1497 mV
AS-LU0_1V0-zl2004  997 mV
AS-LU1_1V0-zl2004  1000 mV
AS-MQ0_1V0-zl2004  998 mV
AS-MQ1_1V0-zl2004  1001 mV
AS-LU2_1V0-zl2004  996 mV
AS-LU3_1V0-zl2004  995 mV
AS-MQ2_1V0-zl2004  998 mV
AS-MQ3_1V0-zl2004  997 mV
AS-PMB_1V1-zl2006  1100 mV

I2C Slave Revision  68

FPC 3 status:
State  Online
Temperature Intake  41 degrees C / 105 degrees F
Temperature Exhaust A  48 degrees C / 118 degrees F
Temperature Exhaust B  58 degrees C / 136 degrees F
Temperature LU 0 TSen  56 degrees C / 132 degrees F
Temperature LU 0 Chip  59 degrees C / 138 degrees F
Temperature LU 1 TSen  56 degrees C / 132 degrees F
Temperature LU 1 Chip  61 degrees C / 141 degrees F
Temperature LU 2 TSen  56 degrees C / 132 degrees F
Temperature LU 2 Chip  51 degrees C / 123 degrees F
Temperature LU 3 TSen  56 degrees C / 132 degrees F
Temperature LU 3 Chip  53 degrees C / 127 degrees F
Temperature MQ 0 TSen  50 degrees C / 122 degrees F
Temperature MQ 0 Chip  51 degrees C / 123 degrees F
Temperature MQ 1 TSen  50 degrees C / 122 degrees F
Temperature MQ 1 Chip  55 degrees C / 131 degrees F
Temperature MQ 2 TSen  50 degrees C / 122 degrees F
Temperature MQ 2 Chip  47 degrees C / 116 degrees F
Temperature MQ 3 TSen  50 degrees C / 122 degrees F
Temperature MQ 3 Chip  50 degrees C / 122 degrees F

Power
AS-BIAS3V3-zl2105  3305 mV
AS-VDD1V8-zl2006  1810 mV
AS-VDD2V5-zl2006  2508 mV
AS-AVDD1V0-zl2004  999 mV
AS-PCIE_1V0-zl2004  1001 mV
AS-VDD3V3-zl2004  3294 mV
AS-VDD_1V5A-zl2004  1500 mV
AS-VDD_1V5B-zl2004  1498 mV
AS-LU0_1V0-zl2004  998 mV
AS-LU1_1V0-zl2004  998 mV
AS-MQ0_1V0-zl2004  999 mV
AS-MQ1_1V0-zl2004  998 mV
AS-LU2_1V0-zl2004  1000 mV
AS-LU3_1V0-zl2004  1001 mV
AS-MQ2_1V0-zl2004  996 mV
AS-MQ3_1V0-zl2004  998 mV
AS-PMB_1V1-zl2006  1098 mV

I2C Slave Revision  68

FPC 4 status:
...

Copyright © 2013, Juniper Networks, Inc.
show chassis environment fpc (MX2010 Router)

```
user@host> show chassis environment fpc

FPC 0 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature Intake</td>
<td>36 degrees C / 96 degrees F</td>
</tr>
<tr>
<td>Temperature Exhaust A</td>
<td>42 degrees C / 107 degrees F</td>
</tr>
<tr>
<td>Temperature Exhaust B</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>Temperature LU 0 TSen</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>Temperature LU 0 Chip</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td>Temperature LU 1 TSen</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>Temperature LU 1 Chip</td>
<td>54 degrees C / 129 degrees F</td>
</tr>
<tr>
<td>Temperature LU 2 TSen</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>Temperature LU 2 Chip</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>Temperature LU 3 TSen</td>
<td>49 degrees C / 120 degrees F</td>
</tr>
<tr>
<td>Temperature LU 3 Chip</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 0 TSen</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 0 Chip</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 1 TSen</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 1 Chip</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 2 TSen</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 2 Chip</td>
<td>38 degrees C / 100 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 3 TSen</td>
<td>40 degrees C / 104 degrees F</td>
</tr>
<tr>
<td>Temperature MQ 3 Chip</td>
<td>41 degrees C / 105 degrees F</td>
</tr>
</tbody>
</table>

Power

<table>
<thead>
<tr>
<th>Power</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS-BIAS3V3-zl2105</td>
<td>3300 mV</td>
</tr>
<tr>
<td>AS-VDD1V8-zl2006</td>
<td>1805 mV</td>
</tr>
<tr>
<td>AS-VDD2V5-zl2006</td>
<td>2505 mV</td>
</tr>
<tr>
<td>AS-AVDD1V0-zl2004</td>
<td>998 mV</td>
</tr>
<tr>
<td>AS-PCIE_1V0-zl2004</td>
<td>999 mV</td>
</tr>
<tr>
<td>AS-VDD3V3-zl2004</td>
<td>3303 mV</td>
</tr>
<tr>
<td>AS-VDD_1V5A-zl2004</td>
<td>1497 mV</td>
</tr>
<tr>
<td>AS-VDD_1V5B-zl2004</td>
<td>1497 mV</td>
</tr>
<tr>
<td>AS-LU0_1V0-zl2004</td>
<td>998 mV</td>
</tr>
<tr>
<td>AS-LU1_1V0-zl2004</td>
<td>1003 mV</td>
</tr>
<tr>
<td>AS-MQ0_1V0-zl2004</td>
<td>998 mV</td>
</tr>
<tr>
<td>AS-MQ1_1V0-zl2004</td>
<td>998 mV</td>
</tr>
<tr>
<td>AS-LU2_1V0-zl2004</td>
<td>997 mV</td>
</tr>
<tr>
<td>AS-LU3_1V0-zl2004</td>
<td>1001 mV</td>
</tr>
<tr>
<td>AS-MQ2_1V0-zl2004</td>
<td>996 mV</td>
</tr>
<tr>
<td>AS-MQ3_1V0-zl2004</td>
<td>994 mV</td>
</tr>
<tr>
<td>AS-PMB_1V1-zl2006</td>
<td>1097 mV</td>
</tr>
</tbody>
</table>

I2C Slave Revision 68

FPC 1 status:

<table>
<thead>
<tr>
<th>State</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature Intake</td>
<td>34 degrees C / 93 degrees F</td>
</tr>
<tr>
<td>Temperature Exhaust A</td>
<td>46 degrees C / 114 degrees F</td>
</tr>
<tr>
<td>Temperature Exhaust B</td>
<td>54 degrees C / 129 degrees F</td>
</tr>
<tr>
<td>Temperature LU 0 TSen</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>Temperature LU 0 Chip</td>
<td>55 degrees C / 131 degrees F</td>
</tr>
<tr>
<td>Temperature LU 1 TSen</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>Temperature LU 1 Chip</td>
<td>44 degrees C / 111 degrees F</td>
</tr>
<tr>
<td>Temperature LU 2 TSen</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>Temperature LU 2 Chip</td>
<td>50 degrees C / 122 degrees F</td>
</tr>
<tr>
<td>Temperature LU 3 TSen</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>Temperature XM 0 TSen</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>Temperature XM 0 Chip</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>Temperature XF 0 TSen</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>Temperature XF 0 Chip</td>
<td>63 degrees C / 145 degrees F</td>
</tr>
<tr>
<td>Temperature PLX Switch TSen</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Temperature</th>
<th>Power</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature PLX Switch Chip</td>
<td>47 degrees C / 116 degrees F</td>
<td>MPC-BIASC3V3-z12105</td>
<td>3300 mV</td>
</tr>
<tr>
<td>MPC-VDD3V3-z16100</td>
<td>3298 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-VDD2V5-z16100</td>
<td>2505 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-VDD1V8-z12004</td>
<td>1796 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-AVDD1V0-z12004</td>
<td>991 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-VDD1V2-z16100</td>
<td>1196 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-VDD1V5A-z12004</td>
<td>1491 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-VDD1V5B-z12004</td>
<td>1492 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-XF_0V9-z12004</td>
<td>996 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-PCIE_1V0-z16100</td>
<td>1003 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-LU0_1V0-z12004</td>
<td>996 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-LU1_1V0-z12004</td>
<td>996 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-LU2_1V0-z12004</td>
<td>998 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-LU3_1V0-z12004</td>
<td>994 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-J2VA-BMR453</td>
<td>12031 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-J2VB-BMR453</td>
<td>12003 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-PMB_1V1-z12006</td>
<td>1104 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-PMB_1V2-z12106</td>
<td>1194 mV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPC-XM_0V9-vt273m</td>
<td>911 mV</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I2C Slave Revision: 110

FPC 8 status:
- State: Online
- Temperature Intake: 32 degrees C / 89 degrees F
- Temperature Exhaust A: 44 degrees C / 111 degrees F
- Temperature Exhaust B: 37 degrees C / 98 degrees F
- Temperature LU 0 TCAM Tsen: 42 degrees C / 105 degrees F
- Temperature LU 0 TCAM Chip: 49 degrees C / 120 degrees F
- Temperature LU 0 Tsen: 41 degrees C / 105 degrees F
- Temperature LU 0 Chip: 52 degrees C / 125 degrees F
- Temperature MQ 0 Tsen: 41 degrees C / 105 degrees F
- Temperature MQ 0 Chip: 47 degrees C / 116 degrees F
- Temperature LU 1 TCAM Tsen: 39 degrees C / 102 degrees F
- Temperature LU 1 TCAM Chip: 42 degrees C / 107 degrees F
- Temperature LU 1 Tsen: 39 degrees C / 102 degrees F
- Temperature LU 1 Chip: 46 degrees C / 114 degrees F
- Temperature MQ 1 Tsen: 39 degrees C / 102 degrees F
- Temperature MQ 1 Chip: 45 degrees C / 113 degrees F

Power:
- MPC-BIAS3V3-z12105 | 3296 mV
- MPC-VDD3V3-z12006 | 3298 mV
- MPC-VDD2V5-z12006 | 2505 mV
- MPC-TCAM_1V0-z12004 | 997 mV
- MPC-AVDD1V0-z12006 | 1007 mV
- MPC-VDD1V8-z12006 | 1803 mV
- MPC-PCIE_1V0-z12006 | 1004 mV
- MPC-LU0_1V0-z12004 | 1000 mV
- MPC-MQ0_1V0-z12004 | 999 mV
- MPC-VDO_1V5-z12004 | 1498 mV
- MPC-PMB_1V1-z12006 | 1102 mV
- MPC-9VA-BMR453 | 9009 mV
- MPC-9VB-BMR453 | 8960 mV
- MPC-PMB_1V2-z12105 | 1202 mV
- MPC-LU1_1V0-z12004 | 1005 mV
- MPC-MQ1_1V0-z12004 | 1000 mV

I2C Slave Revision: 70

FPC 9 status:
- State: Online
- Temperature Intake: 34 degrees C / 93 degrees F
- Temperature Exhaust A: 41 degrees C / 105 degrees F
<table>
<thead>
<tr>
<th>Component</th>
<th>Temperature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature Exhaust A</td>
<td>39 degrees C / 102 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature Exhaust B</td>
<td>53 degrees C / 127 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 0 TSensor</td>
<td>51 degrees C / 123 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 0 Chip</td>
<td>54 degrees C / 129 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 1 TSensor</td>
<td>50 degrees C / 122 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 1 Chip</td>
<td>53 degrees C / 127 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 2 TSensor</td>
<td>48 degrees C / 118 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 2 Chip</td>
<td>51 degrees C / 123 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 3 TSensor</td>
<td>45 degrees C / 113 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature I3 3 Chip</td>
<td>48 degrees C / 118 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature IA 0 TSensor</td>
<td>45 degrees C / 113 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature IA 0 Chip</td>
<td>45 degrees C / 113 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature IA 1 TSensor</td>
<td>45 degrees C / 113 degrees F</td>
<td></td>
</tr>
<tr>
<td>Temperature IA 1 Chip</td>
<td>49 degrees C / 120 degrees F</td>
<td></td>
</tr>
</tbody>
</table>

Power

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 V</td>
<td>1492 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2507 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3306 mV</td>
</tr>
</tbody>
</table>

show chassis environment fpc (MX240 Router)

User@host> show chassis environment fpc

FPC 1 status:

State: Online
Temperature Intake: 34 degrees C / 93 degrees F
Temperature Exhaust A: 39 degrees C / 102 degrees F
Temperature Exhaust B: 53 degrees C / 127 degrees F
Temperature I3 0 TSensor: 51 degrees C / 123 degrees F
Temperature I3 0 Chip: 54 degrees C / 129 degrees F
Temperature I3 1 TSensor: 50 degrees C / 122 degrees F
Temperature I3 1 Chip: 53 degrees C / 127 degrees F
Temperature I3 2 TSensor: 48 degrees C / 118 degrees F
Temperature I3 2 Chip: 51 degrees C / 123 degrees F
Temperature I3 3 TSensor: 45 degrees C / 113 degrees F
Temperature I3 3 Chip: 48 degrees C / 118 degrees F
Temperature IA 0 TSensor: 45 degrees C / 113 degrees F
Temperature IA 0 Chip: 45 degrees C / 113 degrees F
Temperature IA 1 TSensor: 45 degrees C / 113 degrees F
Temperature IA 1 Chip: 49 degrees C / 120 degrees F
Power:

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 V</td>
<td>1492 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2507 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3306 mV</td>
</tr>
</tbody>
</table>
1.8 V PFE 0               1801 mV
1.8 V PFE 1               1804 mV
1.8 V PFE 2               1798 mV
1.8 V PFE 3               1798 mV
1.2 V PFE 0               1169 mV
1.2 V PFE 1               1189 mV
1.2 V PFE 2               1182 mV
1.2 V PFE 3               1176 mV
I2C Slave Revision         42

FPC 2 status:
State                      Online
Temperature Intake         33 degrees C / 91 degrees F
Temperature Exhaust A      41 degrees C / 105 degrees F
Temperature Exhaust B      53 degrees C / 127 degrees F
Temperature I3 0 TSensor  53 degrees C / 127 degrees F
Temperature I3 1 TSensor  52 degrees C / 125 degrees F
Temperature I3 1 Chip      56 degrees C / 132 degrees F
Temperature I3 2 TSensor  50 degrees C / 122 degrees F
Temperature I3 2 Chip      52 degrees C / 125 degrees F
Temperature I3 3 TSensor  46 degrees C / 114 degrees F
Temperature I3 3 Chip      49 degrees C / 120 degrees F
Temperature IA 0 TSensor  51 degrees C / 123 degrees F
Temperature IA 0 Chip      49 degrees C / 120 degrees F
Temperature IA 1 TSensor  48 degrees C / 118 degrees F
Temperature IA 1 Chip      53 degrees C / 127 degrees F
Power
1.5 V                     1492 mV
2.5 V                     2445 mV
3.3 V                     3293 mV
1.8 V PFE 0               1827 mV
1.8 V PFE 1               1775 mV
1.8 V PFE 2               1788 mV
1.8 V PFE 3               1798 mV
1.2 V PFE 0               1250 mV
1.2 V PFE 1               1234 mV
1.2 V PFE 2               1231 mV
1.2 V PFE 3               1192 mV
I2C Slave Revision         42

show chassis environment fpc (MX480 Router)

user@host> show chassis environment fpc
FPC 1 status:
State                      Online
Temperature Intake         36 degrees C / 96 degrees F
Temperature Exhaust A      41 degrees C / 105 degrees F
Temperature Exhaust B      55 degrees C / 131 degrees F
Temperature I3 0 TSensor  55 degrees C / 131 degrees F
Temperature I3 0 Chip      57 degrees C / 134 degrees F
Temperature I3 1 TSensor  53 degrees C / 127 degrees F
Temperature I3 1 Chip      53 degrees C / 127 degrees F
Temperature I3 2 TSensor  52 degrees C / 125 degrees F
Temperature I3 2 Chip      49 degrees C / 120 degrees F
Temperature I3 3 TSensor  47 degrees C / 116 degrees F
Temperature I3 3 Chip      47 degrees C / 116 degrees F
Temperature IA 0 TSensor  54 degrees C / 129 degrees F
Temperature IA 0 Chip      58 degrees C / 136 degrees F
Temperature IA 1 TSensor  48 degrees C / 118 degrees F
Temperature IA 1 Chip      53 degrees C / 127 degrees F
Power
show chassis environment fpc

user@host> show chassis environment fpc

FPC 5 status:

Power

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 V</td>
<td>1479 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2542 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3319 mV</td>
</tr>
<tr>
<td>1.8 V PFE 0</td>
<td>1811 mV</td>
</tr>
<tr>
<td>1.8 V PFE 1</td>
<td>1804 mV</td>
</tr>
<tr>
<td>1.8 V PFE 2</td>
<td>1804 mV</td>
</tr>
<tr>
<td>1.8 V PFE 3</td>
<td>1814 mV</td>
</tr>
<tr>
<td>1.2 V PFE 0</td>
<td>1192 mV</td>
</tr>
<tr>
<td>1.2 V PFE 1</td>
<td>1202 mV</td>
</tr>
<tr>
<td>1.2 V PFE 2</td>
<td>1205 mV</td>
</tr>
<tr>
<td>1.2 V PFE 3</td>
<td>1189 mV</td>
</tr>
</tbody>
</table>

I2C Slave Revision: 40

FPC 6 status:

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Reading</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5 V</td>
<td>1479 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2523 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3254 mV</td>
</tr>
<tr>
<td>1.8 V PFE 0</td>
<td>1798 mV</td>
</tr>
<tr>
<td>1.8 V PFE 1</td>
<td>1798 mV</td>
</tr>
<tr>
<td>1.8 V PFE 2</td>
<td>1807 mV</td>
</tr>
<tr>
<td>1.8 V PFE 3</td>
<td>1791 mV</td>
</tr>
<tr>
<td>1.2 V PFE 0</td>
<td>1173 mV</td>
</tr>
<tr>
<td>1.2 V PFE 1</td>
<td>1179 mV</td>
</tr>
<tr>
<td>1.2 V PFE 2</td>
<td>1179 mV</td>
</tr>
<tr>
<td>1.2 V PFE 3</td>
<td>1185 mV</td>
</tr>
</tbody>
</table>

I2C Slave Revision: 6
Temperature IA 1 TSensor 37 degrees C / 98 degrees F
Temperature IA 1 Chip 42 degrees C / 107 degrees F
Power
1.5 V 1485 mV
2.5 V 2510 mV
3.3 V 3332 mV
1.8 V PFE 0 1801 mV
1.8 V PFE 1 1814 mV
1.8 V PFE 2 1804 mV
1.8 V PFE 3 1820 mV
1.2 V PFE 0 1192 mV
1.2 V PFE 1 1189 mV
1.2 V PFE 2 1202 mV
1.2 V PFE 3 1156 mV
I2C Slave Revision 40

show chassis environment fpc (MX480 Router with 100-Gigabit Ethernet CFP)

user@host> show chassis environment fpc

FPC 0 status:
State             Online
Temperature Intake 32 degrees C / 89 degrees F
Temperature Exhaust A 39 degrees C / 102 degrees F
Temperature Exhaust B 37 degrees C / 98 degrees F
Temperature QX 0 TSen 44 degrees C / 111 degrees F
Temperature QX 0 Chip 48 degrees C / 118 degrees F
Temperature LU 0 TSen 44 degrees C / 111 degrees F
Temperature LU 0 Chip 48 degrees C / 118 degrees F
Temperature MQ 0 TSen 44 degrees C / 111 degrees F
Temperature MQ 0 Chip 47 degrees C / 116 degrees F
Power
MPC-BIAS3V3-zl2105 3297 mV
MPC-VDD3V3-zl2105 3306 mV
MPC-VDD2V5-zl2105 2498 mV
MPC-TCAM_1V0-zl2004 999 mV
MPC-AVDD1V0-zl2006 999 mV
MPC-VDD1V8-zl2006 1796 mV
MPC-PCIE_1V0-zl2006 1002 mV
MPC-LU0_1V0-zl2004 997 mV
MPC-MQ0_1V0-zl2004 995 mV
MPC-VDD_1V5-zl2004 1496 mV
MPC-PMB_1V1-zl2006 1094 mV
MPC-9VA-BMR453 9054 mV
MPC-9VB-BMR453 9037 mV
MPC-PMB_1V2-zl2106 1191 mV
MPC-QXMO_1V0-zl2006 1000 mV
I2C Slave Revision 66

FPC 1 status:
State             Online
Temperature Intake 35 degrees C / 95 degrees F
Temperature Exhaust A 50 degrees C / 122 degrees F
Temperature Exhaust B 56 degrees C / 132 degrees F
Temperature LU 0 TSen 46 degrees C / 114 degrees F
Temperature LU 0 Chip 59 degrees C / 138 degrees F
Temperature LU 1 TSen 46 degrees C / 114 degrees F
Temperature LU 1 Chip 45 degrees C / 113 degrees F
Temperature LU 2 TSen 46 degrees C / 114 degrees F
Temperature LU 2 Chip 60 degrees C / 140 degrees F
Temperature LU 3 TSen 46 degrees C / 114 degrees F
Temperature LU 3 Chip      71 degrees C / 159 degrees F
Temperature XM 0 TSen      46 degrees C / 114 degrees F
Temperature XM 0 Chip      -18 degrees C / 0 degrees F
Temperature XF 0 TSen      46 degrees C / 114 degrees F
Temperature XF 0 Chip      76 degrees C / 168 degrees F

Power
MPC-BIAS3V3-zl2105        3292 mV
MPC-VDD3V3-zl6100         3303 mV
MPC-VDD2V5-zl6100         2501 mV
MPC-VDD1V8-zl2004         1801 mV
MPC-AVDD1V0-zl12006       996 mV
MPC-VDD2V2-zl6100         1199 mV
MPC-VDD1V5A-zl12004       1493 mV
MPC-VDD1V5B-zl12004       1498 mV
MPC-XF_0V9-zl12006        996 mV
MPC-PCI1V0-zl16100        1000 mV
MPC-LU0_1V0-zl2004        994 mV
MPC-LU1_1V0-zl2004        994 mV
MPC-LU2_1V0-zl2004        992 mV
MPC-LU3_1V0-zl2004        993 mV
MPC-12VA-BMR453          12003 mV
MPC-12VB-BMR453          12043 mV
MPC-PMB_1V1-zl12006       1091 mV
MPC-PMB_1V2-zl12106       1196 mV
MPC-XM_0V9-vt273m          899 mV
I2C Slave Revision         81

show chassis environment fpc (MX240, MX480, MX960 with Application Services Modular Line Card)

user@host> show chassis environment fpc 1
FPC 1 status:
State                           Online
Temperature Intake              36 degrees C / 96 degrees F
Temperature Exhaust A           39 degrees C / 102 degrees F
Temperature LU TSen             52 degrees C / 125 degrees F
Temperature LU Chip             54 degrees C / 129 degrees F
Temperature XM TSen             52 degrees C / 125 degrees F
Temperature XM Chip             60 degrees C / 140 degrees F
Temperature PCIe TSen           52 degrees C / 125 degrees F
Temperature PCIe Chip           69 degrees C / 156 degrees F
Power:
MPC-BIAS3V3-zl2106              3302 mV
MPC-VDD3V3-zl6100               3325 mV
MPC-AVDD1V0-zl16100             3007 mV
MPC-PCI1V0-zl16100              904 mV
MPC-LU0_1V0-zl12004             996 mV
MPC-VDD1V5-zl12004              1498 mV
MPC-12VA-BMR453                 11733 mV
MPC-12VB-BMR453                 11728 mV
MPC-XM_0V9-vt273m                900 mV
I2C Slave Revision              81

show chassis environment fpc (T320, T640, and T1600 Routers)

user@host> show chassis environment fpc
FPC 0 status:
State                           Online
Temperature Top                 42 degrees C / 107 degrees F
Temperature Bottom              36 degrees C / 96 degrees F
Temperature MMB1                 39 degrees C / 102 degrees F
Power:

---

Copyright © 2013, Juniper Networks, Inc.
### FPC 1 status:

- **State**: Online
- **Temperature Top**: 42 degrees C / 107 degrees F
- **Temperature Bottom**: 39 degrees C / 102 degrees F
- **Temperature MMB1**: 40 degrees C / 104 degrees F

**Power**:
- **1.8 V**: 1956 mV
- **2.5 V**: 2498 mV
- **3.3 V**: 3340 mV
- **5.0 V**: 5042 mV
- **1.8 V bias**: 1797 mV
- **3.3 V bias**: 3311 mV
- **5.0 V bias**: 5013 mV
- **8.0 V bias**: 7221 mV

**BUS Revision**: 40

### FPC 2 status:

- **State**: Online
- **Temperature Top**: 43 degrees C / 109 degrees F
- **Temperature Bottom**: 39 degrees C / 102 degrees F
- **Temperature MMB1**: 41 degrees C / 105 degrees F

**Power**:
- **1.8 V**: 1963 mV
- **2.5 V**: 2503 mV
- **3.3 V**: 3340 mV
- **5.0 V**: 5042 mV
- **1.8 V bias**: 1797 mV
- **3.3 V bias**: 3311 mV
- **5.0 V bias**: 5013 mV
- **8.0 V bias**: 7221 mV

**BUS Revision**: 40

---

**show chassis environment fpc**

`user@host> show chassis environment fpc`

### FPC 0 status:

- **State**: Online
- **Fan Intake**: 34 degrees C / 93 degrees F
- **Fan Exhaust**: 48 degrees C / 118 degrees F
- **PMB**: 47 degrees C / 116 degrees F
- **LMB0**: 50 degrees C / 122 degrees F
- **LMB1**: 41 degrees C / 105 degrees F
- **LMB2**: 35 degrees C / 95 degrees F
- **PFE1 LU2**: 46 degrees C / 114 degrees F
- **PFE1 LU0**: 41 degrees C / 105 degrees F
- **PFE0 LU0**: 57 degrees C / 134 degrees F
- **XF1**: 47 degrees C / 116 degrees F
- **XF0**: 52 degrees C / 125 degrees F
- **XM1**: 41 degrees C / 105 degrees F
- **XM0**: 50 degrees C / 122 degrees F
- **PFE0 LU1**: 56 degrees C / 132 degrees F
- **PFE0 LU2**: 45 degrees C / 113 degrees F
- **PFE1 LU1**: 37 degrees C / 98 degrees F

---
### Power 1

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V</td>
<td></td>
<td>991</td>
</tr>
<tr>
<td>1.2 V bias</td>
<td></td>
<td>1195</td>
</tr>
<tr>
<td>1.8 V</td>
<td></td>
<td>1788</td>
</tr>
<tr>
<td>2.5 V</td>
<td></td>
<td>2483</td>
</tr>
<tr>
<td>3.3 V</td>
<td></td>
<td>3289</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td></td>
<td>3299</td>
</tr>
<tr>
<td>12.0 V A</td>
<td></td>
<td>10608</td>
</tr>
<tr>
<td>12.0 V B</td>
<td></td>
<td>10637</td>
</tr>
</tbody>
</table>

### Power 2

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9 V</td>
<td></td>
<td>881</td>
</tr>
<tr>
<td>0.9 V PFE0</td>
<td></td>
<td>916</td>
</tr>
<tr>
<td>0.9 V PFE1</td>
<td></td>
<td>903</td>
</tr>
<tr>
<td>1.0 V PFE0</td>
<td></td>
<td>1012</td>
</tr>
<tr>
<td>1.0 V PFE1</td>
<td></td>
<td>1002</td>
</tr>
<tr>
<td>1.1 V</td>
<td></td>
<td>1095</td>
</tr>
<tr>
<td>1.5 V_0</td>
<td></td>
<td>1494</td>
</tr>
<tr>
<td>1.5 V_1</td>
<td></td>
<td>1479</td>
</tr>
</tbody>
</table>

### Power 3

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V PFE0</td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>1.0 V PFE1</td>
<td></td>
<td>1002</td>
</tr>
<tr>
<td>1.0 V PFE0 *</td>
<td></td>
<td>995</td>
</tr>
<tr>
<td>1.0 V PFE1 *</td>
<td></td>
<td>995</td>
</tr>
<tr>
<td>1.8 V PFE 0</td>
<td></td>
<td>1788</td>
</tr>
<tr>
<td>1.8 V PFE 1</td>
<td></td>
<td>1789</td>
</tr>
<tr>
<td>2.5 V</td>
<td></td>
<td>2482</td>
</tr>
<tr>
<td>12.0 V</td>
<td></td>
<td>11614</td>
</tr>
</tbody>
</table>

### Power 4

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 V PFE0 LU0</td>
<td></td>
<td>1003</td>
</tr>
<tr>
<td>1.0 V PFE1 LU0</td>
<td></td>
<td>1003</td>
</tr>
<tr>
<td>1.0 V PFE1 LU2</td>
<td></td>
<td>1004</td>
</tr>
<tr>
<td>1.0 V PFE0 LU0 *</td>
<td></td>
<td>995</td>
</tr>
<tr>
<td>1.0 V PFE1 LU0 *</td>
<td></td>
<td>998</td>
</tr>
<tr>
<td>1.0 V PFE1 LU2 *</td>
<td></td>
<td>996</td>
</tr>
<tr>
<td>12.0 V</td>
<td></td>
<td>11643</td>
</tr>
<tr>
<td>12.0 V C</td>
<td></td>
<td>11711</td>
</tr>
</tbody>
</table>

### Power (Base/PMB/MMB)

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Voltage</th>
<th>mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMB0 VDD2V5</td>
<td></td>
<td>2488</td>
</tr>
<tr>
<td>LMB0 VDD1V8</td>
<td></td>
<td>1788</td>
</tr>
<tr>
<td>LMB0 VDD1V5</td>
<td></td>
<td>1496</td>
</tr>
<tr>
<td>LMB0 PFE0 LU0 AVDD1V0</td>
<td></td>
<td>1002</td>
</tr>
<tr>
<td>LMB0 PFE0 LU0 VDD1V0</td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>LMB0 VDD12V0</td>
<td></td>
<td>10752</td>
</tr>
<tr>
<td>LMB1 VDD2V5</td>
<td></td>
<td>2472</td>
</tr>
<tr>
<td>LMB1 VDD1V8</td>
<td></td>
<td>1792</td>
</tr>
<tr>
<td>LMB1 VDD1V5</td>
<td></td>
<td>1480</td>
</tr>
<tr>
<td>LMB1 PFE0 LU2 AVDD1V0</td>
<td></td>
<td>994</td>
</tr>
<tr>
<td>LMB1 PFE0 LU2 VDD1V0</td>
<td></td>
<td>1002</td>
</tr>
<tr>
<td>LMB1 VDD12V0</td>
<td></td>
<td>10800</td>
</tr>
<tr>
<td>LMB2 VDD2V5</td>
<td></td>
<td>2472</td>
</tr>
<tr>
<td>LMB2 VDD1V8</td>
<td></td>
<td>1792</td>
</tr>
<tr>
<td>LMB2 VDD1V5</td>
<td></td>
<td>1486</td>
</tr>
<tr>
<td>LMB2 PFE1 LU1 AVDD1V0</td>
<td></td>
<td>996</td>
</tr>
<tr>
<td>LMB2 PFE1 LU1 VDD1V0</td>
<td></td>
<td>998</td>
</tr>
<tr>
<td>LMB2 VDD12V0</td>
<td></td>
<td>10704</td>
</tr>
<tr>
<td>PMB 1.05v</td>
<td></td>
<td>1049</td>
</tr>
<tr>
<td>PMB 1.5v</td>
<td></td>
<td>1500</td>
</tr>
<tr>
<td>PMB 2.5v</td>
<td></td>
<td>2500</td>
</tr>
<tr>
<td>PMB 3.3v</td>
<td></td>
<td>3299</td>
</tr>
</tbody>
</table>

### Bus Revision

Bus Revision: 113

FPC 3 status:
<table>
<thead>
<tr>
<th>Component</th>
<th>Temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Online</td>
</tr>
<tr>
<td>Fan Intake</td>
<td>37°C / 98°F</td>
</tr>
<tr>
<td>Fan Exhaust</td>
<td>51°C / 123°F</td>
</tr>
<tr>
<td>PMB</td>
<td>43°C / 109°F</td>
</tr>
<tr>
<td>LMB0</td>
<td>57°C / 134°F</td>
</tr>
<tr>
<td>LMB1</td>
<td>54°C / 129°F</td>
</tr>
<tr>
<td>LMB2</td>
<td>38°C / 100°F</td>
</tr>
<tr>
<td>PFE1 LU2</td>
<td>63°C / 145°F</td>
</tr>
<tr>
<td>PFE1 LU0</td>
<td>45°C / 113°F</td>
</tr>
<tr>
<td>PFE0 LU0</td>
<td>69°C / 156°F</td>
</tr>
<tr>
<td>XF1</td>
<td>62°C / 143°F</td>
</tr>
<tr>
<td>XF0</td>
<td>63°C / 145°F</td>
</tr>
<tr>
<td>XM1</td>
<td>43°C / 129°F</td>
</tr>
<tr>
<td>XM0</td>
<td>67°C / 152°F</td>
</tr>
<tr>
<td>PFE0 LU1</td>
<td>63°C / 145°F</td>
</tr>
<tr>
<td>PFE0 LU2</td>
<td>66°C / 150°F</td>
</tr>
<tr>
<td>PFE1 LU1</td>
<td>41°C / 105°F</td>
</tr>
<tr>
<td>Power 1</td>
<td></td>
</tr>
<tr>
<td>1.0 V</td>
<td>1002 mV</td>
</tr>
<tr>
<td>1.2 V bias</td>
<td>1201 mV</td>
</tr>
<tr>
<td>1.8 V</td>
<td>1785 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2485 mV</td>
</tr>
<tr>
<td>3.3 V</td>
<td>3288 mV</td>
</tr>
<tr>
<td>3.3 V bias</td>
<td>3285 mV</td>
</tr>
<tr>
<td>12.0 V A</td>
<td>10412 mV</td>
</tr>
<tr>
<td>12.0 V B</td>
<td>10515 mV</td>
</tr>
<tr>
<td>Power 2</td>
<td></td>
</tr>
<tr>
<td>0.9 V</td>
<td>882 mV</td>
</tr>
<tr>
<td>0.9 V PFE0</td>
<td>920 mV</td>
</tr>
<tr>
<td>0.9 V PFE1</td>
<td>905 mV</td>
</tr>
<tr>
<td>1.0 V PFE0</td>
<td>1015 mV</td>
</tr>
<tr>
<td>1.0 V PFE1</td>
<td>1001 mV</td>
</tr>
<tr>
<td>1.1 V</td>
<td>1094 mV</td>
</tr>
<tr>
<td>1.5 V_0</td>
<td>1495 mV</td>
</tr>
<tr>
<td>1.5 V_1</td>
<td>1478 mV</td>
</tr>
<tr>
<td>Power 3</td>
<td></td>
</tr>
<tr>
<td>0.92 V PFE1</td>
<td>998 mV</td>
</tr>
<tr>
<td>1.0 V PFE0</td>
<td>997 mV</td>
</tr>
<tr>
<td>1.0 V PFE0</td>
<td>992 mV</td>
</tr>
<tr>
<td>1.0 V PFE1</td>
<td>991 mV</td>
</tr>
<tr>
<td>1.8 V PFE 0</td>
<td>1780 mV</td>
</tr>
<tr>
<td>1.8 V PFE 1</td>
<td>1797 mV</td>
</tr>
<tr>
<td>2.5 V</td>
<td>2492 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11604 mV</td>
</tr>
<tr>
<td>Power 4</td>
<td></td>
</tr>
<tr>
<td>1.0 V PFE0 LU0</td>
<td>1003 mV</td>
</tr>
<tr>
<td>1.0 V PFE1 LU0</td>
<td>1004 mV</td>
</tr>
<tr>
<td>1.0 V PFE1 LU2</td>
<td>1003 mV</td>
</tr>
<tr>
<td>1.0 V PFE0 LU0 *</td>
<td>1000 mV</td>
</tr>
<tr>
<td>1.0 V PFE1 LU0 *</td>
<td>1001 mV</td>
</tr>
<tr>
<td>1.0 V PFE1 LU2 *</td>
<td>1003 mV</td>
</tr>
<tr>
<td>12.0 V</td>
<td>11653 mV</td>
</tr>
<tr>
<td>12.0 V C</td>
<td>11672 mV</td>
</tr>
<tr>
<td>Power (Base/PMB/MMB)</td>
<td></td>
</tr>
<tr>
<td>LMB0 VDD2V5</td>
<td>2512 mV</td>
</tr>
<tr>
<td>LMB0 VDD1V8</td>
<td>1790 mV</td>
</tr>
<tr>
<td>LMB0 VDD1V5</td>
<td>1500 mV</td>
</tr>
<tr>
<td>LMB0 PFE0 LU0 AVDD1V0</td>
<td>1004 mV</td>
</tr>
<tr>
<td>LMB0 PFE0 LU0 VDD1V0</td>
<td>1002 mV</td>
</tr>
<tr>
<td>LMB0 VDD12V0</td>
<td>10608 mV</td>
</tr>
<tr>
<td>LMB1 VDD2V5</td>
<td>2472 mV</td>
</tr>
<tr>
<td>Component</td>
<td>Voltage (mV)</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>LMB1 VDD1V8</td>
<td>1788 mV</td>
</tr>
<tr>
<td>LMB1 VDD1V5</td>
<td>1480 mV</td>
</tr>
<tr>
<td>LMB1 PFE0 LU2 AVDD1V0</td>
<td>1000 mV</td>
</tr>
<tr>
<td>LMB1 PFE0 LU2 VDD1V0</td>
<td>1004 mV</td>
</tr>
<tr>
<td>LMB1 VDD12V0</td>
<td>10672 mV</td>
</tr>
<tr>
<td>LMB2 VDD2V5</td>
<td>2488 mV</td>
</tr>
<tr>
<td>LMB2 VDD1V8</td>
<td>1798 mV</td>
</tr>
<tr>
<td>LMB2 VDD1V5</td>
<td>1494 mV</td>
</tr>
<tr>
<td>LMB2 PFE1 LU1 AVDD1V0</td>
<td>1000 mV</td>
</tr>
<tr>
<td>LMB2 PFE1 LU1 VDD1V0</td>
<td>1004 mV</td>
</tr>
<tr>
<td>LMB2 VDD12V0</td>
<td>10528 mV</td>
</tr>
<tr>
<td>PMB 1.05v</td>
<td>1050 mV</td>
</tr>
<tr>
<td>PMB 1.5v</td>
<td>1500 mV</td>
</tr>
<tr>
<td>PMB 2.5v</td>
<td>2499 mV</td>
</tr>
<tr>
<td>PMB 3.3v</td>
<td>3299 mV</td>
</tr>
<tr>
<td>Bus Revision</td>
<td>113</td>
</tr>
</tbody>
</table>

**FPC 5 status:**

- **State:** Online
- **Temperature Top:** 39 degrees C / 102 degrees F
- **Temperature Bottom:** 38 degrees C / 100 degrees F

**Power**

- **1.8 V** | 1804 mV
- **1.8 V bias** | 1802 mV
- **3.3 V** | 3294 mV
- **3.3 V bias** | 3277 mV
- **5.0 V bias** | 5008 mV
- **5.0 V TOP** | 5067 mV
- **8.0 V bias** | 6642 mV

**Power (Base/PMB/MMB)**

- **1.2 V** | 1202 mV
- **1.5 V** | 1504 mV
- **5.0 V BOT** | 5079 mV
- **12.0 V TOP Base** | 11848 mV
- **12.0 V BOT Base** | 11780 mV
- **1.1 V PMB** | 1111 mV
- **1.2 V PMB** | 1189 mV
- **1.5 V PMB** | 1494 mV
- **1.8 V PMB** | 1819 mV
- **2.5 V PMB** | 2503 mV
- **3.3 V PMB** | 3294 mV
- **5.0 V PMB** | 5035 mV
- **12.0 V PMB** | 11788 mV

- **0.75 MMB TOP** | 766 mV
- **1.5 V MMB TOP** | 1484 mV
- **1.8 V MMB TOP** | 1772 mV
- **2.5 V MMB TOP** | 2485 mV
- **1.2 V MMB TOP** | 1137 mV
- **5.0 V MMB TOP** | 4946 mV
- **12.0 V MMB TOP** | 11772 mV
- **3.3 V MMB TOP** | 3289 mV

- **0.75 MMB BOT** | 759 mV
- **1.5 V MMB BOT** | 1482 mV
- **1.8 V MMB BOT** | 1792 mV
- **2.5 V MMB BOT** | 2490 mV
- **1.2 V MMB BOT** | 1145 mV
- **5.0 V MMB BOT** | 4922 mV
- **12.0 V MMB BOT** | 11625 mV
- **3.3 V MMB BOT** | 3282 mV

- **APS 00** | 2495 mV
- **APS 01** | 3308 mV
- **APS 02** | 3301 mV
<table>
<thead>
<tr>
<th>Voltage</th>
<th>PIC</th>
<th>Voltage</th>
<th>PIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0 V</td>
<td>0</td>
<td>4967 mV</td>
<td></td>
</tr>
<tr>
<td>APS 10</td>
<td></td>
<td>2512 mV</td>
<td></td>
</tr>
<tr>
<td>APS 11</td>
<td></td>
<td>3316 mV</td>
<td></td>
</tr>
<tr>
<td>APS 12</td>
<td></td>
<td>3304 mV</td>
<td></td>
</tr>
<tr>
<td>5.0 V</td>
<td>1</td>
<td>5081 mV</td>
<td></td>
</tr>
</tbody>
</table>

**Bus Revision:** 49

**FPC 6 status:**
- **State:** Online
- **Fan Intake:** 34 degrees C / 93 degrees F
- **Fan Exhaust:** 49 degrees C / 120 degrees F
- **PMB:** 40 degrees C / 104 degrees F
- **LMB0:** 60 degrees C / 140 degrees F
- **LMB1:** 58 degrees C / 136 degrees F
- **LMB2:** 40 degrees C / 104 degrees F
- **PFE1 LU2:** 69 degrees C / 156 degrees F
- **PFE1 LU0:** 45 degrees C / 113 degrees F
- **PFE0 LU0:** 71 degrees C / 159 degrees F
- **XF1:** 58 degrees C / 136 degrees F
- **XF0:** 65 degrees C / 149 degrees F
- **XM1:** 40 degrees C / 104 degrees F
- **XM0:** 66 degrees C / 150 degrees F
- **PFE0 LU1:** 69 degrees C / 156 degrees F
- **PFE0 LU2:** 68 degrees C / 154 degrees F
- **PFE1 LU1:** 42 degrees C / 107 degrees F

**Power 1**
- **1.0 V:** 998 mV
- **1.2 V bias:** 1191 mV
- **1.8 V:** 1781 mV
- **2.5 V:** 2487 mV
- **3.3 V bias:** 3302 mV
- **12.0 V A:** 10388 mV
- **12.0 V B:** 10388 mV

**Power 2**
- **0.9 V:** 902 mV
- **0.9 V PFE0:** 921 mV
- **0.9 V PFE1:** 907 mV
- **1.0 V PFE0:** 996 mV
- **1.0 V PFE1:** 974 mV
- **1.1 V:** 1095 mV
- **1.5 V_0:** 1495 mV
- **1.5 V_1:** 1478 mV

**Power 3**
- **1.0 V PFE0:** 997 mV
- **1.0 V PFE1:** 998 mV
- **1.0 V PFE0 *:** 993 mV
- **1.0 V PFE1 *:** 991 mV
- **1.8 V PFE 0:** 1796 mV
- **1.8 V PFE 1:** 1789 mV
- **2.5 V:** 2465 mV
- **12.0 V:** 11609 mV

**Power 4**
- **1.0 V PFE0 LU0:** 1003 mV
- **1.0 V PFE1 LU0:** 1006 mV
- **1.0 V PFE1 LU2:** 1002 mV
- **1.0 V PFE0 LU0 *:** 1000 mV
- **1.0 V PFE1 LU0 *:** 998 mV
- **1.0 V PFE1 LU2 *:** 998 mV
- **12.0 V:** 11638 mV
- **12.0 V C:** 11702 mV

**Power (Base/PMB/MMB)**
show chassis environment fpc lcc (TX Matrix Router)

user@host> show chassis environment fpc lcc 0
lcc0-re0:

--------------------------------------------------------------------------
FPC 1 status:
State                           Online
Temperature Top              30 degrees C / 86 degrees F
Temperature Bottom           25 degrees C / 77 degrees F
Temperature MMB0                Absent
Temperature MMB1             27 degrees C / 80 degrees F
Power:
  1.8 V                    1813 mV
  2.5 V                    2504 mV
  3.3 V                    3338 mV
  5.0 V                    5037 mV
  1.8 V bias               1797 mV
  3.3 V bias               3301 mV
  5.0 V bias               5013 mV
  8.0 V bias               7345 mV
BUS Revision                 40

FPC 2 status:
State                           Online
Temperature Top              37 degrees C / 98 degrees F
Temperature Bottom           26 degrees C / 78 degrees F
Temperature MMB0             32 degrees C / 89 degrees F
Temperature MMB1             27 degrees C / 80 degrees F
Power:
  1.8 V                    1791 mV
  2.5 V                    2517 mV
  3.3 V                    3308 mV
  5.0 V                    5052 mV
  1.8 V bias               1797 mV
  3.3 V bias               3289 mV
  5.0 V bias               4991 mV
8.0 V bias 7477 mV
BUS Revision 40

show chassis environment fpc lcc (TX Matrix Plus Router)

user@host> show chassis environment fpc lcc 0
lcc0-re0:

--------------------------------------------------------------------------
FPC 1 status:
State Online
Temperature Top 46 degrees C / 114 degrees F
Temperature Bottom 47 degrees C / 116 degrees F
Power
1.8 V 1788 mV
1.8 V bias 1787 mV
3.3 V 3321 mV
3.3 V bias 3306 mV
5.0 V bias 5018 mV
5.0 V TOP 5037 mV
8.0 V bias 7223 mV
Power (Base/PMB/MMB)
1.2 V 1205 mV
1.5 V 1503 mV
5.0 V BOT 5084 mV
12.0 V TOP Base 11775 mV
12.0 V BOT Base 11794 mV
1.1 V PMB 1108 mV
1.2 V PMB 1196 mV
1.5 V PMB 1499 mV
1.8 V PMB 1811 mV
2.5 V PMB 2515 mV
3.3 V PMB 3318 mV
5.0 V PMB 5030 mV
12.0 V PMB 11832 mV
0.75 MMB TOP 752 mV
1.5 V MMB TOP 1489 mV
1.8 V MMB TOP 1782 mV
2.5 V MMB TOP 2498 mV
1.2 V MMB TOP 1335 mV
5.0 V MMB TOP 4902 mV
12.0 V MMB TOP 11721 mV
3.3 V MMB TOP 3316 mV
0.75 MMB BOT 754 mV
1.5 V MMB BOT 1482 mV
1.8 V MMB BOT 1758 mV
2.5 V MMB BOT 2488 mV
1.2 V MMB BOT 1157 mV
5.0 V MMB BOT 4962 mV
12.0 V MMB BOT 11691 mV
3.3 V MMB BOT 3308 mV
APS 00 1484 mV
APS 01 2503 mV
APS 02 3313 mV
5.0 V PIC 0 5025 mV
APS 10 1501 mV
APS 11 2466 mV
APS 12 3311 mV
5.0 V PIC 1 5081 mV
Bus Revision 49
show chassis environment fpc (QFX Series)

user@switch>  show chassis environment fpc 0
FPC 0 status:
  State                      Online
  Temperature                42 degrees C / 107 degrees F

show chassis environment fpc interconnect-device (QFabric Systems)

user@switch>  show chassis environment fpc interconnect-device interconnect1 0
FC 0 FPC 0 status:
  State                      Online
  Left Intake Temperature    24 degrees C / 75 degrees F
  Right Intake Temperature   24 degrees C / 75 degrees F
  Left Exhaust Temperature   27 degrees C / 80 degrees F
  Right Exhaust Temperature  27 degrees C / 80 degrees F
  Power
    BIAS 3V3                  3330 mV
    VDD 3V3                   3300 mV
    VDD 2V5                   2502 mV
    VDD 1V5                   1496 mV
    VDD 1V2                   1194 mV
    VDD 1V0                   1000 mV
    Sw0 VDD 1V0               1020 mV
    Sw0 CVDD 1V025            1032 mV
    Sw1 VDD 1V0               1022 mV
    Sw1 CVDD 1V025            1030 mV
    VDD 12V0 DIV3_33          3414 mV

show chassis environment fpc 0 (PTX5000 Packet Transport Router)

user@switch>  show chassis environment fpc 0
FPC 0 status:
  State                      Online
  PMB Temperature            35 degrees C / 95 degrees F
  Intake Temperature         33 degrees C / 91 degrees F
  Exhaust A Temperature      51 degrees C / 123 degrees F
  Exhaust B Temperature      43 degrees C / 109 degrees F
  TL0 Temperature            48 degrees C / 118 degrees F
  TQ0 Temperature            53 degrees C / 127 degrees F
  TL1 Temperature            56 degrees C / 132 degrees F
  TQ1 Temperature            58 degrees C / 136 degrees F
  TL2 Temperature            55 degrees C / 131 degrees F
  TQ2 Temperature            57 degrees C / 134 degrees F
  TL3 Temperature            59 degrees C / 138 degrees F
  TQ3 Temperature            59 degrees C / 138 degrees F
  Power
    PMB 1.05v                 1049 mV
    PMB 1.5v                  1500 mV
    PMB 2.5v                  2500 mV
    PMB 3.3v                  3299 mV
    PFE0 1.5v                 1500 mV
    PFE0 1.0v                 999 mV
    TQ0 0.9v                  900 mV
    TL0 0.9v                  900 mV
    PFE1 1.5v                 1499 mV
    PFE1 1.0v                 999 mV
    TQ1 0.9v                  899 mV
    TL1 0.9v                  900 mV
    PFE2 1.5v                 1500 mV
    PFE2 1.0v                 1000 mV
show chassis environment FPC 1 (MX Routers with Media Services Blade [MSB])

user@switch> show chassis environment fpc 1
FPC 1 status:
State                      Online
Temperature Intake         36 degrees C / 96 degrees F
Temperature Exhaust A      39 degrees C / 102 degrees F
Temperature LU TSen        52 degrees C / 125 degrees F
Temperature LU Chip        54 degrees C / 129 degrees F
Temperature XM TSen        52 degrees C / 125 degrees F
Temperature XM Chip        60 degrees C / 140 degrees F
Temperature PCIe TSen      52 degrees C / 125 degrees F
Temperature PCIe Chip      69 degrees C / 156 degrees F
Power
MPC-BIAS3V3-zl2106         3302 mV
MPC-VDD3V3-zl6100          3325 mV
MPC-AVDD1V0-zl6100         1007 mV
MPC-PCIE_1V0-zl6100        904 mV
MPC-LU0_1V0-zl2004         996 mV
MPC-VDD_1V5-zl2004         1498 mV
MPC-12VA-BMR453            11733 mV
MPC-12VB-BMR453            11728 mV
MPC-XM_0V9-vt273m          900 mV
I2C Slave Revision         81
### show chassis environment routing-engine

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show chassis environment routing-engine &lt;slot&gt;</td>
<td>Display Routing Engine environmental status information.</td>
</tr>
<tr>
<td>Syntax (TX Matrix Routers)</td>
<td>show chassis environment routing-engine &lt;lcc number</td>
</tr>
<tr>
<td>Syntax (TX Matrix Plus Routers)</td>
<td>show chassis environment routing-engine &lt;lcc number</td>
</tr>
<tr>
<td>Syntax (MX104, MX2010, and MX2020 3D Universal Edge Routers)</td>
<td>show chassis environment routing-engine &lt;slot&gt;</td>
</tr>
<tr>
<td>Syntax (MX Series Routers)</td>
<td>show chassis environment routing-engine &lt;slot&gt; &lt;all-members&gt; &lt;local&gt; &lt;member member-id&gt;</td>
</tr>
<tr>
<td>Syntax (QFX Series)</td>
<td>show chassis environment routing-engine interconnect-device name</td>
</tr>
</tbody>
</table>

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- Command introduced in Junos OS Release 12.1 for the PTX Series Packet Transport Routers.
- Command introduced in Junos OS Release 12.1 for the T4000 Core Routers.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
- Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

**Options**
- **none**—Display environmental information about all Routing Engines. For a TX Matrix router, display environmental information about all Routing Engines on the TX Matrix router and its attached T640 routers. For a TX Matrix Plus router, display environmental information about all Routing Engines on the TX Matrix Plus router and its attached routers.
- **all-members**—(MX Series routers only) (Optional) Display environmental information about the Routing Engines in all member routers in the Virtual Chassis configuration.
- **interconnect-device name**—(QFabric systems only) (Optional) Display environmental information about the Routing Engines for the Interconnect device.
**lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number. Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(MX Series routers only) (Optional) Display environmental information about the Routing Engines in the local Virtual Chassis member.

**member member-id**—(MX Series routers only) (Optional) Display environmental information about the Routing Engines in the specified member in the Virtual Chassis configuration. Replace *member-id* with the value of 0 or 1.

**scc**—(TX Matrix router only) (Optional) Display environmental information about the Routing Engine in the TX Matrix router (switch-card chassis).

**sfc**—(TX Matrix Plus router only) (Optional) Display environmental information about the Routing Engine in the TX Matrix Plus router (switch-fabric chassis).

**slot**—(Optional) Display environmental information about an individual Routing Engine. On M10i, M20, M40e, M120, M160, M320, MX Series, MX104 routers, MX2010 routers, MX2020 routers, and T Series routers, replace *slot* with 0 or 1. On M5, M7i, M10, and M40 routers and on the J Series router, replace *slot* with 0. On EX3200 and EX4200 standalone switches, replace *slot* with 0. On EX4200 switches in a Virtual Chassis configuration and on EX8208 and EX8216 switches, replace *slot* with 0 or 1. On the QFX3500 switch, there is only one Routing Engine, so you do not need to specify the slot number. On PTX Series Packet Transport Routers, replace *slot* with 0 or 1.

**Required Privilege Level**

- view

**Related Documentation**

- request chassis routing-engine master on page 175
- show chassis routing-engine on page 1070

**List of Sample Output**

- show chassis environment routing-engine (Nonredundant) on page 869
- show chassis environment routing-engine (Redundant) on page 869
- show chassis environment routing-engine (MX104 Router) on page 869
- show chassis environment routing-engine (MX2010 Router) on page 870
- show chassis environment routing-engine (MX2020 Router) on page 870
- show chassis environment routing-engine (TX Matrix Plus Router) on page 870
- show chassis environment routing-engine (T4000 Core Router) on page 870
Output Fields  Table 142 on page 869 lists the output fields for the `show chassis environment routing-engine` command. Output fields are listed in the approximate order in which they appear.

Table 142: show chassis environment routing-engine Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing engine slot status</td>
<td>Number of the Routing Engine slot: 0 or 1.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the Routing Engine:</td>
</tr>
<tr>
<td></td>
<td>• Online Master—Routing Engine is online, operating as Master.</td>
</tr>
<tr>
<td></td>
<td>• Online Standby—Routing Engine is online, operating as Standby.</td>
</tr>
<tr>
<td></td>
<td>• Offline—Routing Engine is offline.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Temperature of the air flowing past the Routing Engine.</td>
</tr>
<tr>
<td>CPU Temperature</td>
<td>(PTX Series and T4000 Core Routers only) Temperature of the air flowing past the Routing Engine CPU.</td>
</tr>
</tbody>
</table>

Sample Output

**show chassis environment routing-engine (Nonredundant)**

```
user@host> show chassis environment routing-engine
Routing Engine 0 status:
  State                        Online Master
  Temperature                 27 degrees C / 80 degrees
```

**show chassis environment routing-engine (Redundant)**

```
user@host> show chassis environment routing-engine
Routing Engine 0 status:
  State:                      Online Master
  Temperature:               26 degrees C / 78 degrees F

Routing Engine 1 status:
  State:                      Online Standby
  Temperature:               26 degrees C / 78 degrees F
```

**show chassis environment routing-engine (MX104 Router)**

```
user@host> show chassis environment routing-engine
Routing Engine 0 status:
  State                        Online Master
  Temperature                 34 degrees C / 93 degrees F
  CPU Temperature             43 degrees C / 109 degrees F

Routing Engine 1 status:
  State                        Online Standby
```
show chassis environment routing-engine (MX2010 Router)

user@host> show chassis environment routing-engine
Routing Engine 0 status:
  State                  Online Master
  Temperature            37 degrees C / 98 degrees F
  CPU Temperature        37 degrees C / 98 degrees F
Routing Engine 1 status:
  State                  Online Standby
  Temperature            35 degrees C / 95 degrees F
  CPU Temperature        34 degrees C / 93 degrees F

show chassis environment routing-engine (MX2020 Router)

user@host> show chassis environment routing-engine
Routing Engine 0 status:
  State                  Online Master
  Temperature            35 degrees C / 95 degrees F
  CPU Temperature        34 degrees C / 93 degrees F
Routing Engine 1 status:
  State                  Online Standby
  Temperature            44 degrees C / 111 degrees F
  CPU Temperature        43 degrees C / 109 degrees F

show chassis environment routing-engine (TX Matrix Plus Router)

user@host> show chassis environment routing-engine
sfc0-re0:
------------------------------------------------------------------------
Routing Engine 0 status:
  State                  Online Master
  Temperature            26 degrees C / 78 degrees F
Routing Engine 1 status:
  State                  Online Standby
  Temperature            28 degrees C / 82 degrees F
lcc0-re0:
------------------------------------------------------------------------
Routing Engine 0 status:
  State                  Online Master
  Temperature            30 degrees C / 86 degrees F
Routing Engine 1 status:
  State                  Online Standby
  Temperature            29 degrees C / 84 degrees F

show chassis environment routing-engine (T4000 Core Router)

user@host> show chassis environment routing-engine
Routing Engine 0 status:
  State                  Online Master
  Temperature            33 degrees C / 91 degrees F
  CPU Temperature        50 degrees C / 122 degrees F
Routing Engine 1 status:
  State                  Online Standby
  Temperature            33 degrees C / 91 degrees F
  CPU Temperature        46 degrees C / 114 degrees F
show chassis environment routing-engine (QFX Series)

user@switch> show chassis environment routing-engine
Routing Engine 0 status:
  State            Online Master
  Temperature      42 degrees C / 107 degrees F

show chassis environment routing-engine interconnect-device (QFabric System)

user@switch> show chassis environment routing-engine interconnect-device interconnect1
  routing-engine interconnect-device interconnect1
Routing Engine 0 status:
  State            Online Standby
  Temperature      52 degrees C / 125 degrees F
Routing Engine 1 status:
  State            Online Master
  Temperature      57 degrees C / 134 degrees F

show chassis environment routing-engine (PTX5000 Packet Transport Router)

user@switch> show chassis environment routing-engine
Routing Engine 0 status:
  State            Online Master
  Temperature      55 degrees C / 131 degrees F
  CPU Temperature  66 degrees C / 150 degrees F
Routing Engine 1 status:
  State            Online Standby
  Temperature      52 degrees C / 125 degrees F
  CPU Temperature  64 degrees C / 147 degrees F
### show chassis ethernet-switch

| Syntax (EX8200 Switch) | show chassis ethernet-switch  
<errors <port>> |
|-------------------------|--------------------------------------------------|
| Syntax (T4000 Router)   | show chassis ethernet-switch  
<errors <port> | statistics <port>> |
| Syntax (TX Matrix Router) | show chassis ethernet-switch  
<errors <port> | statistics <port>>  
<icc <number> | scc> |
| Syntax (TX Matrix Plus Router) | show chassis ethernet-switch  
<errors <port> | switch <number>  
<icc number | sfc number>  
<statistics <port> | switch <number> |
| Syntax (MX Series Router) | show chassis ethernet-switch  
<all-members>  
<errors <port>>  
<local>  
<member member-id> |
| Syntax (MX2010 and MX2020 3D Universal Edge Routers) | show chassis ethernet-switch  
<errors <port> | statistics <port>>  
<old-rom-packet-count> |
| Syntax (PTX Series Packet Transport Routers) | show chassis ethernet-switch  
<errors <port>>  
<statistics <port>>  
<port-state <port>> |

#### Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.4 for EX Series switches.
- sfc option introduced in Junos OS Release 9.6 for the TX Matrix Plus router.
- Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

#### Description

(M10i, M40e, M120, M160, M320, MX Series, and T Series routers and EX8200 and PTX Series routers only) Display information about the ports on the Control Board (CB) Ethernet switch.

#### Options

- **none**—Display information about each connected port on the Ethernet switch. On a TX Matrix router, display information about each connected port on the Ethernet switch on the TX Matrix router and its attached T640 routers. On a TX Matrix Plus router,
display information about each connected port on the Ethernet switch on the TX Matrix Plus router and its attached routers.

**all-members**—(MX Series routers only) (Optional) Display information about the ports on the CB Ethernet switch on all the members of the Virtual Chassis configuration.

**errors**—(Optional) Display the numbers and types of errors accumulated on all ports of the Ethernet switch.

**errors port**—(Optional) Display the numbers and types of errors accumulated on the specified port (0 through 15) of the Ethernet switch. On the TX Matrix router, replace `port` with a value from 0 through 15. On the TX Matrix Plus router and EX8200 switch, replace `port` with a value from 0 through 27. On the PTX Series Packet Transport Routers, replace `port` with a value from 0 through 27. On the T4000 routers, MX2020 routers, and MX2010 routers, replace `port` with a value from 0 through 27.

**errors switch number**—(TX Matrix Plus router only) (Optional) Display the numbers and types of errors accumulated on the specified switch. Replace `number` with a value from 0 through 2.

**lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number. Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(MX Series routers only) (Optional) Display information about the ports on the CB Ethernet switch on the local Virtual Chassis member.

**member member-id**—(MX Series routers only) (Optional) Display information about the ports on the CB Ethernet switch on the specified member of the Virtual Chassis configuration. Replace `member-id` with a value of 0 or 1.

**old-rom-packet-count**—(MX 2020 Routers only) (Optional) Display information about installed linecards. A non-zero number indicates that the bootrom on that linecard needs to be updated.

**port-state**—(PTX Series only) (Optional) Display information about current port operation (Blocking, Listening, or Disabled).

**scc**—(TX Matrix router only) (Optional) Display information about the ports on the CB's Ethernet switch on the TX Matrix router (switch-card chassis).
**sfc number**—(TX Matrix Plus router only) (Optional) Display information about the ports on the CB's Ethernet switch on the TX Matrix Plus router (or switch-fabric chassis). Replace `number` with 0.

**statistics**—(Optional) Display traffic statistics for each connected port on the Ethernet switch.

**statistics port**—(Optional) Display traffic statistics for the specified port on the Ethernet switch. On the TX Matrix router, replace `port` with a value from 0 through 25. On the TX Matrix Plus router or EX8200 switch, replace `port` with a value from 0 through 27. On the PTX Series Packet Transport Routers, replace `port` with a value from 0 through 25. On the T4000 routers, MX2020 routers, and MX2010 routers, replace `port` with a value from 0 through 27.

**statistics switch number**—(TX Matrix Plus routers and EX8200 switch only) (Optional) Display traffic statistics for the specified Ethernet switch number. On the TX Matrix Plus router and EX8216 switch, replace `number` with a value from 0 through 2. On the EX8208 switch, replace `number` with a value from 0 through 1.

**Required Privilege Level**

- **view**

**List of Sample Output**

- show chassis ethernet-switch on page 878
- show chassis ethernet-switch (MX480 Router with MPC4E) on page 879
- show chassis ethernet-switch (MX2010 Router) on page 880
- show chassis ethernet-switch statistics (MX2010 Router) on page 882
- show chassis ethernet-switch (MX2020 Router) on page 888
- show chassis ethernet-switch statistics (MX2020 Router) on page 891
- show chassis ethernet-switch (MX2020 Router with MPC4E) on page 899
- show chassis ethernet-switch (TX Matrix Router) on page 900
- show chassis ethernet-switch errors on page 901
- show chassis ethernet-switch statistics on page 902
- show chassis ethernet-switch errors (TX Matrix Plus Router) on page 903
- show chassis ethernet-switch sfc errors (TX Matrix Plus Router) on page 904
- show chassis ethernet-switch statistics (TX Matrix Plus Router) on page 905
- show chassis ethernet-switch (T4000 Router) on page 909
- show chassis ethernet-switch errors (T4000 Router) on page 910
- show chassis ethernet-switch (PTX5000 Packet Transport Router) on page 911
- show chassis ethernet-switch statistics (PTX5000 Packet Transport Router) on page 912
- show chassis ethernet-switch port-state (PTX5000 Packet Transport Router) on page 915

**Output Fields**

Table 143 on page 875 lists the output fields for the `show chassis ethernet-switch` command. Output fields are listed in the approximate order in which they appear.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| Link is good on port n connected to device | Information about the link between each port on the CB's Ethernet switch and one of the following devices:  
- FPC0 (Flexible PIC Concentrator 0) through FPC7  
- Local controller  
- Routing Engine  
- Other Routing Engine (on a system with two Routing Engines)  
- SPMB (Switch Processor Mezzanine Board)  
- (TX Matrix router only) LCC0 (line-card chassis 0) through LCC3 |
| Link is good on Fast Ethernet port n connected to device | or  
| Link is good on Gigabit Ethernet port n connected to device | or  
| Link is down on Gigabit Ethernet port connected to device | or  
| Speed is                               | Speed at which the Ethernet link is running: 10 Mb or 100 Mb. When the device is RE or Other RE on the TX Matrix router, the speed is 1000 Mb.  
**NOTE:** Irrespective of the device, the speed is 1000 Mb on the MX2010 and MX2020 routers. |
| Duplex is                              | Duplex type of the Ethernet link: full or half. |
| Autonegotiate is Enabled (or Disabled) | By default, built-in Fast Ethernet ports on a PIC autonegotiate whether to operate at 10 Mbps or 100 Mbps. All other interfaces automatically choose the correct speed based on the PIC type and whether the PIC is configured to operate in multiplexed mode (using the no-concatenate statement at the [edit chassis] hierarchy level, as described in the Junos OS System Basics Configuration Guide). |
| Flow Control TX is Enabled (or Disabled) | (MX2010 routers, MX2020 routers, and PTX Series) Flow control in the transmit direction is enabled (or disabled). Flow control regulates the flow of packets from the switch to the remote side of the connection. |
| Flow Control RX is Enabled (or Disabled) | (MX2010 routers, MX2020 routers, and PTX Series) Flow control in the receive direction is enabled (or disabled). Flow control regulates the flow of packets from the remote side of the connection to the switch. |
| MLT3                                   | Number of multilevel threshold-3 (MLT-3) Fast Ethernet errors detected. |
| Accumulated error counts for port n connected to device FPCn: (error output only) |  
- Lock                                    | Number of lock errors detected.  
- Xmit                                     | Number of transmission errors detected.  
- ESD                                      | Number of electrostatic discharge (ESD) errors detected.  
- False Carrier                           | Number of false carrier errors detected. |
Table 143: show chassis ethernet-switch Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnects</td>
<td>Number of disconnect errors detected.</td>
</tr>
<tr>
<td>FX mode</td>
<td>Number of errors detected on an Ethernet link over optical fiber.</td>
</tr>
<tr>
<td>Statistics for port n connected to device FPCn (statistics output only)</td>
<td></td>
</tr>
<tr>
<td>TX Packets 64 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 64 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 65 - 127 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 65 through 127 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 128 - 255 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 128 through 255 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 256 - 511 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 256 through 511 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 512 - 1023 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 512 through 1023 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 1024 - 1518 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 1024 through 1518 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 1519 - 2047 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 1519 through 2047 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 2048 - 4095 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 2048 through 4095 octets transmitted.</td>
</tr>
<tr>
<td>TX Packets 4096 - 9216 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 4096 through 9216 octets transmitted.</td>
</tr>
<tr>
<td>TX 1519 - 1522 Good Vlan frms</td>
<td>(MX2010 and MX2020 routers) Number of transmitted frames of size 1519 through 1522 octets that are good VLAN frames.</td>
</tr>
<tr>
<td>TX Octets</td>
<td>Number of octets sent.</td>
</tr>
<tr>
<td>TX Unicast packets</td>
<td>Number of unicast packets sent.</td>
</tr>
<tr>
<td>TX Multicast packets</td>
<td>Number of multicast packets sent.</td>
</tr>
<tr>
<td>TX Broadcast packets</td>
<td>Number of broadcast packets sent.</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>(MX2010 and MX2020 routers) Number of packets sent after one collision.</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>(MX2010 and MX2020 routers) Number of packets sent after multiple collisions.</td>
</tr>
</tbody>
</table>
### Table 143: show chassis ethernet-switch Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Late collisions</td>
<td>Number of packets aborted during sending because of collisions after 64 bytes.</td>
</tr>
<tr>
<td>TX Excessive collisions</td>
<td>Number of packets not sent because of too many collisions.</td>
</tr>
<tr>
<td>TX Dropped packets</td>
<td>Number of transmitted packets that were dropped.</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>Number of Media Access Control (MAC) frames containing PAUSE commands that were sent.</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>Number of oversize packets that were sent.</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>Number of packets discarded because of frame check sequence errors.</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>Number of fragmented packets sent.</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>Number of bytes sent.</td>
</tr>
<tr>
<td>TX Packet OK Counter</td>
<td>Number of viable packets sent.</td>
</tr>
<tr>
<td>TX Pause Packet Counter</td>
<td>Number of PAUSE packets sent.</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 64 octets received.</td>
</tr>
<tr>
<td>RX Packets 65 - 127 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 65 through 127 octets received.</td>
</tr>
<tr>
<td>RX Packets 128 - 255 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 128 through 255 octets received.</td>
</tr>
<tr>
<td>RX Packets 256 - 511 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 256 through 511 octets received.</td>
</tr>
<tr>
<td>RX Packets 512 - 1023 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 512 through 1023 octets received.</td>
</tr>
<tr>
<td>RX Packets 1024 - 1518 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 1024 through 1518 octets received.</td>
</tr>
<tr>
<td>RX Packets 1519 - 2047 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 1519 through 2047 octets received.</td>
</tr>
<tr>
<td>RX Packets 2048 - 4095 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 2048 through 4095 octets received.</td>
</tr>
<tr>
<td>RX Packets 4096 - 9216 Octets</td>
<td>(MX2010 and MX2020 routers) Number of packets of size 4096 through 9216 octets received.</td>
</tr>
</tbody>
</table>
### Table 143: show chassis ethernet-switch Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Octets</td>
<td>Number of octets received.</td>
</tr>
<tr>
<td>RX Unicast packets</td>
<td>Number of unicast packets received.</td>
</tr>
<tr>
<td>RX Multicast packets</td>
<td>Number of multicast packets received.</td>
</tr>
<tr>
<td>RX Broadcast packets</td>
<td>Number of broadcast packets received.</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>Number of packets discarded because of frame check sequence errors.</td>
</tr>
<tr>
<td>RX Alignment Errors</td>
<td>Number of incomplete octets received.</td>
</tr>
<tr>
<td>RX Dropped Packets</td>
<td>Number of incoming packets that were dropped.</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>Number of fragmented packets received.</td>
</tr>
<tr>
<td>RX Symbol Errors</td>
<td>Number of symbols received that the router did not correctly decode.</td>
</tr>
<tr>
<td>RX MAC Control</td>
<td>Number of Media Access Control (MAC) packets received.</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>Number of oversize packets received.</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>Number of undersize packets received.</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>Total number of frames received that exceed the maximum byte count and contain CRC errors.</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>Number of control frames received.</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>Number of pause frames received.</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>Number of packets discarded because of frame check sequence errors.</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>Number of fragmented packets received.</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>Number of bytes received.</td>
</tr>
<tr>
<td>RX Packet OK Counter</td>
<td>Number of viable packets received.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show chassis ethernet-switch
user@host> show chassis ethernet-switch
Link is good on port 0 connected to device: FPC0
  Speed is 100 MB
  Duplex is full
```
Link is good on port 1 connected to device: FPC1
  Speed is 100 MB
  Duplex is full

Link is good on port 2 connected to device: FPC2
  Speed is 100 MB
  Duplex is full

Link is good on port 3 connected to device: FPC3
  Speed is 100 MB
  Duplex is full

Link is good on port 7 connected to device: Local controller
  Speed is 100 MB
  Duplex is full

Link is good on port 9 connected to device: SPMB
  Speed is 100 MB
  Duplex is full

Link is good on port 13 connected to device: FPC5
  Speed is 100 MB
  Duplex is full

show chassis ethernet-switch (MX480 Router with MPC4E)

user@host > show chassis ethernet-switch
Displaying summary for switch 0
Link is down on GE port 0 connected to device: FPC0

Link is down on GE port 1 connected to device: FPC1

Link is good on GE port 2 connected to device: FPC2
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 3 connected to device: FPC3
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 4 connected to device: FPC4
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on GE port 5 connected to device: FPC5

Link is down on GE port 6 connected to device: FPC6

Link is down on GE port 7 connected to device: FPC7
Link is down on GE port 8 connected to device: FPC8

Link is down on GE port 9 connected to device: FPC9

Link is down on GE port 10 connected to device: FPC10

Link is down on GE port 11 connected to device: FPC11

Link is good on GE port 12 connected to device: Other RE
   Speed is 1000Mb
   Duplex is full
   Autonegotiate is Enabled
   Flow Control TX is Disabled
   Flow Control RX is Disabled

Link is good on GE port 13 connected to device: RE-GigE
   Speed is 1000Mb
   Duplex is full
   Autonegotiate is Enabled
   Flow Control TX is Disabled
   Flow Control RX is Disabled

Link is down on GE port 14 connected to device: Debug-GigE

show chassis ethernet-switch (MX2010 Router)

user@host > show chassis ethernet-switch
Displaying summary for switch 0
Link is good on GE port 0 connected to device: FPC0
   Speed is 1000Mb
   Duplex is full
   Autonegotiate is Enabled
   Flow Control TX is Disabled
   Flow Control RX is Disabled

Link is good on GE port 1 connected to device: FPC1
   Speed is 1000Mb
   Duplex is full
   Autonegotiate is Enabled
   Flow Control TX is Disabled
   Flow Control RX is Disabled

Link is good on GE port 2 connected to device: FPC3
   Speed is 1000Mb
   Duplex is full
   Autonegotiate is Enabled
   Flow Control TX is Disabled
   Flow Control RX is Disabled

Link is good on GE port 3 connected to device: FPC2
   Speed is 1000Mb
   Duplex is full
   Autonegotiate is Enabled
   Flow Control TX is Disabled
   Flow Control RX is Disabled

Link is good on GE port 4 connected to device: FPC5
   Speed is 1000Mb
   Duplex is full
   Autonegotiate is Enabled
   Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 5 connected to device: FPC4
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 6 connected to device: FPC6
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 7 connected to device: FPC7
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 8 connected to device: FPC8
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 9 connected to device: FPC9
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 20 connected to device: Other RE-GigE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 21 connected to device: RE-GigE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on GE port 22 connected to device: Debug-GigE

Link is good on GE port 23 connected to device: SPMB
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on XE port 24 connected to device: SFP+ 0
Link is down on XE port 25 connected to device: SFP+ 1

Link is down on XE port 26 connected to device: RE-10GigE

Link is down on XE port 27 connected to device: Other RE-10GigE

show chassis ethernet-switch statistics (MX2010 Router)

user@host > show chassis ethernet-switch statistics
Displaying port statistics for switch 0
Statistics for port 0 connected to device FPC0:
  TX Packets 64 Octets 5088623
  TX Packets 65-127 Octets 2637257
  TX Packets 128-255 Octets 84829
  TX Packets 256-511 Octets 120193
  TX Packets 512-1023 Octets 252371
  TX Packets 1024-1518 Octets 7189736
  TX Packets 1519-2047 Octets 0
  TX Packets 2048-4095 Octets 0
  TX Packets 4096-9216 Octets 0
  TX Packets 1519-1522 Good Vlan frms 0
  TX Octets 15373009
  TX Multicast Packets 14
  TX Broadcast Packets 1679654
  TX Single Collision frames 0
  TX Mult. Collision frames 0
  TX Late Collisions 0
  TX Excessive Collisions 0
  TX Collision frames 0
  TX PAUSEMAC Ctrl Frames 0
  TX MAC ctrl frames 0
  TX Frame deferred Xms 0
  TX Frame excessive deferl 0
  TX Oversize Packets 0
  TX Jabbers 0
  TX FCS Error Counter 0
  TX Fragment Counter 0
  TX Byte Counter 3041239292
RX Packets 64 Octets 874260
RX Packets 65-127 Octets 26066124
RX Packets 128-255 Octets 1386532
RX Packets 256-511 Octets 150539
RX Packets 512-1023 Octets 4636799
RX Packets 1024-1518 Octets 92601
RX Packets 1519-2047 Octets 0
RX Packets 2048-4095 Octets 0
RX Packets 4096-9216 Octets 0
RX Octets 33206855
RX Multicast Packets 0
RX Broadcast Packets 279416
RX FCS Errors 0
RX Align Errors 0
RX Fragments 0
RX Symbol errors 0
RX Unsupported opcodes 0
RX Out of Range Length 0
RX False Carrier Errors 0
RX Undersize Packets 0
RX Oversize Packets 0
RX Jabbers 0
Statistics for port 1 connected to device FPC1:

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Packets 64 Octets</td>
<td>5109146</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>2779473</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>2441286</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>173102</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>1547504</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>7190581</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>19241092</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>14</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>1673369</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xmns</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>4213380187</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>865914</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>26612151</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>1090153</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>25126</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>101158</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>78092</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>28772594</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>285669</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>2327283837</td>
</tr>
</tbody>
</table>
Link is down on GE port 2 connected to device: FPC3
Link is down on GE port 3 connected to device: FPC2
Link is down on GE port 4 connected to device: FPC5
Link is down on GE port 5 connected to device: FPC4
Link is down on GE port 6 connected to device: FPC6
Link is down on GE port 7 connected to device: FPC7

Statistics for port 8 connected to device FPC8:
- TX Packets 64 Octets: 5341094
- TX Packets 65-127 Octets: 2623310
- TX Packets 128-255 Octets: 3315158
- TX Packets 256-511 Octets: 174805
- TX Packets 512-1023 Octets: 976908
- TX Packets 1024-1518 Octets: 7181498
- TX Packets 1519-2047 Octets: 0
- TX Packets 2048-4095 Octets: 0
- TX Packets 4096-9216 Octets: 0
- TX Packets 1024-1518 Good Vlan frms: 0
- TX Octets: 19614773
- TX Multicast Packets: 14
- TX Broadcast Packets: 1673831
- TX Single Collision frames: 0
- TX Mult. Collision frames: 0
- TX Late Collisions: 0
- TX Excessive Collisions: 0
- TX Collision frames: 0
- TX PAUSEMAC Ctrl Frames: 0
- TX MAC ctrl frames: 0
- TX Frame deferred Xmns: 0
- TX Frame excessive deferl: 0
- TX Oversize Packets: 0
- TX Jabbers: 0
- TX FCS Error Counter: 0
- TX Fragment Counter: 0
- TX Byte Counter: 3946762991
- RX Packets 64 Octets: 955509
- RX Packets 65-127 Octets: 27568588
- RX Packets 128-255 Octets: 1460936
- RX Packets 256-511 Octets: 153248
- RX Packets 512-1023 Octets: 2856206
- RX Packets 1024-1518 Octets: 76419
- RX Packets 1519-2047 Octets: 0
- RX Packets 2048-4095 Octets: 0
- RX Packets 4096-9216 Octets: 0
- RX Octets: 33070906
- RX Multicast Packets: 0
- RX Broadcast Packets: 285183
- RX FCS Errors: 0
- RX Align Errors: 0
- RX Fragments: 0
- RX Symbol errors: 0
- RX Unsupported opcodes: 0
- RX Out of Range Length: 0
- RX False Carrier Errors: 0
- RX Undersize Packets: 0
- RX Oversize Packets: 0
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>4256093824</td>
</tr>
</tbody>
</table>

Statistics for port 9 connected to device FPC9:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets 64 Octets</td>
<td>5237213</td>
</tr>
<tr>
<td>TX Packets 65-127 Octets</td>
<td>3268775</td>
</tr>
<tr>
<td>TX Packets 128-255 Octets</td>
<td>2320476</td>
</tr>
<tr>
<td>TX Packets 256-511 Octets</td>
<td>1789844</td>
</tr>
<tr>
<td>TX Packets 512-1023 Octets</td>
<td>501022</td>
</tr>
<tr>
<td>TX Packets 1024-1518 Octets</td>
<td>7800455</td>
</tr>
<tr>
<td>TX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>20917785</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>14</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>1673368</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xmns</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>747012161</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>1036527</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>27590367</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>1590059</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>328257</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>75975</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>73556</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>30694741</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>285586</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>Statistics for port 20 connected to device Other RE-GigE:</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>TX Packets 64 Octets</td>
<td>1682540</td>
</tr>
<tr>
<td>TX Packets 65-127 Octets</td>
<td>3454</td>
</tr>
<tr>
<td>TX Packets 128-255 Octets</td>
<td>659</td>
</tr>
<tr>
<td>TX Packets 256-511 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 512-1023 Octets</td>
<td>1</td>
</tr>
<tr>
<td>TX Packets 1024-1518 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>1686654</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>6</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>1673798</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xmns</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>108042476</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>710214</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>35785510</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>4616</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>232</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>565</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>28798</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>36529935</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>8</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>285546</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>2676440958</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Statistics for port 21 connected to device RE-GigE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets 64 Octets</td>
</tr>
<tr>
<td>TX Packets 65-127 Octets</td>
</tr>
<tr>
<td>TX Packets 128-255 Octets</td>
</tr>
<tr>
<td>TX Packets 256-511 Octets</td>
</tr>
<tr>
<td>TX Packets 512-1023 Octets</td>
</tr>
<tr>
<td>TX Packets 1024-1518 Octets</td>
</tr>
<tr>
<td>TX Packets 1519-2047 Octets</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
</tr>
<tr>
<td>TX Packets 1519-1522 Good Vlan frms</td>
</tr>
<tr>
<td>TX Octets</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
</tr>
<tr>
<td>TX Late Collisions</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
</tr>
<tr>
<td>TX Collision frames</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
</tr>
<tr>
<td>TX Frame deferred Xms</td>
</tr>
<tr>
<td>TX Frame excessive deferral</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
</tr>
<tr>
<td>TX Jabbers</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
</tr>
<tr>
<td>TX Byte Counter</td>
</tr>
</tbody>
</table>

| RX Packets 64 Octets | 14537137 |
| RX Packets 65-127 Octets | 11445505 |
| RX Packets 128-255 Octets | 8161767  |
| RX Packets 256-511 Octets | 2257944  |
| RX Packets 512-1023 Octets | 3277807 |
| RX Packets 1024-1518 Octets | 29373209 |
| RX Packets 1519-2047 Octets | 0       |
| RX Packets 2048-4095 Octets | 0       |
| RX Packets 4096-9216 Octets | 0       |
| RX Octets | 69053369 |
| RX Multicast Packets | 6       |
| RX Broadcast Packets | 285935  |
| RX FCS Errors | 0       |
| RX Align Errors | 0       |
| RX Fragments | 0       |
| RX Symbol errors | 0       |
| RX Unsupported opcodes | 0       |
| RX Out of Range Length | 0       |
| RX False Carrier Errors | 0       |
| RX Undersize Packets | 0       |
| RX Oversize Packets | 0       |
| RX Jabbers | 0       |
| RX 1519-1522 Good Vlan frms | 0 |
| RX MTU Exceed Counter | 0       |
| RX Control Frame Counter | 0       |
| RX Pause Frame Counter | 0       |
| RX Byte Counter | 2980410755 |

Link is down on GE port 22 connected to device: Debug-GigE
Statistics for port 23 connected to device SPMB:
<p>| TX Packets 64 Octets | 1885878 |
| TX Packets 65-127 Octets | 138845  |
| TX Packets 128-255 Octets | 18      |
| TX Packets 256-511 Octets | 1       |
| TX Packets 512-1023 Octets | 2       |
| TX Packets 1024-1518 Octets | 16391   |</p>
<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>2041135</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>14</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>1707267</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xmns</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>148066476</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>374994</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>183398</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>749</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>13658</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>13421</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>9</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>586229</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>252034</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>51431942</td>
</tr>
</tbody>
</table>

**Link is down on XE port 24 connected to device: SFP**

**Link is down on XE port 25 connected to device: SFP**

**Link is down on XE port 26 connected to device: RE-10GigE**

**Link is down on XE port 27 connected to device: Other RE-10GigE**

`show chassis ethernet-switch (MX2020 Router)`

```
user@host > show chassis ethernet-switch
```
Displaying summary for switch 0
Link is good on GE port 0 connected to device: FPC0
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 1 connected to device: FPC1
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 2 connected to device: FPC3
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 3 connected to device: FPC2
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 4 connected to device: FPC5
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 5 connected to device: FPC4
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 6 connected to device: FPC6
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 7 connected to device: FPC7
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 8 connected to device: FPC8
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 9 connected to device: FPC9
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 10 connected to device: FPC10
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 11 connected to device: FPC11
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 12 connected to device: FPC13
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 13 connected to device: FPC12
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 14 connected to device: FPC14
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 15 connected to device: FPC15
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 16 connected to device: FPC17
Speed is 1000Mb
Duplex is full
Autonegotiate is Enabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on GE port 17 connected to device: FPC16
Speed is 1000Mb
show chassis ethernet-switch statistics

TX Packets 64 Octets        1468564
TX Packets 65-127 Octets    153896
TX Packets 128-255 Octets   237
TX Packets 256-511 Octets   286
TX Packets 512-1023 Octets  599
TX Packets 1024-1518 Octets 22803

Link is good on GE port 18 connected to device: FPC18
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 19 connected to device: FPC19
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 20 connected to device: Other RE-GigE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 21 connected to device: RE-GigE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on GE port 22 connected to device: Debug-GigE

Link is good on GE port 23 connected to device: SPMB
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on XE port 24 connected to device: SFP+ 0

Link is down on XE port 25 connected to device: SFP+ 1

Link is down on XE port 26 connected to device: RE-10GigE

Link is down on XE port 27 connected to device: Other RE-10GigE

show chassis ethernet-switch statistics (MX2020 Router)
TX Packets 1519-2047 Octets  0
TX Packets 2048-4095 Octets  0
TX Packets 4096-9216 Octets  0
TX 1519-1522 Good Vlan frms  0
TX Octets  1646385
TX Multicast Packets  6
TX Broadcast Packets  970939
TX Single Collision frames  0
TX Mult. Collision frames  0
TX Late Collisions  0
TX Excessive Collisions  0
TX Collision frames  0
TX PAUSEMAC Ctrl Frames  0
TX MAC ctrl frames  0
TX Frame deferred Xmns  0
TX Frame excessive deferl  0
TX Oversize Packets  0
TX Jabbers  0
TX FCS Error Counter  0
TX Fragment Counter  0
TX Byte Counter  130470290
RX Packets 64 Octets  180266
RX Packets 65-127 Octets  519030
RX Packets 128-255 Octets  1390
RX Packets 256-511 Octets  42857
RX Packets 512-1023 Octets  3482
RX Packets 1024-1518 Octets  8147
RX Packets 1519-2047 Octets  0
RX Packets 2048-4095 Octets  0
RX Packets 4096-9216 Octets  0
RX Octets  755172
RX Multicast Packets  0
RX Broadcast Packets  42822
RX FCS Errors  0
RX Align Errors  0
RX Fragments  0
RX Symbol errors  0
RX Unsupported opcodes  0
RX Out of Range Length  0
RX False Carrier Errors  0
RX Undersize Packets  0
RX Oversize Packets  0
RX Jabbers  0
RX 1519-1522 Good Vlan frms  0
RX MTU Exceed Counter  0
RX Control Frame Counter  0
RX Pause Frame Counter  0
RX Byte Counter  75374021
Statistics for port 1 connected to device FPC1:
TX Packets 64 Octets  1493739
TX Packets 65-127 Octets  126996
TX Packets 128-255 Octets  241
TX Packets 256-511 Octets  283
TX Packets 512-1023 Octets  604
TX Packets 1024-1518 Octets  33687
TX Packets 1519-2047 Octets  0
TX Packets 2048-4095 Octets  0
TX Packets 4096-9216 Octets  0
TX 1519-1522 Good Vlan frms  0
TX Octets  1655550
TX Multicast Packets  6
<table>
<thead>
<tr>
<th>TX Broadcast Packets</th>
<th>969032</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xmns</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>141832690</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>155655</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>545561</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>1394</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>42811</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>3514</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>8171</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets</td>
<td>757106</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>44509</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>44509</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>75691392</td>
</tr>
</tbody>
</table>

Statistics for port 2 connected to device FPC3:
<p>| TX Packets 64 Octets | 1465749 |
| TX Packets 65-127 Octets | 152849 |
| TX Packets 128-255 Octets | 238 |
| TX Packets 256-511 Octets | 289 |
| TX Packets 512-1023 Octets | 602 |
| TX Packets 1024-1518 Octets | 38903 |
| TX Packets 1519-2047 Octets | 0 |
| TX Packets 2048-4095 Octets | 0 |
| TX Packets 4096-9216 Octets | 0 |
| TX Packets | 1658630 |
| TX Multicast Packets | 6 |
| TX Broadcast Packets | 968873 |
| TX Single Collision frames | 0 |
| TX Mult. Collision frames | 0 |
| TX Late Collisions | 0 |
| TX Excessive Collisions | 0 |
| TX Collision frames | 0 |</p>
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xms</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferral</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>147427010</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>181636</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>517526</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>1405</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>42806</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>3515</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>8168</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>753056</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>44490</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>75381869</td>
</tr>
</tbody>
</table>

Statistics for port 3 connected to device FPC2:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets 64 Octets</td>
<td>1473828</td>
</tr>
<tr>
<td>TX Packets 65-127 Octets</td>
<td>145643</td>
</tr>
<tr>
<td>TX Packets 128-255 Octets</td>
<td>253</td>
</tr>
<tr>
<td>TX Packets 256-511 Octets</td>
<td>285</td>
</tr>
<tr>
<td>TX Packets 512-1023 Octets</td>
<td>612</td>
</tr>
<tr>
<td>TX Packets 1024-1518 Octets</td>
<td>26603</td>
</tr>
<tr>
<td>TX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>1647224</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>6</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>968925</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xms</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferral</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>Metric</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>134293832</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>174230</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>525756</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>1404</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>42815</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>3530</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>8176</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>755911</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>44499</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>75517355</td>
</tr>
<tr>
<td>Statistics for port 4 connected to device FPC5:</td>
<td></td>
</tr>
<tr>
<td>TX Packets 64 Octets</td>
<td>1466664</td>
</tr>
<tr>
<td>TX Packets 65-127 Octets</td>
<td>151155</td>
</tr>
<tr>
<td>TX Packets 128-255 Octets</td>
<td>238</td>
</tr>
<tr>
<td>TX Packets 256-511 Octets</td>
<td>277</td>
</tr>
<tr>
<td>TX Packets 512-1023 Octets</td>
<td>615</td>
</tr>
<tr>
<td>TX Packets 1024-1518 Octets</td>
<td>54674</td>
</tr>
<tr>
<td>TX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>1673623</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>6</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>968610</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xms</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>164247790</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>180006</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>518217</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>1406</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>42787</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>3515</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>8164</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>754095</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>44457</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>75311970</td>
</tr>
</tbody>
</table>

Statistics for port 5 connected to device FPC4:

<table>
<thead>
<tr>
<th>TX Packets 64 Octets</th>
<th>1464770</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packets 65-127 Octets</td>
<td>154498</td>
</tr>
<tr>
<td>TX Packets 128-255 Octets</td>
<td>225</td>
</tr>
<tr>
<td>TX Packets 256-511 Octets</td>
<td>280</td>
</tr>
<tr>
<td>TX Packets 512-1023 Octets</td>
<td>637</td>
</tr>
<tr>
<td>TX Packets 1024-1518 Octets</td>
<td>26355</td>
</tr>
<tr>
<td>TX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>1646765</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>6</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>968730</td>
</tr>
<tr>
<td>TX Single Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xmns</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>134058606</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RX Packets 64 Octets</th>
<th>169269</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>515285</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>1527</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>42804</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>3521</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>9142</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Value</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>RX Oktets</td>
<td>741548</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>44470</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>75498393</td>
</tr>
</tbody>
</table>

Statistics for port 6 connected to device FPC6:

| TX Packets 64 Oktets | 1475260 |
| TX Packets 65-127 Oktets | 143324  |
| TX Packets 128-255 Oktets | 260    |
| TX Packets 256-511 Oktets | 274    |
| TX Packets 512-1023 Oktets | 603    |
| TX Packets 1024-1518 Oktets | 40631  |
| TX Packets 1519-2047 Oktets | 0     |
| TX Packets 2048-4095 Oktets | 0     |
| TX Packets 4096-9216 Oktets | 0     |
| TX 1519-1522 Good Vlan frms | 0   |
| TX Oktets          | 1660352 |
| TX Multicast Packets | 6     |
| TX Broadcast Packets | 968466 |
| TX Single Collision frames | 0   |
| TX Mult. Collision frames | 0    |
| TX Late Collisions | 0     |
| TX Excessive Collisions | 0   |
| TX Collision frames | 0     |
| TX PAUSEMAC Ctrl Frames | 0   |
| TX MAC ctrl frames | 0     |
| TX Frame deferred Xmns | 0   |
| TX Frame excessive deferl | 0   |
| TX Oversize Packets | 0     |
| TX Jabbers        | 0     |
| TX FCS Error Counter | 0    |
| TX Fragment Counter | 0    |
| TX Byte Counter   | 149212764 |

| RX Packets 64 Oktets | 172275  |
| RX Packets 65-127 Oktets | 526519  |
| RX Packets 128-255 Oktets | 1394   |
| RX Packets 256-511 Oktets | 42777  |
| RX Packets 512-1023 Oktets | 3514   |
| RX Packets 1024-1518 Oktets | 8161   |
| RX Packets 1519-2047 Oktets | 0     |
| RX Packets 2048-4095 Oktets | 0     |
| RX Packets 4096-9216 Oktets | 0     |
| RX Oktets          | 754640  |
| RX Multicast Packets | 0     |
| RX Broadcast Packets | 44443  |
| RX FCS Errors      | 0      |
| RX Align Errors    | 0      |
| RX Fragments       | 0      |
Statistics for port 7 connected to device FPC7:

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>75386517</td>
</tr>
</tbody>
</table>

TX Packets 64 Octets: 1472361
TX Packets 65-127 Octets: 145646
TX Packets 128-255 Octets: 251
TX Packets 256-511 Octets: 250
TX Packets 512-1023 Octets: 580
TX Packets 1024-1518 Octets: 49530
TX Packets 1519-2047 Octets: 0
TX Packets 2048-4095 Octets: 0
TX Packets 4096-9216 Octets: 0
TX 1519-1522 Good Vlan frms: 0
TX Octets: 1668618
TX Multicast Packets: 6
TX Broadcast Packets: 968317
TX Single Collision frames: 0
TX Multi. Collision frames: 0
TX Late Collisions: 0
TX Excessive Collisions: 0
TX Collision frames: 0
TX PAUSEMAC Ctrl Frames: 0
TX MAC ctrl frames: 0
TX Frame deferred Xmns: 0
TX Frame excessive deferl: 0
TX Oversize Packets: 0
TX Jabbers: 0
TX FCS Error Counter: 0
TX Fragment Counter: 0
TX Byte Counter: 158689814
RX Packets 64 Octets: 174618
RX Packets 65-127 Octets: 523421
RX Packets 128-255 Octets: 1393
RX Packets 256-511 Octets: 42764
RX Packets 512-1023 Octets: 3514
RX Packets 1024-1518 Octets: 8158
RX Packets 1519-2047 Octets: 0
RX Packets 2048-4095 Octets: 0
RX Packets 4096-9216 Octets: 0
RX Octets: 753868
RX Multicast Packets: 0
RX Broadcast Packets: 44429
RX FCS Errors: 0
RX Align Errors: 0
RX Fragments: 0
RX Symbol errors: 0
RX Unsupported opcodes: 0
RX Out of Range Length: 0
RX False Carrier Errors: 0
RX Undersize Packets: 0
RX Oversize Packets: 0
RX Jabbers                  0
RX 1519-1522 Good Vlan frms 0
RX MTU Exceed Counter       0
RX Control Frame Counter    0
RX Pause Frame Counter      0
RX Byte Counter             75309863
Statistics for port 8 connected to device FPC8:

show chassis ethernet-switch (MX2020 Router with MPC4E)

user@ host > show chassis ethernet-switch
Displaying summary for switch 0
Link is good on GE port 0 connected to device: FPC0
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on GE port 1 connected to device: FPC1
Link is down on GE port 2 connected to device: FPC3
Link is down on GE port 3 connected to device: FPC2
Link is down on GE port 4 connected to device: FPC5
Link is down on GE port 5 connected to device: FPC4
Link is down on GE port 6 connected to device: FPC6
Link is down on GE port 7 connected to device: FPC7
Link is down on GE port 8 connected to device: FPC8
Link is good on GE port 9 connected to device: FPC9
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 10 connected to device: FPC10
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on GE port 11 connected to device: FPC11
Link is down on GE port 12 connected to device: FPC13
Link is down on GE port 13 connected to device: FPC12
Link is good on GE port 14 connected to device: FPC14
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
Flow Control RX is Disabled

Link is down on GE port 15 connected to device: FPC15

Link is down on GE port 16 connected to device: FPC17

Link is down on GE port 17 connected to device: FPC16

Link is down on GE port 18 connected to device: FPC18

Link is good on GE port 19 connected to device: FPC19
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 20 connected to device: Other RE-GigE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on GE port 21 connected to device: RE-GigE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on GE port 22 connected to device: Debug-GigE

Link is good on GE port 23 connected to device: SPMB
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is down on XE port 24 connected to device: SFP+ 0

Link is down on XE port 25 connected to device: SFP+ 1

Link is down on XE port 26 connected to device: RE-10GigE

Link is down on XE port 27 connected to device: Other RE-10GigE

show chassis ethernet-switch (TX Matrix Router)

user@host> show chassis ethernet-switch
scc-re0:

Link is good on FE port 4 connected to device: LCC0
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 6 connected to device: LCC2
  Speed is 100 MB
  Duplex is full
Autonegotiate is Enabled

Link is good on FE port 8 connected to device: SPMB
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

lcc0-re0:

Link is good on FE port 1 connected to device: FPC1
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 2 connected to device: FPC2
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 8 connected to device: SPMB
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 10 connected to device: SCC
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

lcc2-re0:

Link is good on FE port 0 connected to device: FPC0
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 1 connected to device: FPC1
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 2 connected to device: FPC2
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 8 connected to device: SPMB
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

Link is good on FE port 10 connected to device: SCC
  Speed is 100 MB
  Duplex is full
  Autonegotiate is Enabled

show chassis ethernet-switch errors

user@host> show chassis ethernet-switch errors
Accumulated error counts for port 0 connected to device FPC0:
  MLT3           2
Lock 0
Xmit 0
ESD 0
False carrier 2
Disconnects 0
FX mode 0

Accumulated error counts for port 1 connected to device FPC1:
MLT3 2
Lock 0
Xmit 0
ESD 0
False carrier 2
Disconnects 0
FX mode 0

Accumulated error counts for port 2 connected to device FPC2:
MLT3 2
Lock 0
Xmit 0
ESD 0
False carrier 3
Disconnects 0
FX mode 0

Accumulated error counts for port 3 connected to device FPC3:
MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0

Accumulated error counts for port 4 connected to device Nothing:
MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0
FX mode 0

...
TX Multicast packets        0
TX Broadcast packets        20080
TX Late collisions          0
TX Excessive collisions     0
TX Dropped packets          0

RX Unicast packets          66037
RX Multicast packets        0
RX Broadcast packets        20080
RX FCS Errors               0
RX Alignment Errors         0
RX Dropped Packets          0
RX Fragments                0
RX Symbol Errors            0

Statistics for port 2 connected to device FPC2:
TX Unicast packets          64206
TX Multicast packets        0
TX Broadcast packets        21183
TX Late collisions          0
TX Excessive collisions     0
TX Dropped packets          0

RX Unicast packets          63671
RX Multicast packets        0
RX Broadcast packets        21183
RX FCS Errors               0
RX Alignment Errors         0
RX Dropped Packets          0
RX Fragments                0
RX Symbol Errors            0

Statistics for port 3 connected to device FPC3:

show chassis ethernet-switch errors (TX Matrix Plus Router)

user@host> show chassis ethernet-switch errors
sfc0-re0:

Displaying error for switch 0

Displaying error for switch 1
Accumulated error counts for port 0 connected to device LCC0:
MLT3        0
Lock        0
Xmit        0
ESD         0
False carrier 0
Disconnects 0
FX mode     0

lcc0-re0:

Displaying error for switch 0

Accumulated error counts for port 6 connected to device FPC0:
MLT3        0
Lock        0
Xmit        0
ESD         0
False carrier 0
Disconnects 0


Accumulated error counts for port 7 connected to device FPC1:

MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 7
Disconnects 0
FX mode 0

Accumulated error counts for port 19 connected to device Other RE:

MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0
FX mode 0

Accumulated error counts for port 20 connected to device SFC0:

MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0
FX mode 0

show chassis ethernet-switch sfc errors (TX Matrix Plus Router)

user@host> show chassis ethernet-switch errors switch sfc

sfc0-re0:

Displaying error for switch 1

Accumulated error counts for port 0 connected to device LCC0:

MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0
FX mode 0

Accumulated error counts for port 2 connected to device LCC1:

MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0
FX mode 0

Accumulated error counts for port 4 connected to device LCC2:

MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0
FX mode 0

Accumulated error counts for port 6 connected to device LCC3:

MLT3 0
Lock 0
Xmit 0
ESD 0
False carrier 0
Disconnects 0
FX mode 0

lcc0-re0:
--------------------------------------------------------------------------
error: command is not valid on the t1600

lcc1-re0:
--------------------------------------------------------------------------
error: command is not valid on the t1600

lcc2-re0:
--------------------------------------------------------------------------
error: command is not valid on the t1600

lcc3-re0:
--------------------------------------------------------------------------
error: command is not valid on the t1600

show chassis ethernet-switch statistics (TX Matrix Plus Router)

user@host> show chassis ethernet-switch statistics
sfc0-re0:
--------------------------------------------------------------------------
Displaying port statistics for switch 0
Statistics for port 1 connected to device IGSW:
  TX Packets 64 Octets  5183577
  TX Packets 65-127 Octets  67820
  TX Packets 128-255 Octets  772
  TX Packets 256-511 Octets  136
  TX Packets 512-1023 Octets  68
  TX Packets 1024-1518 Octets  10881
  TX Packets 1519-2047 Octets  0
  TX Packets 2048-4095 Octets  0
  TX Packets 4096-9216 Octets  0
  TX Packets 9217-16383 Octets  0
  TX Octets  5263254
  TX Multicast Packets  16
  TX Broadcast Packets  723403
  TX PAUSEMAC Ctrl Frames  0
  TX Oversize Packets  0
  TX FCS Error Counter  0
  TX Fragment Counter  0
  TX Byte Counter  349922253
  TX Packet OK Counter  5263254
  TX Pause Packet Counter  0
  TX Unicast Counter  4539835
  RX Packets 64 Octets  6513629
  RX Packets 65-127 Octets  88761
  RX Packets 128-255 Octets  6382
  RX Packets 256-511 Octets  22027
  RX Packets 512-1023 Octets  4319
  RX Packets 1024-1518 Octets  49922
  RX Packets 1519-2047 Octets  0
  RX Packets 2048-4095 Octets  0
  RX Packets 4096-9216 Octets  0
  RX Packets 9217-16383 Octets  0
  RX Octets  6685040
  RX Multicast Packets  4
  RX Broadcast Packets  2137376
<table>
<thead>
<tr>
<th>Metric</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX MAC Control Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>509224602</td>
</tr>
<tr>
<td>RX Unicast Frame Count</td>
<td>4547660</td>
</tr>
<tr>
<td>RX Packet OK Count</td>
<td>6685040</td>
</tr>
<tr>
<td>Statistics for port 9 connected to device RE1:</td>
<td></td>
</tr>
<tr>
<td>TX Packets 64 Octets</td>
<td>2500318</td>
</tr>
<tr>
<td>TX Packets 65-127 Octets</td>
<td>443</td>
</tr>
<tr>
<td>TX Packets 128-255 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 256-511 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 512-1023 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 1024-1518 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Packets 9217-16383 Octets</td>
<td>0</td>
</tr>
<tr>
<td>TX Octets</td>
<td>2500761</td>
</tr>
<tr>
<td>TX Multicast Packets</td>
<td>4</td>
</tr>
<tr>
<td>TX Broadcast Packets</td>
<td>2500757</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>160049670</td>
</tr>
<tr>
<td>TX Packet OK Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Pause Packet Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Unicast Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>701191</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>5882</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>2</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>17965</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>7</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 9217-16383 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>725047</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>8</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>2500757</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX MAC Control Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>62402656</td>
</tr>
<tr>
<td>RX Unicast Frame Count</td>
<td>0</td>
</tr>
<tr>
<td>RX Packet OK Count</td>
<td>0</td>
</tr>
<tr>
<td>Statistics for port 17 connected to device RE0:</td>
<td></td>
</tr>
<tr>
<td>TX Packets 64 Octets</td>
<td>7214818</td>
</tr>
</tbody>
</table>
TX Packets 65-127 Octets    94640
TX Packets 128-255 Octets   6384
TX Packets 256-511 Octets   22027
TX Packets 512-1023 Octets  22284
TX Packets 1024-1518 Octets  49929
TX Packets 1519-2047 Octets  0
TX Packets 2048-4095 Octets  0
TX Packets 4096-9216 Octets  0
TX Packets 9217-16383 Octets  0
TX Octets                   7410082
TX Multicast Packets       12
TX Broadcast Packets       2497247
TX PAUSEMAC Ctrl Frames    0
TX Oversize Packets        0
TX FCS Error Counter       0
TX Fragment Counter        0
TX Byte Counter            571626932
TX Packet OK Counter       0
TX Pause Packet Counter    0
TX Unicast Counter         0
RX Packets 64 Octets       4823701
RX Packets 65-127 Octets   67812
RX Packets 128-255 Octets  772
RX Packets 256-511 Octets  136
RX Packets 512-1023 Octets 68
RX Packets 1024-1518 Octets 10881
RX Packets 1519-2047 Octets 0
RX Packets 2048-4095 Octets 0
RX Packets 4096-9216 Octets 0
RX Packets 9217-16383 Octets 0
RX Octets                   4903370
RX Multicast Packets       8
RX Broadcast Packets       2497247
RX FCS Errors              0
RX Fragments               0
RX MAC Control Packets     0
RX Out of Range Length     0
RX Undersize Packets       0
RX Oversize Packets        0
RX Jabbers                 0
RX Control Frame Counter   0
RX Pause Frame Counter     0
RX Byte Counter            326889517
RX Unicast Frame Count     0
RX Packet OK Count         0

Displaying port statistics for switch 1
Statistics for port 0 connected to device LCC0:
TX Packets 64 Octets       5053443
TX Packets 65-127 Octets   59737
TX Packets 128-255 Octets  768
TX Packets 256-511 Octets  87
TX Packets 512-1023 Octets 68
TX Packets 1024-1518 Octets 85
TX Packets 1519-2047 Octets 0
TX Packets 2048-4095 Octets 0
TX Packets 4096-9216 Octets 0
TX Packets 9217-16383 Octets 0
TX Octets                   5114188
TX Multicast Packets       16
TX Broadcast Packets       1125742
<table>
<thead>
<tr>
<th>TX Single Collision frames</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Mult. Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Late Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Excessive Collisions</td>
<td>0</td>
</tr>
<tr>
<td>TX Collision frames</td>
<td>0</td>
</tr>
<tr>
<td>TX PAUSEMAC Ctrl Frames</td>
<td>0</td>
</tr>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xms</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>329291449</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>5640175</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>79875</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>6338</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>165</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>4317</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>10</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>5730880</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>4</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>1735007</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>371282850</td>
</tr>
</tbody>
</table>

Statistics for port 18 connected to device SPMB:
<p>| TX Packets 64 Octets | 2990326 |
| TX Packets 65-127 Octets | 8572 |
| TX Packets 128-255 Octets | 4 |
| TX Packets 256-511 Octets | 49 |
| TX Packets 512-1023 Octets | 0 |
| TX Packets 1024-1518 Octets | 10793 |
| TX Packets 1519-2047 Octets | 0 |
| TX Packets 2048-4095 Octets | 0 |
| TX Packets 4096-9216 Octets | 0 |
| TX 1519-1522 Good Vlan frms | 0 |
| TX Octets | 3009744 |
| TX Multicast Packets | 20 |
| TX Broadcast Packets | 2458322 |
| TX Single Collision frames | 0 |
| TX Mult. Collision frames | 0 |
| TX Late Collisions | 0 |
| TX Excessive Collisions | 0 |
| TX Collision frames | 0 |
| TX PAUSEMAC Ctrl Frames | 0 |</p>
<table>
<thead>
<tr>
<th>Statistic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX MAC ctrl frames</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame deferred Xmns</td>
<td>0</td>
</tr>
<tr>
<td>TX Frame excessive deferl</td>
<td>0</td>
</tr>
<tr>
<td>TX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>TX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>TX FCS Error Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Fragment Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Byte Counter</td>
<td>203712524</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>873454</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>8886</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>44</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>21862</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>2</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>49912</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>954160</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>402369</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Align Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX Symbol errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Unsupported opcodes</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX False Carrier Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX 1519-1522 Good Vlan frms</td>
<td>0</td>
</tr>
<tr>
<td>RX MTU Exceed Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>137941752</td>
</tr>
</tbody>
</table>

show chassis ethernet-switch (T4000 Router)

```
user@host> show chassis ethernet-switch
Displaying summary for switch 0
Link is good on GE port 6 connected to device: FPC0
  Speed is 100Mb
  Duplex is full
  Autonegotiate is Enabled
  False carrier sense count = 04

Link is good on GE port 9 connected to device: FPC3
  Speed is 100Mb
  Duplex is full
  Autonegotiate is Enabled
  False carrier sense count = 03

Link is good on GE port 11 connected to device: FPC5
  Speed is 100Mb
  Duplex is full
  Autonegotiate is Enabled
  False carrier sense count = 03

Link is good on GE port 12 connected to device: FPC6
  Speed is 100Mb
```
Duplex is full
Autonegotiate is Enabled
False carrier sense count = 03

Link is good on GE port 14 connected to device: SPMB
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled

Link is good on GE port 18 connected to device: RE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled

Link is good on GE port 19 connected to device: Other RE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Enabled

show chassis ethernet-switch errors (T4000 Router)

user@host> show chassis ethernet-switch errors

Displaying error for switch 0
Accumulated error counts for port 6 connected to device FPC0:
  MLT3  0
  Lock  0
  Xmit  0
  ESD   0
  False carrier 4
  Disconnects 0
  FX mode 0
Accumulated error counts for port 9 connected to device FPC3:
  MLT3  0
  Lock  0
  Xmit  0
  ESD   0
  False carrier 3
  Disconnects 0
  FX mode 0
Accumulated error counts for port 11 connected to device FPC5:
  MLT3  0
  Lock  0
  Xmit  0
  ESD   0
  False carrier 3
  Disconnects 0
  FX mode 0
Accumulated error counts for port 12 connected to device FPC6:
  MLT3  0
  Lock  0
  Xmit  0
  ESD   0
  False carrier 3
  Disconnects 0
  FX mode 0
Accumulated error counts for port 19 connected to device Other RE:
  MLT3  0
  Lock  0
  Xmit  0
  ESD   0
False carrier 0
Disconnects 0
FX mode 0

show chassis ethernet-switch (PTX5000 Packet Transport Router)

user@host> show chassis ethernet-switch
Displaying summary for switch 0
Link is good on XE port 2 connected to device: SPMB
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on XE port 11 connected to device: FPC7
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on XE port 12 connected to device: FPC6
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on XE port 13 connected to device: FPC5
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on XE port 15 connected to device: FPC3
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on XE port 16 connected to device: FPC2
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on XE port 18 connected to device: FPC0
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
  Flow Control TX is Disabled
  Flow Control RX is Disabled

Link is good on XE port 19 connected to device: OTHER RE
  Speed is 1000Mb
  Duplex is full
  Autonegotiate is Disabled
Flow Control TX is Disabled
Flow Control RX is Disabled

Link is good on XE port 20 connected to device: RE
Speed is 1000Mb
Duplex is full
Autonegotiate is Disabled
Flow Control TX is Disabled
Flow Control RX is Disabled

show chassis ethernet-switch statistics (PTX5000 Packet Transport Router)

user@host> show chassis ethernet-switch statistics
Displaying port statistics for switch 0
Statistics for port 2 connected to device SPMB:
TX Packets 64 Octets 10942
TX Packets 65-127 Octets 843
TX Packets 128-255 Octets 2
TX Packets 256-511 Octets 2
TX Packets 512-1023 Octets 0
TX Packets 1024-1518 Octets 6862
TX Packets 1519-2047 Octets 0
TX Packets 2048-4095 Octets 0
TX Packets 4096-9216 Octets 0
TX Packets 9217-16383 Octets 0
TX Octets 18651
TX Multicast Packets 6
TX Broadcast Packets 10331
TX PAUSEMAC Ctrl Frames 0
TX Oversize Packets 0
TX FCS Error Counter 0
TX Fragment Counter 0
TX Byte Counter 8105166
TX Packet OK Counter 0
TX Pause Packet Counter 0
TX Unicast Counter 0
RX Packets 64 Octets 8679
RX Packets 65-127 Octets 2364
RX Packets 128-255 Octets 531
RX Packets 256-511 Octets 112
RX Packets 512-1023 Octets 26
RX Packets 1024-1518 Octets 8
RX Packets 1519-2047 Octets 0
RX Packets 2048-4095 Octets 0
RX Packets 4096-9216 Octets 0
RX Packets 9217-16383 Octets 0
RX Octets 11720
RX Multicast Packets 0
RX Broadcast Packets 10331
RX FCS Errors 0
RX Fragments 0
RX MAC Control Packets 0
RX Out of Range Length 0
RX Undersize Packets 0
RX Oversize Packets 0
RX Jabbers 0
RX Control Frame Counter 0
RX Pause Frame Counter 0
RX Byte Counter 938105
RX Unicast Frame Count 0
RX Packet OK Count 0
Statistics for port 11 connected to device FPC7:
  TX Packets 64 Octets 14492
  TX Packets 65-127 Octets 3542
  TX Packets 128-255 Octets 6
  TX Packets 256-511 Octets 45
  TX Packets 512-1023 Octets 60

Continued...

Statistics for port 18 connected to device FPC0:
  TX Packets 64 Octets 15212
  TX Packets 65-127 Octets 3810
  TX Packets 128-255 Octets 6
  TX Packets 256-511 Octets 43
  TX Packets 512-1023 Octets 66
  TX Packets 1024-1518 Octets 169
  TX Packets 1519-2047 Octets 0
  TX Packets 2048-4095 Octets 0
  TX Packets 4096-9216 Octets 0
  TX Packets 9217-16383 Octets 0
  TX Octets 19306
  TX Multicast Packets 0
  TX Broadcast Packets 10886
  TX PAUSEMAC Ctrl Frames 0
  TX Oversize Packets 0
  TX FCS Error Counter 0
  TX Fragment Counter 0
  TX Byte Counter 1569412
  TX Packet OK Counter 0
  TX Pause Packet Counter 0
  TX Unicast Counter 0
  RX Packets 64 Octets 17994
  RX Packets 65-127 Octets 8006
  RX Packets 128-255 Octets 230
  RX Packets 256-511 Octets 19
  RX Packets 512-1023 Octets 53
  RX Packets 1024-1518 Octets 11
  RX Packets 1519-2047 Octets 0
  RX Packets 2048-4095 Octets 0
  RX Packets 4096-9216 Octets 0
  RX Packets 9217-16383 Octets 0
  RX Octets 26313
  RX Multicast Packets 0
  RX Broadcast Packets 10886
  RX FCS Errors 0
  RX Fragments 0
  RX MAC Control Packets 0
  RX Out of Range Length 0
  RX Undersize Packets 0
  RX Oversize Packets 0
  RX Jabbers 0
  RX Control Frame Counter 2
  RX Pause Frame Counter 2
  RX Byte Counter 1836287
  RX Unicast Frame Count 0
  RX Packet OK Count 0

Statistics for port 19 connected to device OTHER RE:
  TX Packets 64 Octets 10234
  TX Packets 65-127 Octets 162
  TX Packets 128-255 Octets 0
  TX Packets 256-511 Octets 0
| TX Packets 512-1023 Octets | 0 |
| TX Packets 1024-1518 Octets | 0 |
| TX Packets 1519-2047 Octets | 0 |
| TX Packets 2048-4095 Octets | 0 |
| TX Packets 4096-9216 Octets | 0 |
| TX Packets 9217-16383 Octets | 0 |
| TX Octets | 10396 |
| TX Multicast Packets | 8 |
| TX Broadcast Packets | 10317 |
| TX PAUSEMAC Ctrl Frames | 0 |
| TX Oversize Packets | 0 |
| TX FCS Error Counter | 0 |
| TX Fragment Counter | 0 |
| TX Byte Counter | 666260 |
| TX Packet OK Counter | 0 |
| TX Pause Packet Counter | 0 |
| TX Unicast Counter | 0 |
| RX Packets 64 Octets | 4073 |
| RX Packets 65-127 Octets | 325 |
| RX Packets 128-255 Octets | 1 |
| RX Packets 256-511 Octets | 0 |
| RX Packets 512-1023 Octets | 0 |
| RX Packets 1024-1518 Octets | 72 |
| RX Packets 1519-2047 Octets | 0 |
| RX Packets 2048-4095 Octets | 0 |
| RX Packets 4096-9216 Octets | 0 |
| RX Packets 9217-16383 Octets | 0 |
| RX Octets | 4471 |
| RX Multicast Packets | 0 |
| RX Broadcast Packets | 10317 |
| RX FCS Errors | 0 |
| RX Fragments | 0 |
| RX MAC Control Packets | 0 |
| RX Out of Range Length | 0 |
| RX Undersize Packets | 0 |
| RX Oversize Packets | 0 |
| RX Jabbers | 0 |
| RX Control Frame Counter | 0 |
| RX Pause Frame Counter | 0 |
| RX Byte Counter | 387333 |
| RX Unicast Frame Count | 0 |
| RX Packet OK Count | 0 |

Statistics for port 20 connected to device RE:

<p>| TX Packets 64 Octets | 658856 |
| TX Packets 65-127 Octets | 45535 |
| TX Packets 128-255 Octets | 1900 |
| TX Packets 256-511 Octets | 532 |
| TX Packets 512-1023 Octets | 372 |
| TX Packets 1024-1518 Octets | 191 |
| TX Packets 1519-2047 Octets | 0 |
| TX Packets 2048-4095 Octets | 0 |
| TX Packets 4096-9216 Octets | 0 |
| TX Packets 9217-16383 Octets | 0 |
| TX Octets | 707386 |
| TX Multicast Packets | 0 |
| TX Broadcast Packets | 10421 |
| TX PAUSEMAC Ctrl Frames | 0 |
| TX Oversize Packets | 0 |
| TX FCS Error Counter | 0 |
| TX Fragment Counter | 0 |
| TX Byte Counter | 46608676 |</p>
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX Packet OK Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Pause Packet Counter</td>
<td>0</td>
</tr>
<tr>
<td>TX Unicast Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 64 Octets</td>
<td>27394</td>
</tr>
<tr>
<td>RX Packets 65-127 Octets</td>
<td>20271</td>
</tr>
<tr>
<td>RX Packets 128-255 Octets</td>
<td>78</td>
</tr>
<tr>
<td>RX Packets 256-511 Octets</td>
<td>215</td>
</tr>
<tr>
<td>RX Packets 512-1023 Octets</td>
<td>269</td>
</tr>
<tr>
<td>RX Packets 1024-1518 Octets</td>
<td>253370</td>
</tr>
<tr>
<td>RX Packets 1519-2047 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 2048-4095 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 4096-9216 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Packets 9217-16383 Octets</td>
<td>0</td>
</tr>
<tr>
<td>RX Octets</td>
<td>301597</td>
</tr>
<tr>
<td>RX Multicast Packets</td>
<td>8</td>
</tr>
<tr>
<td>RX Broadcast Packets</td>
<td>10421</td>
</tr>
<tr>
<td>RX FCS Errors</td>
<td>0</td>
</tr>
<tr>
<td>RX Fragments</td>
<td>0</td>
</tr>
<tr>
<td>RX MAC Control Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Out of Range Length</td>
<td>0</td>
</tr>
<tr>
<td>RX Undersize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Oversize Packets</td>
<td>0</td>
</tr>
<tr>
<td>RX Jabbers</td>
<td>0</td>
</tr>
<tr>
<td>RX Control Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Pause Frame Counter</td>
<td>0</td>
</tr>
<tr>
<td>RX Byte Counter</td>
<td>275043436</td>
</tr>
<tr>
<td>RX Unicast Frame Count</td>
<td>0</td>
</tr>
<tr>
<td>RX Packet OK Count</td>
<td>0</td>
</tr>
</tbody>
</table>

Continued ...

show chassis ethernet-switch port-state (PTX5000 Packet Transport Router)

user@host> show chassis ethernet-switch port-state
Displaying port state for switch 0
Port : 02
Target : SPMB

Error reading port 2 connected to device: SPMB
**show chassis fabric fpcs**

**Syntax**

```
show chassis fabric fpcs
<lcc number>
```

**Syntax (MX Series Routers)**

```
show chassis fabric fpcs
<all-members>
<local>
<member member-id>
```

**Syntax (MX2010 and MX2020 3D Universal Edge Routers)**

```
show chassis fabric fpcs
```

**Syntax (T4000 Core Router)**

```
show chassis fabric fpcs
```

**Syntax (PTX Series Packet Transport Routers)**

```
show chassis fabric fpcs <slot fpc-slot>
```

**Syntax (TX Matrix Plus Router)**

```
show chassis fabric fpcs
<lcc number>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.4 for EX Series switches.
Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

**Description**

(M320, MX Series, and T Series routers, EX8200 switches, and PTX Series Packet Transport Routers only) Display the state of the electrical switch fabric links between the Flexible PIC Concentrators (FPCs) and the Switch Interface Boards (SIBs).

**Options**

- **none**—Display the switch fabric link state. On a TX Matrix router, display the switching fabric link states for the FPCs in all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display the switching fabric link states for the FPCs in all routers connected to the TX Matrix Plus router.

- **all-members**—(MX Series routers only) (Optional) Display the switching fabric link states for the FPCs in all members of the Virtual Chassis configuration.

- **lcc number**—(TX Matrix router and TX Matrix Plus router only) (Optional) On a TX Matrix router, display the switch fabric link state for the FPCs in the specified T640 router (line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, display the switch fabric link state for the FPCs in the specified router (line-card chassis) that is connected to the TX Matrix Plus router. Replace *number* with a following value depending on the LCC configurations:
• From 0 through 3 on a T640 router on the routing matrix with TX Matrix routers.

• From 0 through 3 on a T1600 router on the routing matrix with TX Matrix Plus routers.

• From 0 through 7 on a T1600 router in a routing matrix with TX Matrix Plus router with 3D SIBs.

• 0, 2, 4, 6 on a T4000 router in a routing matrix with TX Matrix Plus router with 3D SIBs.

**local**—(MX Series routers only) (Optional) Display the switching fabric link states for the FPCs in the local Virtual Chassis member.

**member member-id**—(MX Series routers only) (Optional) Display the switching fabric link states for the FPCs in the specified member of the Virtual Chassis configuration. Replace **member-id** with a value of 0 or 1.

**slot fpc-slot**—(PTX Series Packet Transport Routers only) (Optional) Display the fabric state of the specified FPC slot. If no value is provided, display the status of all FPCs.

**Required Privilege Level**

**view**

**List of Sample Output**

- show chassis fabric fpacs (M320 Router) on page 918
- show chassis fabric fpacs (MX240 Router) on page 919
- show chassis fabric fpacs (MX480 Router) on page 919
- show chassis fabric fpacs (MX960 Router) on page 920
- show chassis fabric fpacs (MX240 with AS MLC Modular Carrier Card) on page 922
- show chassis fabric fpacs (MX480 with AS MLC Modular Carrier Card) on page 922
- show chassis fabric fpacs (MX480 Router with MPC4E) on page 923
- show chassis fabric fpacs (MX960 with AS MLC Modular Carrier Card) on page 924
- show chassis fabric fpacs (MX2010 Router) on page 926
- show chassis fabric fpacs (MX2020 Router) on page 929
- show chassis fabric fpacs (MX2020 Router with MPC4E) on page 932
- show chassis fabric fpacs (T320 Router) on page 933
- show chassis fabric fpacs (T640 Router) on page 934
- show chassis fabric fpacs (TX Matrix Router) on page 934
- show chassis fabric fpacs (TX Matrix Router with 3D SIBs) on page 936
- show chassis fabric fpacs lcc (TX Matrix Router with 3D SIBs) on page 939
- show chassis fabric fpacs (T1600 Router) on page 939
- show chassis fabric fpacs (T4000 Core Router) on page 941
- show chassis fabric fpacs (TX Matrix Plus Router) on page 942
- show chassis fabric fpacs lcc (TX Matrix Plus Router) on page 950
- show chassis fabric fpacs (EX8200 Switch) on page 950
- show chassis fabric fpacs (PTX Series Packet Transport Routers) on page 951

**Output Fields**

Table 144 on page 918 lists the output fields for the **show chassis fabric fpacs** command. Output fields are listed in the approximate order in which they appear.
Table 144: show chassis fabric fpcs Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fabric management FPC state</strong></td>
<td>Switching fabric link (link from SIB to FPC) state for each FPC:</td>
</tr>
<tr>
<td><strong>Unused</strong></td>
<td>FPC is not present.</td>
</tr>
<tr>
<td></td>
<td>(On MX240 and MX480 routers with AS- MLC modular carrier card or MPC4E only) the fabric plane from the pair that share physical links (1 and 5, and 3 and 7) is inactive.</td>
</tr>
<tr>
<td><strong>Destination error on PFEs list of PFEnumbers</strong></td>
<td>Destination errors to the listed Packet Forwarding Engines. Indicates that the link is not carrying traffic to the listed Packet Forwarding Engines.</td>
</tr>
<tr>
<td><strong>Links ok</strong></td>
<td>Link between the spare SIB and FPC is eligible to carry traffic.</td>
</tr>
<tr>
<td><strong>Link error</strong></td>
<td>Link between the SIB and FPC has CRC errors. However, the link is still eligible to carry traffic.</td>
</tr>
<tr>
<td><strong>Plane disabled</strong></td>
<td>Fabric plane has been disabled for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>- Destination errors have exceeded the thresholds.</td>
</tr>
<tr>
<td></td>
<td>- Run-time link errors have exceeded the thresholds.</td>
</tr>
<tr>
<td></td>
<td>- Initialization time link errors detected, and link training was unsuccessful.</td>
</tr>
<tr>
<td><strong>Plane Disabled, Links Error</strong> (PTX Series Packet Transport Routers only)</td>
<td>The plane is disabled because of link errors detected at the FPC RX.</td>
</tr>
<tr>
<td><strong>Plane Disabled, Links Down</strong> (PTX Series Packet Transport Routers only)</td>
<td>The plane is disabled because of link errors detected at the SIB RX.</td>
</tr>
<tr>
<td><strong>Plane enabled</strong></td>
<td>Link between the active SIB and FPC is eligible to carry traffic.</td>
</tr>
</tbody>
</table>

**NOTE:** In Junos OS Release 9.6 and later, the list of Packet Forwarding Engines with destination errors is displayed in the output. In Junos OS Releases before 9.6, the output only indicates that there are destination errors. However, the list of Packet Forwarding Engines with destination errors is not displayed.

- **Links ok**—Link between the spare SIB and FPC is eligible to carry traffic.
- **Link error**—Link between the SIB and FPC has CRC errors. However, the link is still eligible to carry traffic.
- **Plane disabled**—Fabric plane has been disabled for the following reasons:
  - Destination errors have exceeded the thresholds.
  - Run-time link errors have exceeded the thresholds.
  - Initialization time link errors detected, and link training was unsuccessful.
  - **Plane Disabled, Links Error** (PTX Series Packet Transport Routers only)—The plane is disabled because of link errors detected at the FPC RX.
  - **Plane Disabled, Links Down** (PTX Series Packet Transport Routers only)—The plane is disabled because of link errors detected at the SIB RX.
  - **Plane enabled**—Link between the active SIB and FPC is eligible to carry traffic.

**NOTE:** On the Enhanced MX SCB with MPC, a maximum of 4 planes are operational and running. On all the other SCBs with MPC, all the planes are operational and running.

- **Plane Enabled, Links OK** (PTX Series Packet Transport Routers only)—The FPC CCL RX link is eligible to carry traffic.
- **Plane Enabled, Links OK** (TX Matrix and TX Matrix Plus routers only)—The FPC HSL RX link is eligible to carry traffic.

Sample Output

show chassis fabric fpcs (M320 Router)

```
user@host> show chassis fabric fpcs
Fabric management FPC state:
FPC #2
  PFE #1
```
SIB #0
  Plane enabled
SIB #1
  Plane enabled
SIB #2
  Plane enabled
SIB #3
  Plane enabled

show chassis fabric fpscs (MX240 Router)

user@host> show chassis fabric fpscs
Fabric management FPC state:
FPC 2
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Links ok
    Plane 5: Links ok
    Plane 6: Links ok
    Plane 7: Links ok
  PFE #1
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Links ok
    Plane 5: Links ok
    Plane 6: Links ok
    Plane 7: Links ok
  PFE #2
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Links ok
    Plane 5: Links ok
    Plane 6: Links ok
    Plane 7: Links ok
  PFE #3
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Links ok
    Plane 5: Links ok
    Plane 6: Links ok
    Plane 7: Links ok

show chassis fabric fpscs (MX480 Router)

user@host> show chassis fabric fpscs
FPC 0
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
Plane 6: Links ok
Plane 7: Links ok

PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
Plane 6: Links ok
Plane 7: Links ok

PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
Plane 6: Links ok
Plane 7: Links ok

PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
Plane 6: Links ok
Plane 7: Links ok

FPC 1
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

show chassis fabric fpcs (MX960 Router)

user@host> show chassis fabric fpcs
FPC 0
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
FPC 1
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
FPC 2
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
...
show chassis fabric fpscs (MX240 with AS MLC Modular Carrier Card)

In the following output, FPC 1 is the AS MLC modular carrier card (AS MCC).

```
user@host> show chassis fabric fpscs
FPC 1
  PFE #0
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Plane enabled
  Plane 5: Unused
  Plane 6: Plane enabled
  Plane 7: Unused

FPC 2
  PFE #0
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Plane enabled
  Plane 5: Plane enabled
  Plane 6: Plane enabled
  Plane 7: Plane enabled
```

show chassis fabric fpscs (MX480 with AS MLC Modular Carrier Card)

In the following output, FPC 5 is the AS MLC modular carrier card (AS MCC).

```
user@host> show chassis fabric fpscs
FPC 2
  PFE #0
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Plane enabled
  Plane 5: Plane enabled
  Plane 6: Plane enabled
  Plane 7: Plane enabled

FPC 4
  PFE #0
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Links ok
  Plane 5: Links ok
  Plane 6: Links ok
  Plane 7: Links ok
  PFE #2
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Links ok
  Plane 5: Links ok
  Plane 6: Links ok
  Plane 7: Links ok

FPC 5
```
In the following output, **FPC4** is the MPC4E (MPC4E-3D-32XGE-SFPP) card.

```
user@host > show chassis fabric fpcs
Fabric management FPC state:
FPC 0
  PFE #0
    Plane 0: Links ok
    Plane 1: Links ok
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Links ok
    Plane 6: Plane enabled
    Plane 7: Links ok
  PFE #1
    Plane 0: Links ok
    Plane 1: Links ok
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Links ok
    Plane 6: Plane enabled
    Plane 7: Links ok
FPC 1
  PFE #0
    Plane 0: Links ok
    Plane 1: Links ok
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Links ok
    Plane 6: Plane enabled
    Plane 7: Links ok
  PFE #1
    Plane 0: Links ok
    Plane 1: Links ok
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Links ok
    Plane 6: Plane enabled
    Plane 7: Links ok
  PFE #2
    Plane 0: Links ok
    Plane 1: Links ok
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Links ok
```
In the following output, FPC 5 is the AS MLC modular carrier card (AS MCC).

show chassis fabric fpcs

Fabric management FPC state:
FPC 0
PFE #0
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Plane enabled
  Plane 5: Links ok
  Plane 6: Plane enabled
  Plane 7: Links ok

PFE #1
  Plane 0: Plane enabled
  Plane 1: Plane enabled
  Plane 2: Plane enabled
  Plane 3: Plane enabled
  Plane 4: Plane enabled
  Plane 5: Unused
  Plane 6: Plane enabled
  Plane 7: Unused
Plane 5: Links ok

FPC 1
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok

FPC 4
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok

FPC 5
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok

FPC 8
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Links ok
Plane 5: Links ok
show chassis fabric fpcs (MX2010 Router)

user@host> show chassis fabric fpcs
Fabric management FPC state:
FPC 0
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 1
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 2
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 3
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 4
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 5
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 6
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
FPC 7
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 8
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 9
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane disabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

show chassis fabric fpcs (MX2020 Router)

user@host> show chassis fabric fpcs
Fabric management FPC state:
FPC 0
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 1

PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 2

PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 3
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

FPC 4
...

show chassis fabric fpcs (MX2020 Router with MPC4E)

user@host > show chassis fabric fpcs
Fabric management FPC state:
FPC 0
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
  PFE #1
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
FPC 9
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
  PFE #1
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
FPC 10
  PFE #0
    Plane 0: Plane enabled
    Plane 1: Plane enabled
    Plane 2: Plane enabled
    Plane 3: Plane enabled
    Plane 4: Plane enabled
    Plane 5: Plane enabled
    Plane 6: Plane enabled
    Plane 7: Plane enabled
FPC 14
PFE #0
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #1
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #2
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled
PFE #3
Plane 0: Plane enabled
Plane 1: Plane enabled
Plane 2: Plane enabled
Plane 3: Plane enabled
Plane 4: Plane enabled
Plane 5: Plane enabled
Plane 6: Plane enabled
Plane 7: Plane enabled

show chassis fabric fpcs (T320 Router)

  user@host> show chassis fabric fpcs
  FPC #3
  PFE #1
show chassis fabric fpcs (T640 Router)

user@host> show chassis fabric fpcs
Fabric management FPC state:

FPC #2
PFE #1
SIB #0
    Links ok
SIB #1
    Plane enabled
SIB #2
    Plane enabled
FPC #7
PFE #1
SIB #0
    Links ok
SIB #1
    Plane enabled
SIB #2
    Plane enabled
SIB #3
    Plane enabled
SIB #4
    Plane enabled
FPC #3
PFE #1
SIB #2
    Plane enabled
SIB #3
    Link error
Destination error on PFEs 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
SIB #4
    Destination error on PFEs 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21

show chassis fabric fpcs (TX Matrix Router)

user@host> show chassis fabric fpcs
lcc0-re0:
-------------------------------------------------------------------------
Fabric management FPC state:
FPC #0
    PFE #1
SIB #0 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok

FPC #2
PFE #1
SIB #0 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok FPC #3

PFE #1 SIB #2 Plane enabled
SIB #3 Link error

Destination error on PFEs 0 1 2 3 4 5 6 7
8 9 10 11 12 13 14 15 16 17 18 19 20 21

... FPC #4
PFE #0 SIB #4 Links ok
PFE #1 SIB #4 Links ok
FPC #5
PFE #1 SIB #4 Links ok
FPC #6
PFE #1 SIB #4 Links ok

lcc2-re0:
---------------------------------------------------------------------
Fabric management FPC state:
FPC #0 PFE #1 SIB #4 Links ok
FPC #1 PFE #1 SIB #4 Links ok
FPC #2 PFE #0 SIB #4 Links ok PFE #1 SIB #4 Links ok
FPC #4 PFE #0 SIB #4 Links ok PFE #1 SIB #4 Links ok
FPC #5
PFE #1
SIB #4 Links ok

show chassis fabric fpcs (TX Matrix Router with 3D SIBs)

user@host> show chassis fabric fpcs
lcc0-re0:
------------------------------------------------------------------------
Fabric management FPC state:
FPC #0
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  PFE #1
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
FPC #3
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  PFE #1
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
FPC #4
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok

SIB #4
   Links ok

lcc2-re0:
--------------------------------------------------------------------------

lcc4-re0:
--------------------------------------------------------------------------

Fabric management FPC state:
FPC #2
   PFE #0
      SIB #0
         Links ok
      SIB #1
         Links ok
      SIB #2
         Links ok
      SIB #3
         Links ok
      SIB #4
         Links ok
   PFE #1
      SIB #0
         Links ok
      SIB #1
         Links ok
      SIB #2
         Links ok
      SIB #3
         Links ok
      SIB #4
         Links ok

FPC #3
   PFE #0
      SIB #0
         Links ok
      SIB #1
         Links ok
      SIB #2
         Links ok
      SIB #3
         Links ok
      SIB #4
         Links ok
   PFE #1
      SIB #0
         Links ok
      SIB #1
         Links ok
      SIB #2
         Links ok
      SIB #3
         Links ok
      SIB #4
         Links ok

lcc6-re0:
--------------------------------------------------------------------------
show chassis fabric fpcs lcc (TX Matrix Router with 3D SIBs)

user@host> show chassis fabric fpcs lcc 4
lcc4-re0:
------------------------------------------------------------------------------------------------------------------------
Fabric management FPC state:
FPC #2
 PFE #0
   SIB #0
   Links ok
   SIB #1
   Links ok
   SIB #2
   Links ok
   SIB #3
   Links ok
   SIB #4
   Links ok
 PFE #1
   SIB #0
   Links ok
   SIB #1
   Links ok
   SIB #2
   Links ok
   SIB #3
   Links ok
   SIB #4
   Links ok
FPC #3
 PFE #0
   SIB #0
   Links ok
   SIB #1
   Links ok
   SIB #2
   Links ok
   SIB #3
   Links ok
   SIB #4
   Links ok
 PFE #1
   SIB #0
   Links ok
   SIB #1
   Links ok
   SIB #2
   Links ok
   SIB #3
   Links ok
   SIB #4
   Links ok

show chassis fabric fpcs (T1600 Router)

user@host> show chassis fabric fpcs
Fabric management FPC state:
FPC #0
 PFE #0
   SIB #0
   Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled

PFE #1
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled

FPC #1
PFE #0
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled

PFE #1
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled

FPC #2
PFE #0
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
Plane enabled
SIB #3
Plane enabled
SIB #4
Plane enabled

FPC #4
PFE #0
SIB #0
Links ok
SIB #1
Plane enabled
SIB #2
show chassis fabric fpcs (T4000 Core Router)

Fabric management FPC state:
FPC #2
 PFE #0
  SIB #0
  Links ok
  SIB #1
  Plane enabled
  SIB #2
  Plane enabled
  SIB #3
  Plane enabled
  SIB #4
  Plane enabled
FPC #3
 PFE #0
  SIB #0
  Links ok
  SIB #1
  Plane enabled
  SIB #2
  Plane enabled
  SIB #3
  Plane enabled
  SIB #4
  Plane enabled
FPC #5
 PFE #0
  SIB #0
  Links ok
  SIB #1
  Plane enabled

Destination error on PFEs       0    1    2    3    4    5    6    7
     8    9   10   11   12   13   14   15   16   17   18   19   20   21
SIB #4
 Destination error on PFEs       0    1    2    3    4    5    6    7
     8    9   10   11   12   13   14   15   16   17   18   19   20   21
show chassis fabric fpcs (TX Matrix Plus Router)

user@host> show chassis fabric fpcs

-------------------------------------------------------------------------
Fabric management FPC state:
FPC #0
PFE #1
  SIB #0
    Unused
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #2
PFE #0
SIB #0
Unused
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok

PFE #1
SIB #0
Unused
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok

FPC #3
PFE #1
SIB #2
Plane enabled
SIB #3
Link error
  Destination error on PFEs       0    1    2    3    4    5    6    7
  8    9   10   11   12   13   14   15   16   17   18   19   20   21
SIB #4
  Destination error on PFEs       0    1    2    3    4    5    6    7
  8    9   10   11   12   13   14   15   16   17   18   19   20   21

FPC #4
PFE #0
SIB #0
Unused
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok

PFE #1
SIB #0
Unused
SIB #1
Links ok
SIB #2
Links ok
SIB #3
Links ok
SIB #4
Links ok

FPC #6
PFE #0
SIB #0
Unused
SIB #1
Links ok
Fabric management FPC state:

FPC #1
PFE #0
SIB #0
    Unused
    SIB #1
    Links ok
    SIB #2
    Links ok
    SIB #3
    Links ok
    SIB #4
    Links ok

FPC #0
PFE #0
SIB #0
    Links ok
    SIB #1
    Links ok
    SIB #2
    Links ok
    SIB #3
    Links ok
    SIB #4
    Links ok

FPC #4
PFE #0
SIB #0
    Links ok
    SIB #1
    Links ok
lcc2-re0:

Fabric management FPC state:
FPC #0
  PFE #0
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  PFE #1
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  PFE #1
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  PFE #1
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  FPC #6
  PFE #0
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  PFE #1
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  PFE #1
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  FPC #7
  PFE #0
    SIB #0 Links ok
    SIB #1 Links ok
    SIB #2 Links ok
    SIB #3 Links ok
    SIB #4 Links ok

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  FPC #0
  PFE #0

  SIB #0 Links ok
  SIB #1 Links ok
  SIB #2 Links ok
  SIB #3 Links ok
  SIB #4 Links ok

  Destination error on PFEs 1 8 9 29 40 65 72 73 93 104


Copyright © 2013, Juniper Networks, Inc.
Fabric management FPC state:
FPC #0
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #1
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #2
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #3
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #4
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #5
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #6
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
FPC #7
  PFE #0
    SIB #0
      Links ok
    SIB #1
      Links ok
    SIB #2
      Links ok
    SIB #3
      Links ok
    SIB #4
      Links ok
  SIB #0
    Links ok
  SIB #1
    Links ok
  SIB #2
    Links ok
  SIB #3
    Links ok
  SIB #4
    Links ok
SIB #4

Links ok

show chassis fabric fpcs lcc (TX Matrix Plus Router)

user@host> show chassis fabric fpcs lcc 0
lcc0-rel:

Fabric management FPC state:
FPC #3
PFE #1
  SIB #2
    Plane enabled
SIB #3
  Link error
    Destination error on PFEs
      0    1    2    3    4    5    6    7
     8    9   10   11   12   13   14   15   16   17   18   19   20   21
SIB #4
  Destination error on PFEs
      0    1    2    3    4    5    6    7
     8    9   10   11   12   13   14   15   16   17   18   19   20   21
FPC #4
PFE #0
  SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok
PFE #1
  SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok
FPC #6
PFE #0
  SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok
PFE #1
  SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok
FPC #7
PFE #0
  SIB #0 Links ok
SIB #1 Links ok
SIB #2 Links ok
SIB #3 Links ok
SIB #4 Links ok

show chassis fabric fpcs (EX8200 Switch)

user@host> show chassis fabric fpcs

Fabric management FPC state
FPC 6
PFE #0
  Plane 0: Plane enabled
show chassis fabric fpcs (PTX Series Packet Transport Routers)

user@host> show chassis fabric fpcs slot 0
Fabric management FPC state:
FPC #0
PFE #0
SIB0_Fcore0 (plane 0) Plane Enabled, Links OK
SIB0_Fcore1 (plane 1) Plane Enabled, Links OK
SIB1_Fcore0 (plane 2) Plane Disabled, Links Down
SIB1_Fcore1 (plane  3)   Plane Enabled, Links OK
SIB2_Fcore0 (plane  4)   Plane Enabled, Links OK
SIB2_Fcore1 (plane  5)   Plane Enabled, Links OK
SIB3_Fcore0 (plane  6)   Plane Enabled, Links OK
SIB3_Fcore1 (plane  7)   Plane Enabled, Links OK
SIB5_Fcore0 (plane 10)   Plane Enabled, Links OK
SIB5_Fcore1 (plane 11)   Plane Enabled, Links OK
SIB6_Fcore0 (plane 12)   Plane Enabled, Links OK
SIB6_Fcore1 (plane 13)   Plane Enabled, Links OK
SIB7_Fcore0 (plane 14)   Plane Enabled, Links OK
SIB7_Fcore1 (plane 15)   Plane Enabled, Links OK
SIB8_Fcore0 (plane 16)   Plane Enabled, Links OK
SIB8_Fcore1 (plane 17)   Plane Enabled, Links OK
## show chassis fabric map

### Syntax

```
show chassis fabric map
plane <plane-number>
```

### Syntax (MX Series Router)

```
show chassis fabric map
<all-members>
<local>
<member member-id>
<plane plane-number>
```

### Release Information

Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.4 for EX Series switches.

### Description

(M120 and MX Series routers and EX8200 switches only) On the M120 router, display the state of the switching fabric map for connections from the Forwarding Engine Boards (FEBs) to the ports on the fabric planes, as interpreted by the fabric plane. On the MX Series router and the EX8200 switch, display the state of the switching fabric map for connections from each Packet Forwarding Engine on the Dense Port Concentrators (DPCs) to the ports on the fabric planes, as interpreted by the fabric plane. For information about the meaning of “fabric plane”, “DPCs”, and “SIBs” on the switches, see “EX Series Switches Hardware and CLI Terminology Mapping” on page 389.

### Options

- **none**—Display the switching fabric map state for the M120 or MX Series router or EX8200 switch.
- **all-members**—(MX Series routers only) (Optional) Display the switching fabric map state for all the members of the Virtual Chassis configuration.
- **local**—(MX Series routers only) (Optional) Display the switching fabric map state for the local Virtual Chassis member.
- **member member-id**—(MX Series routers only) (Optional) Display the switching fabric map state for the specified member of the Virtual Chassis configuration. Replace the `member-id` with a value of 0 or 1.
- **plane plane-number**—(Optional) Display the state of the fabric link for the specified plane number.
  - For the M120 router, replace `plane-number` with a value from 0 through 3.
  - For the MX480 and MX240 routers, replace `plane-number` with a value from 0 through 7.
  - For the MX960 router, replace `plane-number` with a value from 0 through 5.
  - For the EX8208 switch, replace `plane-number` with a value from 0 through 11.
  - For the EX8216 switch, replace `plane-number` with a value from 0 through 7.

### Required Privilege

- **view**
List of Sample Output

show chassis fabric map (M120 Router) on page 954
show chassis fabric map (MX Series Routers) on page 954
show chassis fabric map plane 1 (EX8200 Switch) on page 958

Output Fields

Table 145 on page 954 lists the output fields for the show chassis fabric map command. Output fields are listed in the approximate order in which they appear.

Table 145: show chassis fabric map Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>in-links</td>
<td>Fabric map for receive side links.</td>
</tr>
<tr>
<td>out-links</td>
<td>Fabric map for transmit side links.</td>
</tr>
<tr>
<td>state</td>
<td>State of the fabric link:</td>
</tr>
<tr>
<td></td>
<td>• RESET—Link between SIB and FPC/DPC is powered down on purpose. This is done in all non-dual PFE based boards.</td>
</tr>
<tr>
<td></td>
<td>• UP—Link between SIB and FPC/DPC is up and running.</td>
</tr>
<tr>
<td></td>
<td>• DOWN—Link between SIB and FPC/DPC is powered down.</td>
</tr>
<tr>
<td></td>
<td>• FAULT—SIB is in alarmed state where the SIB's plane is not operational for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• On-board F-chip is not operational.</td>
</tr>
<tr>
<td></td>
<td>• Fiber optic connector faults.</td>
</tr>
<tr>
<td></td>
<td>• FPC connector faults.</td>
</tr>
<tr>
<td></td>
<td>• SIB midplane connector faults.</td>
</tr>
</tbody>
</table>

Sample Output

show chassis fabric map (M120 Router)

user@host> show chassis fabric map
FEB0->CB0F0_00  up  CB0F0_08->FEB7  Down
FEB1->CB0F0_01  Down  CB0F0_09->FEB6  Down
FEB6->CB0F0_02  Down  CB0F0_10->FEB1  Down
FEB2->CB0F0_03  Down  CB0F0_11->FEB0  up
FEB3->CB0F0_04  Down  CB0F0_12->FEB3  Down
FEB4->CB0F0_05  up  CB0F0_13->FEB2  Down
FEB7->CB0F0_06  Down  CB0F0_14->FEB5  Down
FEB5->CB0F0_07  Down  CB0F0_15->FEB4  up:

show chassis fabric map (MX Series Routers)

user@host> show chassis fabric map
DPC4PFE0->CB0F0_00_0  up  CB0F0_00_0->DPC4PFE0  up
DPC4PFE1->CB0F0_00_1  up  CB0F0_00_1->DPC4PFE1  up
DPC4PFE2->CB0F0_00_2  up  CB0F0_00_2->DPC4PFE2  up
DPC4PFE3->CB0F0_00_3  up  CB0F0_00_3->DPC4PFE3  up
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Down/Up Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPC7PFE0-&gt;CB0F0_01_0</td>
<td>Down</td>
<td>CB0F0_01_0-&gt;DPC7PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE1-&gt;CB0F0_01_1</td>
<td>Down</td>
<td>CB0F0_01_1-&gt;DPC7PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE2-&gt;CB0F0_01_2</td>
<td>Down</td>
<td>CB0F0_01_2-&gt;DPC7PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE3-&gt;CB0F0_01_3</td>
<td>Down</td>
<td>CB0F0_01_3-&gt;DPC7PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE0-&gt;CB0F0_03_0</td>
<td>Down</td>
<td>CB0F0_03_0-&gt;DPC3PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE1-&gt;CB0F0_03_1</td>
<td>Down</td>
<td>CB0F0_03_1-&gt;DPC3PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE2-&gt;CB0F0_03_2</td>
<td>Down</td>
<td>CB0F0_03_2-&gt;DPC3PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE3-&gt;CB0F0_03_3</td>
<td>Down</td>
<td>CB0F0_03_3-&gt;DPC3PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE0-&gt;CB0F0_05_0</td>
<td>Down</td>
<td>CB0F0_05_0-&gt;DPC8PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE1-&gt;CB0F0_05_1</td>
<td>Down</td>
<td>CB0F0_05_1-&gt;DPC8PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE2-&gt;CB0F0_05_2</td>
<td>Down</td>
<td>CB0F0_05_2-&gt;DPC8PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE3-&gt;CB0F0_05_3</td>
<td>Down</td>
<td>CB0F0_05_3-&gt;DPC8PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE0-&gt;CB0F0_06_0</td>
<td>Down</td>
<td>CB0F0_06_0-&gt;DPC1PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE1-&gt;CB0F0_06_1</td>
<td>Down</td>
<td>CB0F0_06_1-&gt;DPC1PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE2-&gt;CB0F0_06_2</td>
<td>Down</td>
<td>CB0F0_06_2-&gt;DPC1PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE3-&gt;CB0F0_06_3</td>
<td>Down</td>
<td>CB0F0_06_3-&gt;DPC1PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE0-&gt;CB0F0_07_0</td>
<td>Down</td>
<td>CB0F0_07_0-&gt;DPC10PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE1-&gt;CB0F0_07_1</td>
<td>Down</td>
<td>CB0F0_07_1-&gt;DPC10PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE2-&gt;CB0F0_07_2</td>
<td>Down</td>
<td>CB0F0_07_2-&gt;DPC10PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE3-&gt;CB0F0_07_3</td>
<td>Down</td>
<td>CB0F0_07_3-&gt;DPC10PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE0-&gt;CB0F0_08_0</td>
<td>Down</td>
<td>CB0F0_08_0-&gt;DPC11PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE1-&gt;CB0F0_08_1</td>
<td>Down</td>
<td>CB0F0_08_1-&gt;DPC11PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE2-&gt;CB0F0_08_2</td>
<td>Down</td>
<td>CB0F0_08_2-&gt;DPC11PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE3-&gt;CB0F0_08_3</td>
<td>Down</td>
<td>CB0F0_08_3-&gt;DPC11PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE0-&gt;CB0F0_09_0</td>
<td>Down</td>
<td>CB0F0_09_0-&gt;DPC0PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE1-&gt;CB0F0_09_1</td>
<td>Down</td>
<td>CB0F0_09_1-&gt;DPC0PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE2-&gt;CB0F0_09_2</td>
<td>Down</td>
<td>CB0F0_09_2-&gt;DPC0PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE3-&gt;CB0F0_09_3</td>
<td>Down</td>
<td>CB0F0_09_3-&gt;DPC0PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE0-&gt;CB0F0_11_0</td>
<td>Down</td>
<td>CB0F0_11_0-&gt;DPC9PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE1-&gt;CB0F0_11_1</td>
<td>Down</td>
<td>CB0F0_11_1-&gt;DPC9PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE2-&gt;CB0F0_11_2</td>
<td>Down</td>
<td>CB0F0_11_2-&gt;DPC9PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE3-&gt;CB0F0_11_3</td>
<td>Down</td>
<td>CB0F0_11_3-&gt;DPC9PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC2PFE0-&gt;CB0F0_13_0</td>
<td>Up</td>
<td>CB0F0_13_0-&gt;DPC2PFE0</td>
<td>Up</td>
</tr>
<tr>
<td>DPC2PFE1-&gt;CB0F0_13_1</td>
<td>Up</td>
<td>CB0F0_13_1-&gt;DPC2PFE1</td>
<td>Up</td>
</tr>
<tr>
<td>DPC2PFE2-&gt;CB0F0_13_2</td>
<td>Up</td>
<td>CB0F0_13_2-&gt;DPC2PFE2</td>
<td>Up</td>
</tr>
<tr>
<td>DPC2PFE3-&gt;CB0F0_13_3</td>
<td>Up</td>
<td>CB0F0_13_3-&gt;DPC2PFE3</td>
<td>Up</td>
</tr>
<tr>
<td>DPC6PFE0-&gt;CB0F0_14_0</td>
<td>Down</td>
<td>CB0F0_14_0-&gt;DPC6PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE1-&gt;CB0F0_14_1</td>
<td>Down</td>
<td>CB0F0_14_1-&gt;DPC6PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE2-&gt;CB0F0_14_2</td>
<td>Down</td>
<td>CB0F0_14_2-&gt;DPC6PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE3-&gt;CB0F0_14_3</td>
<td>Down</td>
<td>CB0F0_14_3-&gt;DPC6PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE0-&gt;CB0F0_15_0</td>
<td>Down</td>
<td>CB0F0_15_0-&gt;DPC5PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE1-&gt;CB0F0_15_1</td>
<td>Down</td>
<td>CB0F0_15_1-&gt;DPC5PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE2-&gt;CB0F0_15_2</td>
<td>Down</td>
<td>CB0F0_15_2-&gt;DPC5PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE3-&gt;CB0F0_15_3</td>
<td>Down</td>
<td>CB0F0_15_3-&gt;DPC5PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC4PFE0-&gt;CB0F1_00_0</td>
<td>Up</td>
<td>CB0F1_00_0-&gt;DPC4PFE0</td>
<td>Up</td>
</tr>
<tr>
<td>DPC4PFE1-&gt;CB0F1_00_1</td>
<td>Up</td>
<td>CB0F1_00_1-&gt;DPC4PFE1</td>
<td>Up</td>
</tr>
<tr>
<td>DPC4PFE2-&gt;CB0F1_00_2</td>
<td>Up</td>
<td>CB0F1_00_2-&gt;DPC4PFE2</td>
<td>Up</td>
</tr>
<tr>
<td>DPC4PFE3-&gt;CB0F1_00_3</td>
<td>Up</td>
<td>CB0F1_00_3-&gt;DPC4PFE3</td>
<td>Up</td>
</tr>
<tr>
<td>DPC7PFE0-&gt;CB0F1_01_0</td>
<td>Down</td>
<td>CB0F1_01_0-&gt;DPC7PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE1-&gt;CB0F1_01_1</td>
<td>Down</td>
<td>CB0F1_01_1-&gt;DPC7PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE2-&gt;CB0F1_01_2</td>
<td>Down</td>
<td>CB0F1_01_2-&gt;DPC7PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE3-&gt;CB0F1_01_3</td>
<td>Down</td>
<td>CB0F1_01_3-&gt;DPC7PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE0-&gt;CB0F1_03_0</td>
<td>Down</td>
<td>CB0F1_03_0-&gt;DPC3PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE1-&gt;CB0F1_03_1</td>
<td>Down</td>
<td>CB0F1_03_1-&gt;DPC3PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE2-&gt;CB0F1_03_2</td>
<td>Down</td>
<td>CB0F1_03_2-&gt;DPC3PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE3-&gt;CB0F1_03_3</td>
<td>Down</td>
<td>CB0F1_03_3-&gt;DPC3PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE0-&gt;CB0F1_05_0</td>
<td>Down</td>
<td>CB0F1_05_0-&gt;DPC8PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE1-&gt;CB0F1_05_1</td>
<td>Down</td>
<td>CB0F1_05_1-&gt;DPC8PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE2-&gt;CB0F1_05_2</td>
<td>Down</td>
<td>CB0F1_05_2-&gt;DPC8PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE3-&gt;CB0F1_05_3</td>
<td>Down</td>
<td>CB0F1_05_3-&gt;DPC8PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE0-&gt;CB0F1_06_0</td>
<td>Down</td>
<td>CB0F1_06_0-&gt;DPC1PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>Device 1</td>
<td>Device 2</td>
<td>Action</td>
<td>Device 1</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>DPC1PFE1</td>
<td>CB0F1_06_1</td>
<td>Down</td>
<td>CB0F1_06_1</td>
</tr>
<tr>
<td>DPC1PFE2</td>
<td>CB0F1_06_2</td>
<td>Down</td>
<td>CB0F1_06_2</td>
</tr>
<tr>
<td>DPC1PFE3</td>
<td>CB0F1_06_3</td>
<td>Down</td>
<td>CB0F1_06_3</td>
</tr>
<tr>
<td>DPC10PFE0</td>
<td>CB0F1_07_0</td>
<td>Down</td>
<td>CB0F1_07_0</td>
</tr>
<tr>
<td>DPC10PFE1</td>
<td>CB0F1_07_1</td>
<td>Down</td>
<td>CB0F1_07_1</td>
</tr>
<tr>
<td>DPC10PFE2</td>
<td>CB0F1_07_2</td>
<td>Down</td>
<td>CB0F1_07_2</td>
</tr>
<tr>
<td>DPC10PFE3</td>
<td>CB0F1_07_3</td>
<td>Down</td>
<td>CB0F1_07_3</td>
</tr>
<tr>
<td>DPC11PFE0</td>
<td>CB0F1_08_0</td>
<td>Down</td>
<td>CB0F1_08_0</td>
</tr>
<tr>
<td>DPC11PFE1</td>
<td>CB0F1_08_1</td>
<td>Down</td>
<td>CB0F1_08_1</td>
</tr>
<tr>
<td>DPC11PFE2</td>
<td>CB0F1_08_2</td>
<td>Down</td>
<td>CB0F1_08_2</td>
</tr>
<tr>
<td>DPC11PFE3</td>
<td>CB0F1_08_3</td>
<td>Down</td>
<td>CB0F1_08_3</td>
</tr>
<tr>
<td>DPC0PFE0</td>
<td>CB0F1_09_0</td>
<td>Down</td>
<td>CB0F1_09_0</td>
</tr>
<tr>
<td>DPC0PFE1</td>
<td>CB0F1_09_1</td>
<td>Down</td>
<td>CB0F1_09_1</td>
</tr>
<tr>
<td>DPC0PFE2</td>
<td>CB0F1_09_2</td>
<td>Down</td>
<td>CB0F1_09_2</td>
</tr>
<tr>
<td>DPC0PFE3</td>
<td>CB0F1_09_3</td>
<td>Down</td>
<td>CB0F1_09_3</td>
</tr>
<tr>
<td>DPC9PFE0</td>
<td>CB0F1_11_0</td>
<td>Down</td>
<td>CB0F1_11_0</td>
</tr>
<tr>
<td>DPC9PFE1</td>
<td>CB0F1_11_1</td>
<td>Down</td>
<td>CB0F1_11_1</td>
</tr>
<tr>
<td>DPC9PFE2</td>
<td>CB0F1_11_2</td>
<td>Down</td>
<td>CB0F1_11_2</td>
</tr>
<tr>
<td>DPC9PFE3</td>
<td>CB0F1_11_3</td>
<td>Down</td>
<td>CB0F1_11_3</td>
</tr>
<tr>
<td>DPC2PFE0</td>
<td>CB1F0_00_0</td>
<td>Up</td>
<td>CB1F0_00_0</td>
</tr>
<tr>
<td>DPC2PFE1</td>
<td>CB1F0_00_1</td>
<td>Up</td>
<td>CB1F0_00_1</td>
</tr>
<tr>
<td>DPC2PFE2</td>
<td>CB1F0_00_2</td>
<td>Up</td>
<td>CB1F0_00_2</td>
</tr>
<tr>
<td>DPC2PFE3</td>
<td>CB1F0_00_3</td>
<td>Up</td>
<td>CB1F0_00_3</td>
</tr>
<tr>
<td>DPC6PFE0</td>
<td>CB1F0_14_0</td>
<td>Down</td>
<td>CB1F0_14_0</td>
</tr>
<tr>
<td>DPC6PFE1</td>
<td>CB1F0_14_1</td>
<td>Down</td>
<td>CB1F0_14_1</td>
</tr>
<tr>
<td>DPC6PFE2</td>
<td>CB1F0_14_2</td>
<td>Down</td>
<td>CB1F0_14_2</td>
</tr>
<tr>
<td>DPC6PFE3</td>
<td>CB1F0_14_3</td>
<td>Down</td>
<td>CB1F0_14_3</td>
</tr>
<tr>
<td>DPC5PFE0</td>
<td>CB1F0_15_0</td>
<td>Down</td>
<td>CB1F0_15_0</td>
</tr>
<tr>
<td>DPC5PFE1</td>
<td>CB1F0_15_1</td>
<td>Down</td>
<td>CB1F0_15_1</td>
</tr>
<tr>
<td>DPC5PFE2</td>
<td>CB1F0_15_2</td>
<td>Down</td>
<td>CB1F0_15_2</td>
</tr>
<tr>
<td>DPC5PFE3</td>
<td>CB1F0_15_3</td>
<td>Down</td>
<td>CB1F0_15_3</td>
</tr>
<tr>
<td>DPC4PFE0</td>
<td>CB1F0_00_0</td>
<td>Up</td>
<td>CB1F0_00_0</td>
</tr>
<tr>
<td>DPC4PFE1</td>
<td>CB1F0_00_1</td>
<td>Up</td>
<td>CB1F0_00_1</td>
</tr>
<tr>
<td>DPC4PFE2</td>
<td>CB1F0_00_2</td>
<td>Up</td>
<td>CB1F0_00_2</td>
</tr>
<tr>
<td>DPC4PFE3</td>
<td>CB1F0_00_3</td>
<td>Up</td>
<td>CB1F0_00_3</td>
</tr>
<tr>
<td>DPC7PFE0</td>
<td>CB1F0_01_0</td>
<td>Down</td>
<td>CB1F0_01_0</td>
</tr>
<tr>
<td>DPC7PFE1</td>
<td>CB1F0_01_1</td>
<td>Down</td>
<td>CB1F0_01_1</td>
</tr>
<tr>
<td>DPC7PFE2</td>
<td>CB1F0_01_2</td>
<td>Down</td>
<td>CB1F0_01_2</td>
</tr>
<tr>
<td>DPC7PFE3</td>
<td>CB1F0_01_3</td>
<td>Down</td>
<td>CB1F0_01_3</td>
</tr>
<tr>
<td>DPC3PFE0</td>
<td>CB1F0_03_0</td>
<td>Down</td>
<td>CB1F0_03_0</td>
</tr>
<tr>
<td>DPC3PFE1</td>
<td>CB1F0_03_1</td>
<td>Down</td>
<td>CB1F0_03_1</td>
</tr>
<tr>
<td>DPC3PFE2</td>
<td>CB1F0_03_2</td>
<td>Down</td>
<td>CB1F0_03_2</td>
</tr>
<tr>
<td>DPC3PFE3</td>
<td>CB1F0_03_3</td>
<td>Down</td>
<td>CB1F0_03_3</td>
</tr>
<tr>
<td>DPC8PFE0</td>
<td>CB1F0_05_0</td>
<td>Down</td>
<td>CB1F0_05_0</td>
</tr>
<tr>
<td>DPC8PFE1</td>
<td>CB1F0_05_1</td>
<td>Down</td>
<td>CB1F0_05_1</td>
</tr>
<tr>
<td>DPC8PFE2</td>
<td>CB1F0_05_2</td>
<td>Down</td>
<td>CB1F0_05_2</td>
</tr>
<tr>
<td>DPC8PFE3</td>
<td>CB1F0_05_3</td>
<td>Down</td>
<td>CB1F0_05_3</td>
</tr>
<tr>
<td>DPC1PFE0</td>
<td>CB1F0_06_0</td>
<td>Down</td>
<td>CB1F0_06_0</td>
</tr>
<tr>
<td>DPC1PFE1</td>
<td>CB1F0_06_1</td>
<td>Down</td>
<td>CB1F0_06_1</td>
</tr>
<tr>
<td>DPC1PFE2</td>
<td>CB1F0_06_2</td>
<td>Down</td>
<td>CB1F0_06_2</td>
</tr>
<tr>
<td>DPC1PFE3</td>
<td>CB1F0_06_3</td>
<td>Down</td>
<td>CB1F0_06_3</td>
</tr>
<tr>
<td>DPC10PFE0</td>
<td>CB1F0_07_0</td>
<td>Down</td>
<td>CB1F0_07_0</td>
</tr>
<tr>
<td>DPC10PFE1</td>
<td>CB1F0_07_1</td>
<td>Down</td>
<td>CB1F0_07_1</td>
</tr>
<tr>
<td>DPC10PFE2</td>
<td>CB1F0_07_2</td>
<td>Down</td>
<td>CB1F0_07_2</td>
</tr>
<tr>
<td>DPC10PFE3</td>
<td>CB1F0_07_3</td>
<td>Down</td>
<td>CB1F0_07_3</td>
</tr>
<tr>
<td>Device 1</td>
<td>Device 2</td>
<td>Status</td>
<td>Device 1 Action</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>--------</td>
<td>----------------</td>
</tr>
<tr>
<td>DPC0PFE2-&gt;CB1F0_09_2</td>
<td>Down</td>
<td>CB1F0_09_2-&gt;DPC0PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE3-&gt;CB1F0_09_3</td>
<td>Down</td>
<td>CB1F0_09_3-&gt;DPC0PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE0-&gt;CB1F0_11_0</td>
<td>Down</td>
<td>CB1F0_11_0-&gt;DPC9PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE1-&gt;CB1F0_11_1</td>
<td>Down</td>
<td>CB1F0_11_1-&gt;DPC9PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE2-&gt;CB1F0_11_2</td>
<td>Down</td>
<td>CB1F0_11_2-&gt;DPC9PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE3-&gt;CB1F0_11_3</td>
<td>Down</td>
<td>CB1F0_11_3-&gt;DPC9PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC2PFE0-&gt;CB1F0_13_0</td>
<td>up</td>
<td>CB1F0_13_0-&gt;DPC2PFE0</td>
<td>up</td>
</tr>
<tr>
<td>DPC2PFE1-&gt;CB1F0_13_1</td>
<td>up</td>
<td>CB1F0_13_1-&gt;DPC2PFE1</td>
<td>up</td>
</tr>
<tr>
<td>DPC2PFE2-&gt;CB1F0_13_2</td>
<td>up</td>
<td>CB1F0_13_2-&gt;DPC2PFE2</td>
<td>up</td>
</tr>
<tr>
<td>DPC2PFE3-&gt;CB1F0_13_3</td>
<td>up</td>
<td>CB1F0_13_3-&gt;DPC2PFE3</td>
<td>up</td>
</tr>
<tr>
<td>DPC6PFE0-&gt;CB1F0_14_0</td>
<td>Down</td>
<td>CB1F0_14_0-&gt;DPC6PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE1-&gt;CB1F0_14_1</td>
<td>Down</td>
<td>CB1F0_14_1-&gt;DPC6PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE2-&gt;CB1F0_14_2</td>
<td>Down</td>
<td>CB1F0_14_2-&gt;DPC6PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE3-&gt;CB1F0_14_3</td>
<td>Down</td>
<td>CB1F0_14_3-&gt;DPC6PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE0-&gt;CB1F0_15_0</td>
<td>Down</td>
<td>CB1F0_15_0-&gt;DPC5PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE1-&gt;CB1F0_15_1</td>
<td>Down</td>
<td>CB1F0_15_1-&gt;DPC5PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE2-&gt;CB1F0_15_2</td>
<td>Down</td>
<td>CB1F0_15_2-&gt;DPC5PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE3-&gt;CB1F0_15_3</td>
<td>Down</td>
<td>CB1F0_15_3-&gt;DPC5PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC4PFE0-&gt;CB1F1_00_0</td>
<td>up</td>
<td>CB1F1_00_0-&gt;DPC4PFE0</td>
<td>up</td>
</tr>
<tr>
<td>DPC4PFE1-&gt;CB1F1_00_1</td>
<td>up</td>
<td>CB1F1_00_1-&gt;DPC4PFE1</td>
<td>up</td>
</tr>
<tr>
<td>DPC4PFE2-&gt;CB1F1_00_2</td>
<td>up</td>
<td>CB1F1_00_2-&gt;DPC4PFE2</td>
<td>up</td>
</tr>
<tr>
<td>DPC4PFE3-&gt;CB1F1_00_3</td>
<td>up</td>
<td>CB1F1_00_3-&gt;DPC4PFE3</td>
<td>up</td>
</tr>
<tr>
<td>DPC7PFE0-&gt;CB1F1_01_0</td>
<td>Down</td>
<td>CB1F1_01_0-&gt;DPC7PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE1-&gt;CB1F1_01_1</td>
<td>Down</td>
<td>CB1F1_01_1-&gt;DPC7PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE2-&gt;CB1F1_01_2</td>
<td>Down</td>
<td>CB1F1_01_2-&gt;DPC7PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC7PFE3-&gt;CB1F1_01_3</td>
<td>Down</td>
<td>CB1F1_01_3-&gt;DPC7PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE0-&gt;CB1F1_03_0</td>
<td>Down</td>
<td>CB1F1_03_0-&gt;DPC3PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE1-&gt;CB1F1_03_1</td>
<td>Down</td>
<td>CB1F1_03_1-&gt;DPC3PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE2-&gt;CB1F1_03_2</td>
<td>Down</td>
<td>CB1F1_03_2-&gt;DPC3PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE3-&gt;CB1F1_03_3</td>
<td>Down</td>
<td>CB1F1_03_3-&gt;DPC3PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE0-&gt;CB1F1_05_0</td>
<td>Down</td>
<td>CB1F1_05_0-&gt;DPC8PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE1-&gt;CB1F1_05_1</td>
<td>Down</td>
<td>CB1F1_05_1-&gt;DPC8PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE2-&gt;CB1F1_05_2</td>
<td>Down</td>
<td>CB1F1_05_2-&gt;DPC8PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC8PFE3-&gt;CB1F1_05_3</td>
<td>Down</td>
<td>CB1F1_05_3-&gt;DPC8PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE0-&gt;CB1F1_06_0</td>
<td>Down</td>
<td>CB1F1_06_0-&gt;DPC1PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE1-&gt;CB1F1_06_1</td>
<td>Down</td>
<td>CB1F1_06_1-&gt;DPC1PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE2-&gt;CB1F1_06_2</td>
<td>Down</td>
<td>CB1F1_06_2-&gt;DPC1PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC1PFE3-&gt;CB1F1_06_3</td>
<td>Down</td>
<td>CB1F1_06_3-&gt;DPC1PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE0-&gt;CB1F1_07_0</td>
<td>Down</td>
<td>CB1F1_07_0-&gt;DPC10PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE1-&gt;CB1F1_07_1</td>
<td>Down</td>
<td>CB1F1_07_1-&gt;DPC10PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE2-&gt;CB1F1_07_2</td>
<td>Down</td>
<td>CB1F1_07_2-&gt;DPC10PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC10PFE3-&gt;CB1F1_07_3</td>
<td>Down</td>
<td>CB1F1_07_3-&gt;DPC10PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE0-&gt;CB1F1_08_0</td>
<td>Down</td>
<td>CB1F1_08_0-&gt;DPC11PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE1-&gt;CB1F1_08_1</td>
<td>Down</td>
<td>CB1F1_08_1-&gt;DPC11PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE2-&gt;CB1F1_08_2</td>
<td>Down</td>
<td>CB1F1_08_2-&gt;DPC11PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC11PFE3-&gt;CB1F1_08_3</td>
<td>Down</td>
<td>CB1F1_08_3-&gt;DPC11PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE0-&gt;CB1F1_09_0</td>
<td>Down</td>
<td>CB1F1_09_0-&gt;DPC0PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE1-&gt;CB1F1_09_1</td>
<td>Down</td>
<td>CB1F1_09_1-&gt;DPC0PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE2-&gt;CB1F1_09_2</td>
<td>Down</td>
<td>CB1F1_09_2-&gt;DPC0PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC0PFE3-&gt;CB1F1_09_3</td>
<td>Down</td>
<td>CB1F1_09_3-&gt;DPC0PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE0-&gt;CB1F1_11_0</td>
<td>Down</td>
<td>CB1F1_11_0-&gt;DPC9PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE1-&gt;CB1F1_11_1</td>
<td>Down</td>
<td>CB1F1_11_1-&gt;DPC9PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE2-&gt;CB1F1_11_2</td>
<td>Down</td>
<td>CB1F1_11_2-&gt;DPC9PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC9PFE3-&gt;CB1F1_11_3</td>
<td>Down</td>
<td>CB1F1_11_3-&gt;DPC9PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC2PFE0-&gt;CB1F1_13_0</td>
<td>up</td>
<td>CB1F1_13_0-&gt;DPC2PFE0</td>
<td>up</td>
</tr>
<tr>
<td>DPC2PFE1-&gt;CB1F1_13_1</td>
<td>up</td>
<td>CB1F1_13_1-&gt;DPC2PFE1</td>
<td>up</td>
</tr>
<tr>
<td>DPC2PFE2-&gt;CB1F1_13_2</td>
<td>up</td>
<td>CB1F1_13_2-&gt;DPC2PFE2</td>
<td>up</td>
</tr>
<tr>
<td>DPC2PFE3-&gt;CB1F1_13_3</td>
<td>up</td>
<td>CB1F1_13_3-&gt;DPC2PFE3</td>
<td>up</td>
</tr>
<tr>
<td>DPC6PFE0-&gt;CB1F1_14_0</td>
<td>Down</td>
<td>CB1F1_14_0-&gt;DPC6PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE1-&gt;CB1F1_14_1</td>
<td>Down</td>
<td>CB1F1_14_1-&gt;DPC6PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE2-&gt;CB1F1_14_2</td>
<td>Down</td>
<td>CB1F1_14_2-&gt;DPC6PFE2</td>
<td>Down</td>
</tr>
</tbody>
</table>
plane 4 is not up
plane 5 is not up

show chassis fabric map plane 1 (EX8200 Switch)

```
user@host> show chassis fabric map plane 1
regrss@tp-grande01> show chassis fabric map plane 1
```
<table>
<thead>
<tr>
<th>Interface 1</th>
<th>Interface 2</th>
<th>State 1</th>
<th>State 2</th>
<th>State 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPC2PFE1</td>
<td>CB0F0_12_1</td>
<td>Down</td>
<td>CB0F0_12_1→DPC2PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC2PFE2</td>
<td>CB0F0_12_2</td>
<td>Down</td>
<td>CB0F0_12_2→DPC2PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC2PFE3</td>
<td>CB0F0_12_3</td>
<td>Down</td>
<td>CB0F0_12_3→DPC2PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE0</td>
<td>CB0F0_13_0</td>
<td>Down</td>
<td>CB0F0_13_0→DPC5PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE1</td>
<td>CB0F0_13_1</td>
<td>Down</td>
<td>CB0F0_13_1→DPC5PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE2</td>
<td>CB0F0_13_2</td>
<td>Down</td>
<td>CB0F0_13_2→DPC5PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC5PFE3</td>
<td>CB0F0_13_3</td>
<td>Down</td>
<td>CB0F0_13_3→DPC5PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE0</td>
<td>CB0F0_14_0</td>
<td>Down</td>
<td>CB0F0_14_0→DPC3PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE1</td>
<td>CB0F0_14_1</td>
<td>Down</td>
<td>CB0F0_14_1→DPC3PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE2</td>
<td>CB0F0_14_2</td>
<td>Down</td>
<td>CB0F0_14_2→DPC3PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC3PFE3</td>
<td>CB0F0_14_3</td>
<td>Down</td>
<td>CB0F0_14_3→DPC3PFE3</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE0</td>
<td>CB0F0_15_0</td>
<td>Down</td>
<td>CB0F0_15_0→DPC6PFE0</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE1</td>
<td>CB0F0_15_1</td>
<td>Down</td>
<td>CB0F0_15_1→DPC6PFE1</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE2</td>
<td>CB0F0_15_2</td>
<td>Down</td>
<td>CB0F0_15_2→DPC6PFE2</td>
<td>Down</td>
</tr>
<tr>
<td>DPC6PFE3</td>
<td>CB0F0_15_3</td>
<td>Down</td>
<td>CB0F0_15_3→DPC6PFE3</td>
<td>Down</td>
</tr>
</tbody>
</table>
**show chassis fabric plane**

**Syntax**

```
show chassis fabric plane
```

**Syntax (TX Matrix Plus Router)**

```
show chassis fabric plane
<detail | extensive | terse>
<lcc number | sfc number>
```

**Syntax (MX Series Routers)**

```
show chassis fabric plane
<detail | extensive | terse>
<all-members>
<local>
<member member-id>
```

**Syntax (MX2010 and MX2020 3D Universal Edge Routers)**

```
show chassis fabric plane
```

**Release Information**

- Command introduced in Junos OS Release 8.0.
- Command introduced in Junos OS Release 9.4 for EX Series switches.
- Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
- Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

**Description**

(TX Matrix Plus router, T4000, T1600, M120, and MX Series routers and EX8200 switches only) On the M120 router, display the state of all fabric plane connections to the Forwarding Engine Boards (FEBs). On MX Series routers, display the state of all fabric plane connections to the Dense Port Concentrators (DPCs) and Packet Forwarding Engines (PFEs) on the Flexible PIC Concentrators (FPCs). On the TX Matrix Plus router, and on T1600 or T4000 routers in a routing matrix, display the state of the fabric management plane and the logical planes on the switch-fabric chassis (SFC) and line-card chassis (LCC). On EX8200 switches, display the state of all fabric planes. This command can be used on the master Routing Engine only.

**Options**

- **none**—(MX2010 and MX2020 Routers only) (Optional) Display the state of the fabric management plane.

- **detail**—(TX Matrix Plus routers, T1600 or T4000 routers in a routing matrix, and MX Series routers only) (Optional) Display detailed output for the fabric management plane. Show Switch Interface Board (SIB) states for the TXP-F13 SIB and the TXP-F2S SIB.

- **extensive**—(TX Matrix Plus routers, T1600 or T4000 routers in a routing matrix, and MX Series routers only) (Optional) Display extensive output for the fabric management plane.

- **terse**—(TX Matrix Plus routers and MX Series routers only) (Optional) Display terse output for the fabric management plane.

- **all-members**—(MX Series routers only) (Optional) Display the state of all fabric plane connections on all members of the Virtual Chassis configuration.
**lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number. Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(MX Series routers only) (Optional) Display the state of all fabric plane connections on the local Virtual Chassis member.

**member member-id**—(MX Series routers only) (Optional) Display the state of all fabric plane connections on the specified member of the Virtual Chassis configuration. Replace *member-id* with a value of 0 or 1.

**sfc number**—(TX Matrix Plus router only) (Optional) Show information about the TX Matrix Plus router (SFC). Replace *number* with 0.

**Required Privilege Level**

- `view`

**Related Documentation**

- request chassis fabric plane on page 747
- show chassis fabric plane-location on page 1002
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

**List of Sample Output**

- show chassis fabric plane (M120 Router) on page 968
- show chassis fabric plane (MX240 Router) on page 969
- show chassis fabric plane (MX480 Router) on page 970
- show chassis fabric plane (MX960 Router) on page 971
- show chassis fabric plane (MX240 with AS MLC Modular Carrier Card) on page 972
- show chassis fabric plane (MX480 with AS MLC Modular Carrier Card) on page 973
- show chassis fabric plane (MX480 Router with MPC4E) on page 974
- show chassis fabric plane (MX960 with AS-MLC Modular Carrier Card) on page 976
- show chassis fabric plane (MX2010 Router) on page 978
- show chassis fabric plane (MX2020 Router) on page 982
- show chassis fabric plane (MX2020 Router with MPC4E) on page 987
- show chassis fabric plane (TX Matrix Plus Router) on page 990
- show chassis fabric plane (TX Matrix Plus Router with 3D SIBs) on page 990
- show chassis fabric plane detail (TX Matrix Plus Router) on page 991
- show chassis fabric plane extensive (TX Matrix Plus Router ) on page 992
- show chassis fabric plane extensive (TX Matrix Plus Router with 3D SIBs) on page 994
- show chassis fabric plane terse (TX Matrix Plus Router) on page 996
Output Fields

Table 146 on page 962 lists the output fields for the `show chassis fabric plane` command. Output fields are listed in the approximate order in which they appear.

### Table 146: show chassis fabric plane Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plane</td>
<td>(TX Matrix Plus, MX Series routers, M120 routers, and EX8200 switches only) Number of the plane.</td>
<td>none</td>
</tr>
<tr>
<td>Plane state</td>
<td>(MX Series and M120 routers and EX8200 switches only) State of each plane:</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <strong>ACTIVE</strong>—SIB is operational and running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> On the Enhanced MX SCB with MPCs, a maximum of 4 planes are operational and running. On all the other SCBs with MPCs, all the planes are operational and running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FAULTY</strong>—SIB is in alarmed state where the SIB's plane is not operational for the following reasons:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On-board fabric ASIC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fiber optic connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FPC connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIB midplane connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(MX2010 and MX2020 Routers only) State of each plane:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ACTIVE</strong>—SFB is operational and running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>OFFLINE</strong>—SFB is in offline.</td>
<td></td>
</tr>
<tr>
<td>FEB</td>
<td>(M120 routers only) FEB number and state of links to each FEB:</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link error</strong>—Link between SIB and FPC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Links ok</strong>—Link between SIB and FPC is active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unused</strong>—No FPC is present.</td>
<td></td>
</tr>
<tr>
<td>FPC</td>
<td>(MX Series routers only) Slot number of each Dense Port Concentrator (DPC) or Flexible PIC Concentrator (FPC). An FPC occupies two DPC slots on an MX Series router. The interface corresponds to the lowest numbered DPC slot for which the FPC is installed.</td>
<td>none</td>
</tr>
</tbody>
</table>
Table 146: show chassis fabric plane Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of output</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFE</td>
<td>(MX Series and M120 routers only) Slot number of each Packet Forwarding Engine and the state of the links to the DCP: Links ok, Link error, or Unused. Each DPC includes four Packet Forwarding Engines.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• Links ok: Link between SIB and FPC is active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link error: Link between SIB and FPC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unused: No FPC is present.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(On MX240 and MX480 routers with AS MLC modular carrier card and MPC4E only) Indicates that the link between the fabric plane and the hardware link on the modular carrier card or MPC4E is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(MX2010 and MX2020 routers only) Slot number of each Packet Forwarding Engine and the state of the links to the DPC: Links ok, Link error, or Unused. Each DPC includes four Packet Forwarding Engines.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Links ok: Link between SFB and FPC is active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link error: Link between SFB and FPC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unused: No FPC is present.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>(TX Matrix Plus, and T1600 or T4000 routers in a routing matrix only)—State of the fabric plane:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Online: Fabric plane is operational and running and links on the SIB are operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Offline: Fabric plane state is Offline because the plane does not have four or more F2S and one F13 online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Empty: Fabric plane state is Empty if all SIBs in the plane are absent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Spare: Fabric plane is redundant and can be operational if the operational fabric plane encounters an error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Check: Fabric plane is in alarmed state due to the following reason and the cause of the error must be resolved:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• One or more SIBs (belonging to the fabric plane) in the Online or Spare states has transitioned to the Check state. Check state of the SIB can be caused by link errors or destination errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fault: Fabric plane is in alarmed state if one or more SIBs belonging to the plane are in the Fault state. A SIB can be in the Fault state because of the following reasons:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On-board fabric ASIC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fiber optic connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FPC connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIB midplane connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link errors have exceeded the threshold.</td>
<td></td>
</tr>
<tr>
<td>Link Errors</td>
<td>(TX Matrix Plus routers with 3D SIBs only) indicate the number of links which are marked faulty because the errors on them have crossed threshold.</td>
<td>none</td>
</tr>
</tbody>
</table>
Table 146: show chassis fabric plane Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Errors</td>
<td>(TX Matrix Plus routers with 3D SIBs only) Indicate the number of mandatory cables</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>that are not connected, or in up state for that plane</td>
<td></td>
</tr>
<tr>
<td>Destination Errors</td>
<td>(TX Matrix Plus routers with 3D SIBs only) Indicates the number of destinations that are not reachable on this plane.</td>
<td>none</td>
</tr>
<tr>
<td>Uptime</td>
<td>(TX Matrix Plus, and T1600 or T4000 routers in a routing matrix only)—Time the fabric plane has been up and running.</td>
<td>none</td>
</tr>
</tbody>
</table>

Fabric Management Plane State Output Fields for the show chassis fabric plane extensive Command on a TX Matrix Plus Router

<table>
<thead>
<tr>
<th>PLANE number</th>
<th>State of the fabric plane:</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Online: Fabric plane is operational and running and links on the SIB are operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Offline: Fabric plane state is Offline because the plane does not have 4 or more F2S and 1 F13 online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Empty: Fabric plane state is Empty if all SIBs in the plane are absent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Spare: Fabric plane is redundant and can be operational if the operational fabric plane encounters an error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Check: Fabric plane is in alarmed state due to the following reasons and the cause of the error must be resolved:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• One or more SIBs (belonging to the fabric plane) in the Online or Spare states has transitioned to the Check state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Check state of the SIB can be caused because of link errors or destination errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fault: Fabric plane is in alarmed state if one or more SIBs belonging to the plane are in the Fault state. A SIB can be in the Fault state because of the following reasons:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On-board fabric ASIC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fiber optic connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FPC connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIB midplane connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link errors have exceeded the threshold.</td>
<td></td>
</tr>
</tbody>
</table>
Table 146: show chassis fabric plane Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIB F13/F2S slt-number</td>
<td>State of the TXP-F13 SIB or TXP-F2S SIB:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Activating</strong>—Transitional state when the SIB is transitioning to the Online or Spare state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Deactivating</strong>—Transitional state when the SIB is going offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>—SIB is operational and running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Offline</strong>—SIB is powered down.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Spare</strong>—SIB is redundant and will move to active state if one of the working SIBs fails to pass traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Empty</strong>—No SIB is present.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Fault</strong>—SIB is in an alarmed state because of the following reasons and the cause of the error must be resolved:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On-board fabric ASIC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fiber optic connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FPC connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIB midplane connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link errors have exceeded the threshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Check</strong>—SIB is in an alarmed state where the SIB is partially operational because of link or destination errors. Only a SIB that is <strong>Online</strong> or <strong>Spare</strong> can transition to the <strong>Check</strong> state.</td>
<td></td>
</tr>
<tr>
<td>NOTE: If a SIB is not inserted properly, the SIB cannot transition to the <strong>Online</strong> or <strong>Spare</strong> state, and therefore cannot transition to the <strong>Check</strong> state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIB F13 slt-number</td>
<td>State of the TXP-F13 SIB even and odd port connection optical links from the TX Matrix Plus router (SFC) to the router (LCC) in the routing matrix. The left four ports on the SFC are labeled <strong>Even</strong> and provide connections to one even-numbered LCC—LCC0 or LCC2. The right four ports on the SFC are labeled <strong>Odd</strong> and provide connections to one odd-numbered LCC—LCC1 or LCC3.</td>
<td>extensive</td>
</tr>
<tr>
<td>Odd/Even</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCC number, SIB slt-number</td>
<td>State of the SIB on the LCC that is connected to the <strong>Even</strong> or <strong>Odd</strong> port on the TXP-F13 SIB faceplate:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Links ok</strong>—Links between the TXP-F13 SIB on the SFC and the LCC are active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Links error</strong>—One or more links between the TXP-F13 SIB on the SFC and the LCC, have experienced an error, but the affected links remain operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unused</strong>—No SIB is present.</td>
<td></td>
</tr>
</tbody>
</table>
Table 146: show chassis fabric plane Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of output</th>
</tr>
</thead>
</table>
| **SG number Port number** | State of the SG chip ports on the LCC:  
  - Links ok—Link is active.  
  - Link error—Link is operational with errors.  
  - Link error crc saturated—CRC has exceeded the rate threshold and reached saturation without optical issues—that is, a cable has not been cut, removed, or otherwise experienced an error.  
  - Link error crc saturated with optical errors—CRC has exceeded the rate threshold and reached saturation with optical issues—that is, a cable has been cut, removed, or otherwise experienced an error.  
  - Unused—Port is not in use. | extensive |
| **SIB F2S slot-number** | State of the intra-chassis links between the TXP-F2S and TXP-F13 SIBs. | extensive |

Fabric Management SIB State Output Fields for the show chassis fabric plane extensive Command on a TX Matrix Plus Router
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIB slot-number</td>
<td>State of the SIBs on the T1600/T4000 router (LCC) in the routing matrix:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Activating</strong>—Transitional state when the SIB is coming online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Deactivating</strong>—Transitional state when the SIB is going offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Connected</strong>—SIBS on an LCC are connected and trained, but are either not online or are spare, because the plane on the the TX Matrix Plus router (SFC) is still offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The LCC SIB transitions to the <strong>Connected</strong> state when the F13 SIB to which it connects is online but the SFC plane (to which the LCC SIB connects) is offline for some reason; for instance, when there are insufficient number of F2 SIBs in the plane.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Disconnected</strong>—If an F13 SIB on the TX Matrix Plus router (SFC) goes offline, then the SIBs on the LCCs connected to the F13 SIB get disconnected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On the TX Matrix Plus router with 3D SIBs, the LCC SIB is also disconnected if the F13 SIB is online, but none of the cables are connected or trained.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The <strong>Disconnected</strong> state is valid only for SIBs on an LCC. An LCC SIB transitions to the <strong>Disconnected</strong> state when the F13 SIB to which it connects goes <strong>Offline</strong>, irrespective of the state of the SFC plane.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>SFC Error</strong>—If an F13 SIB on the TX Matrix Plus router (SFC) transitions to the <strong>Fault</strong> state (because of link errors, for instance), and if an LCC SIB connected to the F13 SIB comes online, the LCC SIB transitions to the <strong>SFC Error</strong> state. This state indicates that the F13 SIB to which the LCC SIB is connected has errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The <strong>Connected</strong>, <strong>Disconnected</strong>, and <strong>SFC Error</strong> states are applicable only to the SIBs on an LCC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>—SIB is operational and running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Offline</strong>—SIB is powered down.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Spare</strong>—SIB is redundant and will move to active state if one of the working SIBs fails to pass traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Empty</strong>—No SIB is present.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Fault</strong>—SIB is in alarmed state where the SIB’s plane is not operational for the following reasons:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On-board fabric ASIC is not operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fiber optic connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FPC connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SIB midplane connector faults.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link errors have exceeded the threshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Check</strong>—SIB is in alarmed state where the SIB is partially operational because of link or destination errors. Only a SIB that is <strong>Online</strong> or <strong>Spare</strong> can transition to the <strong>Check</strong> state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: If a SIB is not inserted properly, the SIB cannot transition to the <strong>Online</strong> or <strong>Spare</strong> state, and therefore cannot transition to the <strong>Check</strong> state.</td>
<td></td>
</tr>
</tbody>
</table>
Table 146: show chassis fabric plane Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LCC SIB Link State</strong></td>
<td>State of the LCC SIB link:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Links ok—Link is active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Links error—A link error has occurred, but the link remains operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unused—SIB is not in use.</td>
<td></td>
</tr>
<tr>
<td><strong>SG number Port number</strong></td>
<td>State of the SG chip ports on the LCC:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Links ok—Link is active.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link error—Link is operational with errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link error crc saturated—CRC has exceeded the rate threshold and reached saturation without optical issues—that is, a cable has not been cut, removed, or otherwise experienced an error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link error crc saturated with optical errors—CRC has exceeded the rate threshold and reached saturation with optical issues—that is, a cable has been cut, removed, or otherwise experienced an error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unused—Port is not in use.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

**show chassis fabric plane (M120 Router)**

```
user@host> show chassis fabric plane
Fabric management PLANE state
Plane 0
Plane state: ACTIVE
FEB 0: Links ok
FEB 1: Links ok
FEB 2: Links ok
FEB 3: Links ok
FEB 4: Links ok
FEB 5: Links ok
Plane 1
Plane state: ACTIVE
FEB 0: Links ok
FEB 1: Links ok
FEB 2: Links ok
FEB 3: Links ok
FEB 4: Links ok
FEB 5: Links ok
Plane 2
Plane state: ACTIVE
FEB 0: Links ok
FEB 1: Links ok
FEB 2: Links ok
FEB 3: Links ok
FEB 4: Links ok
FEB 5: Links ok
Plane 3
Plane state: ACTIVE
FEB 0: Links ok
FEB 1: Links ok
```
show chassis fabric plane (MX240 Router)

user@host> show chassis fabric plane
Plane 0
  Plane state: ACTIVE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok
  FPC 2
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 1
  Plane state: ACTIVE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok
  FPC 2
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 2
  Plane state: ACTIVE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok
  FPC 2
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 3
  Plane state: ACTIVE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok
  FPC 2
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 4
  Plane state: SPARE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 2
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok

Plane 5
Plane state: SPARE
FPC 1
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 2
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok

Plane 6
Plane state: SPARE
FPC 1
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 2
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok

Plane 7
Plane state: SPARE
FPC 1
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 2
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok

**show chassis fabric plane (MX480 Router)**

```
user@host> show chassis fabric plane
Fabric management PLANE state
Plane 0
Plane state: ACTIVE
FPC 1
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok

Plane 1
Plane state: ACTIVE
FPC 1
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
```
Plane 2
  Plane state: ACTIVE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 3
  Plane state: ACTIVE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 4
  Plane state: SPARE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 5
  Plane state: SPARE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 6
  Plane state: SPARE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

Plane 7
  Plane state: SPARE
  FPC 1
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok

show chassis fabric plane (MX960 Router)

user@host> show chassis fabric plane
Plane 0
  Plane state: ACTIVE
  FPC 0
    PFE 0: Links ok
  FPC 2
    PFE 0: Links ok
    PFE 1: Links ok

Plane 1
  Plane state: ACTIVE
  FPC 0
    PFE 0: Links ok
  FPC 2
    PFE 0: Links ok
    PFE 1: Links ok
Plane 2
  Plane state: ACTIVE
  FPC 0
    PFE 0 :Links ok
  FPC 2
    PFE 0 :Links ok
    PFE 1 :Links ok
Plane 3
  Plane state: ACTIVE
  FPC 0
    PFE 0 :Links ok
  FPC 2
    PFE 0 :Links ok
    PFE 1 :Links ok

show chassis fabric plane (MX240 with AS MLC Modular Carrier Card)

In the following output, FPC 1 is the AS MLC modular carrier card (AS MCC).

user@host>show chassis fabric plane
Fabric management PLANE state
Plane 0
  Plane state: ACTIVE
  FPC 1
    PFE 0 :Links ok
  FPC 2
    PFE 0 :Links ok
Plane 1
  Plane state: ACTIVE
  Plane state: ACTIVE
  FPC 1
    PFE 0 :Links ok
  FPC 2
    PFE 0 :Links ok
Plane 2
  Plane state: ACTIVE
  FPC 2
    PFE 0 :Links ok
  FPC 4
    PFE 0 :Links ok
    PFE 2 :Links ok
  FPC 5
    PFE 0 :Links ok
Plane 3
  Plane state: ACTIVE
  Plane state: ACTIVE
  FPC 1
    PFE 0 :Links ok
  FPC 2
    PFE 0 :Links ok
Plane 4
  Plane state: ACTIVE
  Plane state: ACTIVE
  FPC 1
    PFE 0 :Links ok
  FPC 2
    PFE 0 :Links ok
Plane 5
  Plane state: ACTIVE
  FPC 1
    PFE 0 :Unused
show chassis fabric plane (MX480 with AS MLC Modular Carrier Card)

In the following output, FPC 5 is the AS MLC modular carrier card (AS MCC).
PFE 0 :Links ok
FPC 4
PFE 0 :Links ok
PFE 2 :Links ok
FPC 5
PFE 0 :Links ok
Plane 5
Plane state: ACTIVE
FPC 2
PFE 0 :Links ok
FPC 4
PFE 0 :Links ok
PFE 2 :Links ok
FPC 5
PFE 0 :Unused
Plane 6
Plane state: ACTIVE
FPC 2
PFE 0 :Links ok
FPC 4
PFE 0 :Links ok
PFE 2 :Links ok
FPC 5
PFE 0 :Links ok
Plane 7
Plane state: ACTIVE
FPC 2
PFE 0 :Links ok
FPC 4
PFE 0 :Links ok
PFE 2 :Links ok
FPC 5
PFE 0 :Unused

show chassis fabric plane (MX480 Router with MPC4E)

user@host > show chassis fabric plane
Fabric management PLANE state
Plane 0
Plane state: ACTIVE
FPC 0
PFE 0 :Links ok
PFE 1 :Links ok
FPC 1
PFE 0 :Links ok
PFE 1 :Links ok
PFE 2 :Links ok
PFE 3 :Links ok
FPC 3
PFE 0 :Links ok
FPC 4
PFE 0 :Links ok
PFE 1 :Links ok
Plane 1
Plane state: ACTIVE
FPC 0
PFE 0 :Links ok
PFE 1 :Links ok
FPC 1
PFE 0 :Links ok
PFE 1 :Links ok
Plane 2
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 3
  PFE 0 : Links ok
FPC 4
  PFE 0 : Links ok
  PFE 1 : Links ok
Plane 3
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 3
  PFE 0 : Links ok
FPC 4
  PFE 0 : Links ok
  PFE 1 : Links ok
Plane 4
Plane state: SPARE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 3
  PFE 0 : Links ok
FPC 4
  PFE 0 : Links ok
  PFE 1 : Links ok
Plane 5
Plane state: SPARE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
show chassis fabric plane (MX960 with AS-MLC Modular Carrier Card)

In the following output, FPC 1 is a modular carrier card.

user@host> show chassis fabric plane
Fabric management PLANE state
Plane 0
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 4
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 5
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 8
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok

Plane 6
Plane state: SPARE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 3
  PFE 0 : Links ok
FPC 4
  PFE 0 : Links ok
  PFE 1 : Links ok

Plane 7
Plane state: SPARE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 3
  PFE 0 : Links ok
FPC 4
  PFE 0 : Links ok
  PFE 1 : Links ok
Plane 1
Plane state: ACTIVE
FPC 0
  PFE 0: Links ok
  PFE 1: Links ok
  FPC 1
    PFE 0: Links ok
  FPC 4
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok
  FPC 5
    PFE 0: Links ok
    FPC 8
      PFE 0: Links ok
      PFE 1: Links ok
      PFE 2: Links ok
      PFE 3: Links ok

Plane 2
Plane state: ACTIVE
FPC 0
  PFE 0: Links ok
  PFE 1: Links ok
  FPC 1
    PFE 0: Links ok
  FPC 4
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok
  FPC 5
    PFE 0: Links ok
    FPC 8
      PFE 0: Links ok
      PFE 1: Links ok
      PFE 2: Links ok
      PFE 3: Links ok

Plane 3
Plane state: ACTIVE
FPC 0
  PFE 0: Links ok
  PFE 1: Links ok
  FPC 1
    PFE 0: Links ok
  FPC 4
    PFE 0: Links ok
    PFE 1: Links ok
    PFE 2: Links ok
    PFE 3: Links ok
  FPC 5
    PFE 0: Links ok
    FPC 8
      PFE 0: Links ok
      PFE 1: Links ok
      PFE 2: Links ok
      PFE 3: Links ok

Plane 4
Plane state: SPARE
FPC 0
show chassis fabric plane (MX2010 Router)

user@host>show chassis fabric plane
Fabric management PLANE state
Plane 0
  Plane state: ACTIVE
    FPC 0
      PFE 0 : Links ok
      PFE 1 : Links ok
    FPC 1
      PFE 0 : Links ok
    FPC 2
      PFE 0 : Links ok
    FPC 3
      PFE 0 : Links ok
      PFE 1 : Links ok
    FPC 4
      PFE 0 : Links ok
      PFE 1 : Links ok
      PFE 2 : Links ok
      PFE 3 : Links ok
    FPC 5
      PFE 0 : Links ok
      PFE 1 : Links ok
      PFE 2 : Links ok
      PFE 3 : Links ok
Plane 1
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
FPC 2
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 3
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 4
  PFE 0 : Links ok
FPC 5
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 6
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 7
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 8
  PFE 0 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok
Plane 2
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
FPC 2
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 3
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 4
Plane 3
Plane state: OFFLINE

Plane 4
Plane state: ACTIVE

Plane 5
Plane state: ACTIVE
PFE 1 : Links ok
FPC 3
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 4
  PFE 0 : Links ok
FPC 5
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 6
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 7
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 8
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok

Plane 6
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 1
  PFE 0 : Links ok
FPC 2
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 3
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 4
  PFE 0 : Links ok
FPC 5
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 6
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 7
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 8
  PFE 0 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok

Plane 7
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
show chassis fabric plane (MX2020 Router)

user@host>show chassis fabric plane
Fabric management PLANE state
Plane 0
  Plane state: ACTIVE
  FPC 0
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 1
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 2
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 3
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 4
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 5
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 6
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 7
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 8
    PFE 0 :Links ok
    PFE 1 :Links ok
    PFE 2 :Links ok
    PFE 3 :Links ok
  FPC 9
    PFE 0 :Links ok
    PFE 1 :Links ok
FPC 5
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 6
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 7
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 8
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 10
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 11
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 12
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 13
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 14
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 15
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 16
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 17
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 10
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 11
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 12
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 13
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 14
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 15
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 16
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 17
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 18
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
FPC 19
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok

Plane 2
  Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
PFE 3 : Links ok
FPC 1
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 2
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 3
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 4
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 5
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 6
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 7
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 8
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 9
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 10
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 11
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
FPC 12
PFE 0 : Links ok
PFE 1 : Links ok
PFE 2 : Links ok
PFE 3 : Links ok
show chassis fabric plane (MX2020 Router with MPC4E)

user@host > show chassis fabric plane
Fabric management PLANE state
Plane 0
Plane state: ACTIVE
  FPC 0
  PFE 0 :Links ok
  PFE 1 :Links ok
  FPC 9
  PFE 0 :Links ok
  PFE 1 :Links ok
  FPC 10
  PFE 0 :Links ok
  FPC 14
  PFE 0 :Links ok
  PFE 1 :Links ok
  FPC 19
  PFE 0 :Links ok
  PFE 1 :Links ok
  Plane 1
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 10
  PFE 0 : Links ok
FPC 14
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 19
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok

Plane 2
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 10
  PFE 0 : Links ok
FPC 14
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 19
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok

Plane 3
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 10
  PFE 0 : Links ok
FPC 14
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 19
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok

Plane 4
Plane state: ACTIVE
FPC 0
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 9
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 10
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 14
  PFE 0 : Links ok
  PFE 1 : Links ok
FPC 19
  PFE 0 : Links ok
  PFE 1 : Links ok
  PFE 2 : Links ok
  PFE 3 : Links ok
Plane 5
  Plane state: ACTIVE
  FPC 0
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 9
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 10
    PFE 0 : Links ok
  FPC 14
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 19
    PFE 0 : Links ok
    PFE 1 : Links ok
    PFE 2 : Links ok
    PFE 3 : Links ok
Plane 6
  Plane state: ACTIVE
  FPC 0
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 9
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 10
    PFE 0 : Links ok
  FPC 14
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 19
    PFE 0 : Links ok
    PFE 1 : Links ok
    PFE 2 : Links ok
    PFE 3 : Links ok
Plane 7
  Plane state: ACTIVE
  FPC 0
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 9
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 10
    PFE 0 : Links ok
  FPC 14
    PFE 0 : Links ok
    PFE 1 : Links ok
  FPC 19
    PFE 0 : Links ok
show chassis fabric plane (TX Matrix Plus Router)

```
user@host> show chassis fabric plane
sfc0-re0:
```

<table>
<thead>
<tr>
<th>Plane</th>
<th>State</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 16 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 13 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 9 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 7 seconds</td>
</tr>
</tbody>
</table>

```
lcc0-re0:
```

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 16 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 13 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 9 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 7 seconds</td>
</tr>
</tbody>
</table>

```
lcc2-re0:
```

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 16 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 12 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 9 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>10 hours, 7 seconds</td>
</tr>
</tbody>
</table>

show chassis fabric plane (TX Matrix Plus Router with 3D SIBs)

```
user@host> show chassis fabric plane
sfc0-re0:
```

<table>
<thead>
<tr>
<th>Plane</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>5 hours, 11 minutes, 3 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 4 minutes, 24 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 3 minutes, 16 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 2 minutes, 12 seconds</td>
</tr>
</tbody>
</table>

```
lcc2-re0:
```

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>5 hours, 11 minutes, 3 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 4 minutes, 57 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 3 minutes, 53 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 2 minutes, 45 seconds</td>
</tr>
</tbody>
</table>
### lcc4-re0:

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>5 hours, 11 minutes, 12 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 4 minutes, 24 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 3 minutes, 16 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 2 minutes, 12 seconds</td>
</tr>
</tbody>
</table>

### lcc5-re0:

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>5 hours, 11 minutes, 12 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 4 minutes, 24 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 3 minutes, 16 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>8 hours, 2 minutes, 11 seconds</td>
</tr>
</tbody>
</table>

### show chassis fabric plane detail (TX Matrix Plus Router)

```
user@host> show chassis fabric plane detail
sfc0-re0:

Fabric Management PLANE State:
PLANE 0:  Spare
    SIB F13 0 :  Spare
    SIB F13 1 :  Empty
    SIB F2S 0/0 :  Spare
    SIB F2S 0/2 :  Spare
    SIB F2S 0/4 :  Spare
    SIB F2S 0/6 :  Spare
PLANE 1:  Online
    SIB F13 3 :  Online
    SIB F13 4 :  Empty
    SIB F2S 1/0 :  Online
    SIB F2S 1/2 :  Online
    SIB F2S 1/4 :  Online
    SIB F2S 1/6 :  Online
PLANE 2:  Online
    SIB F13 6 :  Online
    SIB F13 7 :  Empty
    SIB F2S 2/0 :  Online
    SIB F2S 2/2 :  Online
    SIB F2S 2/4 :  Online
    SIB F2S 2/6 :  Online
PLANE 3:  Online
    SIB F13 8 :  Online
    SIB F13 9 :  Online
    SIB F2S 3/0 :  Online
    SIB F2S 3/2 :  Online
    SIB F2S 3/4 :  Online
    SIB F2S 3/6 :  Online
```
PLANE 4:  Online
  SIB F13 11 :  Online
  SIB F13 12 :  Online
  SIB F2S 4/0 :  Online
  SIB F2S 4/2 :  Online
  SIB F2S 4/4 :  Online
  SIB F2S 4/6 :  Online

lcc0-re0:

Fabric Management SIB State:
  SIB  0 :  Spare
  SIB  1 :  Online
  SIB  2 :  Online
  SIB  3 :  Online
  SIB  4 :  Online

lcc1-re0:

Fabric Management SIB State:
  SIB  0 :  Spare
  SIB  1 :  Online
  SIB  2 :  Online
  SIB  3 :  Online
  SIB  4 :  Online
...

show chassis fabric plane extensive (TX Matrix Plus Router)

user@host> show chassis fabric plane extensive
sfc0-re0:

Fabric Management PLANE State:
PLANE 0:  Spare
  SIB F13 0 :  Spare
  SIB F13 1 :  Empty
  SIB F2S 0/0 :  Spare
  SIB F2S 0/2 :  Spare
  SIB F2S 0/4 :  Spare
  SIB F2S 0/6 :  Spare
  SIB F13 0 Even:
    LCC 0, SIB 0 : Links ok
      SG 0
        Port 0 : Links ok
        Port 1 : Links ok
        Port 2 : Links ok
        Port 3 : Links ok
      SG 1
        Port 0 : Links ok
        Port 1 : Links ok
        Port 2 : Links ok
        Port 3 : Links ok
      SG 2
        Port 0 : Links ok
        Port 1 : Links ok
        Port 2 : Links ok
        Port 3 : Links ok
      SG 3
        Port 0 : Links ok
        Port 1 : Links ok
        Port 2 : Links ok
Port 3 : Links ok

SIB F13 0 Odd:
  LCC 1, SIB 0 : Links ok
    SG 0
      Port 0 : Links ok
      Port 1 : Links ok
      Port 2 : Links ok
      Port 3 : Links ok
    SG 1
      Port 0 : Links ok
      Port 1 : Links ok
      Port 2 : Links ok
      Port 3 : Links ok
    SG 2
      Port 0 : Links ok
      Port 1 : Links ok
      Port 2 : Links ok
      Port 3 : Links ok
    SG 3
      Port 0 : Links ok
      Port 1 : Links ok
      Port 2 : Links ok
      Port 3 : Links ok
  SIB F2S 0/0: Links ok
  SIB F2S 0/2: Links ok
  SIB F2S 0/4: Links ok
  SIB F2S 0/6: Links ok

SIB F13 1 Even:
  LCC 2, SIB 0 : Unused
    SG 0
      Port 0 : Unused
      Port 1 : Unused
      Port 2 : Unused
      Port 3 : Unused
    SG 1
      Port 0 : Unused
      Port 1 : Unused
      Port 2 : Unused
      Port 3 : Unused
    SG 2
      Port 0 : Unused
      Port 1 : Unused
      Port 2 : Unused
      Port 3 : Unused
    SG 3
      Port 0 : Unused
      Port 1 : Unused
      Port 2 : Unused
      Port 3 : Unused
  SIB F2S 0/0: Links ok
  SIB F2S 0/2: Links ok
  SIB F2S 0/4: Links ok
  SIB F2S 0/6: Links ok

SIB F13 1 Odd:
  LCC 3, SIB 0 : Unused
    SG 0
      Port 0 : Unused
      Port 1 : Unused
      Port 2 : Unused
      Port 3 : Unused
    SG 1
      Port 0 : Unused
      Port 1 : Unused
      Port 2 : Unused
      Port 3 : Unused

Copyright © 2013, Juniper Networks, Inc.
SG 2
  Port 0 : Unused
  Port 1 : Unused
  Port 2 : Unused
  Port 3 : Unused

SG 3
  Port 0 : Unused
  Port 1 : Unused
  Port 2 : Unused
  Port 3 : Unused
  SIB F2S 0/0: Unused
  SIB F2S 0/2: Unused
  SIB F2S 0/4: Unused
  SIB F2S 0/6: Unused

PLANE 1:    Online
  SIB F13 3   :    Online
  SIB F13 4   :    Empty
  SIB F2S 1/0 :    Online
  SIB F2S 1/2 :    Online
  SIB F2S 1/4 :    Online
  SIB F2S 1/6 :    Online
  SIB F13 3 Even:
  ...

show chassis fabric plane extensive (TX Matrix Plus Router with 3D SIBs)

user@host> show chassis fabric plane extensive
sfc0-re0:
--------------------------------------------------------------------------
Fabric Management PLANE State:
PLANE 0:    Online
  SIB F13 0   :    Empty
  SIB F13 1   :    Online
  SIB F2S 0/0 :    Online
  SIB F2S 0/2 :    Online
  SIB F2S 0/4 :    Online
  SIB F2S 0/6 :    Online
  SIB F13 0
    LCC 0, SIB 0 : Unused
      PFE 0   : Unused
      PFE 1   : Unused
      PFE 2   : Unused
      PFE 3   : Unused
      PFE 4   : Unused
      PFE 5   : Unused
      PFE 6   : Unused
      PFE 7   : Unused
      PFE 8   : Unused
      PFE 9   : Unused
      PFE 10  : Unused
      PFE 11  : Unused
      PFE 12  : Unused
      PFE 13  : Unused
      PFE 14  : Unused
      PFE 15  : Unused
    LCC 1, SIB 0 : Unused
      PFE 0   : Unused
      PFE 1   : Unused
      PFE 2   : Unused
      PFE 3   : Unused
      PFE 4   : Unused
<table>
<thead>
<tr>
<th>PFE 0</th>
<th>Unused</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFE 1</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 2</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 3</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 4</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 5</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 6</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 7</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 8</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 9</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 10</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 11</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 12</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 13</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 14</td>
<td>Unused</td>
</tr>
<tr>
<td>LCC 2, SIB 0</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 0</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 1</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 2</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 3</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 4</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 5</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 6</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 7</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 8</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 9</td>
<td>Unused</td>
</tr>
<tr>
<td>PFE 10</td>
<td>Unused</td>
</tr>
</tbody>
</table>

Fabric Management SIB State:

<table>
<thead>
<tr>
<th>SIB 0</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCC SIB Link State : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 0 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 1 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 2 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 3 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 4 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 5 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 6 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 7 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 8 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 9 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 10 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 11 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 12 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 13 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 14 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 15 : Links ok</td>
<td></td>
</tr>
<tr>
<td>FPC 1</td>
<td></td>
</tr>
<tr>
<td>PFE 0 : Links ok</td>
<td></td>
</tr>
<tr>
<td>FPC 2</td>
<td></td>
</tr>
<tr>
<td>PFE 0 : Links ok</td>
<td></td>
</tr>
<tr>
<td>FPC 3</td>
<td></td>
</tr>
<tr>
<td>PFE 0 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 1 : Links ok</td>
<td></td>
</tr>
<tr>
<td>FPC 4</td>
<td></td>
</tr>
<tr>
<td>PFE 0 : Links ok</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIB 1</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCC SIB Link State : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 0 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 1 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 2 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 3 : Links ok</td>
<td></td>
</tr>
<tr>
<td>PFE 4 : Links ok</td>
<td></td>
</tr>
</tbody>
</table>
PFE  5  : Links ok
PFE  6  : Links ok
PFE  7  : Links ok
PFE  8  : Links ok
PFE  9  : Links ok
PFE 10 : Links ok
PFE 11 : Links ok
PFE 12 : Links ok
PFE 13 : Links ok
PFE 14 : Links ok
PFE 15 : Links ok
FPC  0
FPC  1
  PFE 0  : Links ok
FPC  2
  PFE 0  : Links ok
FPC  3
  PFE 0  : Links ok
  PFE 1  : Links ok
FPC  4
  PFE 0  : Links ok

show chassis fabric plane terse (TX Matrix Plus Router)

user@host> show chassis fabric plane terse
sfc0-re0:
-----------------------------------------------------------------------
| Plane | State   | Link errors | Destination errors | Uptime               |
-----------------------------------------------------------------------
| 0     | Spare   | NONE        | NONE               | 18 minutes, 37 seconds |
| 1     | Online  | NONE        | NONE               | 18 minutes, 36 seconds |
| 2     | Online  | NONE        | NONE               | 18 minutes, 33 seconds |
| 3     | Online  | NONE        | NONE               | 18 minutes, 31 seconds |
| 4     | Online  | NONE        | NONE               | 18 minutes, 31 seconds |

lcc1-re0:
-----------------------------------------------------------------------
| SIB  | State | Link errors | Destination errors | Uptime               |
-----------------------------------------------------------------------
| 0    | Spare | NONE        | NONE               | 18 minutes, 37 seconds |
| 1    | Online| NONE        | NONE               | 18 minutes, 37 seconds |
| 2    | Online| NONE        | NONE               | 18 minutes, 36 seconds |
| 3    | Online| NONE        | NONE               | 18 minutes, 32 seconds |
| 4    | Empty | NONE        | NONE               |                      |

lcc2-re0:
-----------------------------------------------------------------------
| SIB  | State | Link errors | Destination errors | Uptime               |
-----------------------------------------------------------------------
| 0    | Spare | NONE        | NONE               | 18 minutes, 37 seconds |
| 1    | Online| NONE        | NONE               | 18 minutes, 37 seconds |
| 2    | Online| NONE        | NONE               | 18 minutes, 36 seconds |
| 3    | Online| NONE        | NONE               | 18 minutes, 32 seconds |
| 4    | Online| NONE        | NONE               | 18 minutes, 31 seconds |

show chassis fabric plane terse (TX Matrix Plus Router with 3D SIBs)

user@host> show chassis fabric plane terse
### show chassis fabric plane sfc0-re0:

<table>
<thead>
<tr>
<th>Plane</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 14 hours, 14 minutes, 26 seconds</td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 26 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 26 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 26 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 26 seconds</td>
</tr>
</tbody>
</table>

### show chassis fabric plane lcc2-re0:

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 17 minutes</td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 17 minutes</td>
</tr>
<tr>
<td>2</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 17 minutes</td>
</tr>
<tr>
<td>3</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 17 minutes</td>
</tr>
<tr>
<td>4</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 17 minutes</td>
</tr>
</tbody>
</table>

### show chassis fabric plane lcc4-re0:

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 38 seconds</td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 38 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 38 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 38 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 38 seconds</td>
</tr>
</tbody>
</table>

### show chassis fabric plane lcc5-re0:

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 34 seconds</td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 34 seconds</td>
</tr>
<tr>
<td>2</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 34 seconds</td>
</tr>
<tr>
<td>3</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 34 seconds</td>
</tr>
<tr>
<td>4</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 14 minutes, 34 seconds</td>
</tr>
</tbody>
</table>

### show chassis fabric plane lcc (TX Matrix Plus Router)

```
user@host> show chassis fabric plane lcc 1
```

**lcc1-re0:**

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Spare</td>
<td>NONE</td>
<td>NONE</td>
<td>25 minutes, 17 seconds</td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Disconnected</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Disconnected</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td>NONE</td>
<td>NONE</td>
<td></td>
</tr>
</tbody>
</table>

### show chassis fabric plane lcc (TX Matrix Plus Router with 3D SIBs)

```
user@host> show chassis fabric plane lcc 2
```

**lcc2-re0:**

<table>
<thead>
<tr>
<th>SIB</th>
<th>State</th>
<th>Cable errors</th>
<th>Link errors</th>
<th>Destination errors</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Offline</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 17 minutes</td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>1 day, 18 hours, 17 minutes</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
show chassis fabric plane sfc (TX Matrix Plus Router)

```
user@host> show chassis fabric planesfc
sfc0-re0:

Plane  State        Cable errors   Link errors   Destination errors  Uptime
0     Offline          NONE          NONE              NONE
1     Online           NONE          NONE              NONE         1 day, 18 hours, 14 minutes, 20 seconds
2     Offline          NONE          NONE              NONE
3     Offline          NONE          NONE              NONE
4     Offline          NONE          NONE              NONE

show chassis fabric plane sfc (TX Matrix Plus Router with 3D SIBs)

user@host> show chassis fabric planesfc
sfc0-re0:

Plane  State        Cable errors   Link errors   Destination errors  Uptime
0     Offline          NONE          NONE              NONE
1     Online           NONE          NONE              NONE         1 day, 18 hours, 14 minutes, 20 seconds
2     Offline          NONE          NONE              NONE
3     Offline          NONE          NONE              NONE
4     Offline          NONE          NONE              NONE

show chassis fabric plane (T1600 Router)

user@host> show chassis fabric plane

Plane  State               Uptime
0    Online               15 hours, 42 minutes, 9 seconds
1    Online               15 hours, 42 minutes, 9 seconds
2    Fault
3    Online               15 hours, 42 minutes, 9 seconds
4    Online               15 hours, 42 minutes, 9 seconds

show chassis fabric plane extensive (T1600 Router)

user@host> show chassis fabric planesfc extensive

Fabric Management PLANE State:
PLANE 0:    Online
ST-SIB-L  0: Links ok
  SG 0
    Port 0  : Links ok
    Port 1  : Links ok
    Port 2  : Links ok
    Port 3  : Links ok
  SG 1
    Port 0  : Links ok
    Port 1  : Links ok
    Port 2  : Links ok
    Port 3  : Links ok
  SG 2
    Port 0  : Links ok
    Port 1  : Links ok
Port 2 : Links ok
Port 3 : Links ok
SG 3
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok
ST-SIB-L 0
FPC 4
PFE 0: Links ok
PFE 1: Links ok
FPC 6
PFE 0: Links ok
PFE 1: Links ok
FPC 7
PFE 0: Links ok
PLANE 1: Online
ST-SIB-L 1: Links ok
SG 0
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok
SG 1
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok
SG 2
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok
SG 3
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok
ST-SIB-L 1
FPC 4
PFE 0: Links ok
PFE 1: Links ok
FPC 6
PFE 0: Links ok
PFE 1: Links ok
FPC 7
PFE 0: Links ok
PLANE 2: Online
ST-SIB-L 2: Links ok
SG 0
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok
SG 1
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok
SG 2
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

SG 3
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

ST-SIB-L 2
FPC 4
PFE 0: Links ok
PFE 1: Links ok
FPC 6
PFE 0: Links ok
PFE 1: Links ok
FPC 7
PFE 0: Links ok

PLANE 3: Spare
ST-SIB-L 3: Links ok

SG 0
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

SG 1
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

SG 2
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

SG 3
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

ST-SIB-L 3
FPC 4
PFE 0: Links ok
PFE 1: Links ok
FPC 6
PFE 0: Links ok
PFE 1: Links ok
FPC 7
PFE 0: Links ok

PLANE 4: Online
ST-SIB-L 4: Links ok

SG 0
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

SG 1
Port 0 : Links ok
Port 1 : Links ok
Port 2 : Links ok
Port 3 : Links ok

SG 2
Port 0    : Links ok
Port 1    : Links ok
Port 2    : Links ok
Port 3    : Links ok

SG 3
Port 0    : Links ok
Port 1    : Links ok
Port 2    : Links ok
Port 3    : Links ok

ST-SIB-L 4
FPC 4
PFE 0: Links ok
PFE 1: Links ok
FPC 6
PFE 0: Links ok
PFE 1: Links ok
FPC 7
PFE 0: Links ok

show chassis fabric plane detail (T1600 Router)

user@host> show chassis fabric plane detail
Fabric Management PLANE State:
PLANE 0:    Online
PLANE 1:    Online
PLANE 2:    Online
PLANE 3:    Spare
PLANE 4:    Online

show chassis fabric plane (EX8200 Switch)

user@host> show chassis fabric plane
Fabric management PLANE state
Plane 0
  Plane state: ACTIVE
Plane 1
  Plane state: ACTIVE
Plane 2
  Plane state: ACTIVE
Plane 3
  Plane state: ACTIVE
Plane 4
  Plane state: SPARE
Plane 5
  Plane state: SPARE
Plane 6
  Plane state: SPARE
Plane 7
  Plane state: SPARE
Plane 8
  Plane state: ACTIVE
Plane 9
  Plane state: ACTIVE
Plane 10
  Plane state: ACTIVE
Plane 11
  Plane state: ACTIVE
**show chassis fabric plane-location**

**Syntax**

```
show chassis fabric plane-location
```

**Syntax (MX Series Routers)**

```
<all-members>
<local>
<member member-id>
```

**Syntax (MX2010 3D Universal Edge Routers)**

```
show chassis fabric plane-location
```

**Syntax (MX2020 3D Universal Edge Routers)**

```
show chassis fabric plane-location
```

**Syntax (TX Matrix Plus Router)**

```
show chassis fabric plane-location
```

**Release Information**

Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.4 for EX Series switches.
Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

**Description**

(M120, MX Series routers, and EX8200 switches only) Display the Control Board (CB) location of each plane. This command can be used on the master Routing Engine or the backup Routing Engine. For information about the meaning of “CBs” and “fabric plane” on the switches, see “EX Series Switches Hardware and CLI Terminology Mapping” on page 389.

(TX Matrix Plus routers only) Display the SIB location of each fabric plane.

(PTX Series Packet Transport Routers only) Display the fabric plane location of each SIB.

(MX2010 and MX2020 Routers only) Display the fabric plane location of each Switch Fabric Board (SFB).

**Options**

- **all-members**—(MX Series routers only) (Optional) Display the CB location of each fabric plane on the Routing Engines in all member routers in the Virtual Chassis configuration.
- **local**—(MX Series routers only) (Optional) Display the CB location of each fabric plane on the Routing Engines in the local Virtual Chassis member.
- **member member-id**—(MX Series routers only) (Optional) Display the CB location of each fabric plane on the Routing Engines in the specified member in the Virtual Chassis configuration. Replace `member-id` with a value of 0 or 1.
Required Privilege Level

view

List of Sample Output

show chassis fabric plane-location (M120 Router) on page 1004
show chassis fabric plane-location (MX240 and MX480 Routers) on page 1004
show chassis fabric plane-location (MX960 Router) on page 1004
show chassis fabric plane-location (MX2010 Router) on page 1004
show chassis fabric plane-location (MX2020 Router) on page 1004
show chassis fabric plane-location (TX Matrix Plus Router) on page 1005
show chassis fabric plane-location (TX Matrix Plus Router with 3D SIBs) on page 1005
show chassis fabric plane-location (EX8200 Switch) on page 1005
show chassis fabric plane-location (PTX Series Packet Transport Routers) on page 1005

Output Fields

Table 147 on page 1003 lists the output fields for the show chassis fabric plane-location command. Output fields are listed in the approximate order in which they appear.

Table 147: show chassis fabric plane-location Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plane n</td>
<td>Plane number.</td>
</tr>
<tr>
<td></td>
<td>(PTX Series Packet Transport Routers only) Plane numbers associated with the SIB.</td>
</tr>
<tr>
<td></td>
<td>(MX2010 and MX2020 Routers only) Plane numbers associated with the SFB.</td>
</tr>
<tr>
<td>Control Board n</td>
<td>Control board number.</td>
</tr>
<tr>
<td>SFC ABS-SIB-F13</td>
<td>(TX Matrix Plus routers only) Switch Interface Board (SIB) slot number on the F13 SIB.</td>
</tr>
<tr>
<td>SFC ABS-SIB-F2S</td>
<td>(TX Matrix Plus routers only) SIB slot number on the F2S SIB.</td>
</tr>
<tr>
<td>LCC ST-SIB-L</td>
<td>(TX Matrix Plus routers only) Line-card chassis (LCC) SIB slot number.</td>
</tr>
<tr>
<td>SFC SIB F13</td>
<td>(TX Matrix Plus routers with 3D SIBs only) Switch Interface Board (SIB) slot number on the F13 SIB.</td>
</tr>
<tr>
<td>SFC SIB F2S</td>
<td>(TX Matrix Plus routers with 3D SIBs only) SIB slot number on the F2S SIB.</td>
</tr>
<tr>
<td>LCC SIB</td>
<td>(TX Matrix Plus routers with 3D SIBs only) Line-card chassis (LCC) SIB slot number.</td>
</tr>
<tr>
<td>SIB</td>
<td>(PTX Series Packet Transport Routers only) SIB number.</td>
</tr>
<tr>
<td>Switch Fabric Board n</td>
<td>(MX2010 and MX2020 Routers only) SFB number.</td>
</tr>
</tbody>
</table>
### Sample Output

#### show chassis fabric plane-location (M120 Router)

```
user@host> show chassis fabric plane-location
------------Fabric Plane Locations-------------
Plane 0     Control Board 0
Plane 1     Control Board 0
Plane 2     Control Board 1
Plane 3     Control Board 1
```

#### show chassis fabric plane-location (MX240 and MX480 Routers)

```
user@host> show chassis fabric plane-location
------------Fabric Plane Locations-------------
Plane 0     Control Board 0
Plane 1     Control Board 0
Plane 2     Control Board 0
Plane 3     Control Board 0
Plane 4     Control Board 1
Plane 5     Control Board 1
Plane 6     Control Board 1
Plane 7     Control Board 1
```

#### show chassis fabric plane-location (MX960 Router)

```
user@host> show chassis fabric plane-location
------------Fabric Plane Locations-------------
Plane 0     Control Board 0
Plane 1     Control Board 0
Plane 2     Control Board 1
Plane 3     Control Board 1
Plane 4     Control Board 2
Plane 5     Control Board 2
```

#### show chassis fabric plane-location (MX2010 Router)

```
user@host> show chassis fabric plane-location
------------Fabric Plane Locations-------------
Plane 0     Switch Fabric Board 0
Plane 1     Switch Fabric Board 1
Plane 2     Switch Fabric Board 2
Plane 3     Switch Fabric Board 3
Plane 4     Switch Fabric Board 4
Plane 5     Switch Fabric Board 5
Plane 6     Switch Fabric Board 6
Plane 7     Switch Fabric Board 7
```

#### show chassis fabric plane-location (MX2020 Router)

```
user@host> show chassis fabric plane-location
------------Fabric Plane Locations-------------
Plane 0     Switch Fabric Board 0
Plane 1     Switch Fabric Board 1
Plane 2     Switch Fabric Board 2
Plane 3     Switch Fabric Board 3
Plane 4     Switch Fabric Board 4
Plane 5     Switch Fabric Board 5
Plane 6     Switch Fabric Board 6
Plane 7     Switch Fabric Board 7
```
### show chassis fabric plane-location (TX Matrix Plus Router)

<table>
<thead>
<tr>
<th>Plane</th>
<th>SFC ABS-SIB-F13</th>
<th>SFC ABS-SIB-F2</th>
<th>LCC ST-SIB-L</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0, 1</td>
<td>0/0, 0/2, 0/4, 0/6</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>3, 4</td>
<td>1/0, 1/2, 1/4, 1/6</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>6, 7</td>
<td>2/0, 2/2, 2/4, 2/6</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>8, 9</td>
<td>3/0, 3/2, 3/4, 3/6</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>11, 12</td>
<td>4/0, 4/2, 4/4, 4/6</td>
<td>4</td>
</tr>
</tbody>
</table>

### show chassis fabric plane-location (TX Matrix Plus Router with 3D SIBs)

<table>
<thead>
<tr>
<th>Plane</th>
<th>SFC SIB F13</th>
<th>SFC SIB F2</th>
<th>LCC SIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0, 1</td>
<td>0/0, 0/2, 0/4, 0/6</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>3, 4</td>
<td>1/0, 1/2, 1/4, 1/6</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>6, 7</td>
<td>2/0, 2/2, 2/4, 2/6</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>8, 9</td>
<td>3/0, 3/2, 3/4, 3/6</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>11, 12</td>
<td>4/0, 4/2, 4/4, 4/6</td>
<td>4</td>
</tr>
</tbody>
</table>

### show chassis fabric plane-location (EX8200 Switch)

<table>
<thead>
<tr>
<th>Plane</th>
<th>Control Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

### show chassis fabric plane-location (PTX Series Packet Transport Routers)

<table>
<thead>
<tr>
<th>SIB</th>
<th>Planes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0, 1</td>
</tr>
<tr>
<td>1</td>
<td>2, 3</td>
</tr>
<tr>
<td>2</td>
<td>4, 5</td>
</tr>
<tr>
<td>3</td>
<td>6, 7</td>
</tr>
<tr>
<td>4</td>
<td>8, 9</td>
</tr>
<tr>
<td>5</td>
<td>10, 11</td>
</tr>
<tr>
<td>6</td>
<td>12, 13</td>
</tr>
<tr>
<td>7</td>
<td>14, 15</td>
</tr>
<tr>
<td>8</td>
<td>16, 17</td>
</tr>
</tbody>
</table>
show chassis fabric summary

Syntax

show chassis fabric summary

Release Information

Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 9.4 for EX Series switches.
Command introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.

Description

(MX Series routers and EX8200 switches only) Display the state of all fabric planes and the elapsed uptime.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show chassis fabric summary (MX240 Router) on page 1008
show chassis fabric summary (MX480 Router) on page 1008
show chassis fabric summary (MX480 Router with MPC4E) on page 1008
show chassis fabric summary (MX960 Router) on page 1008
show chassis fabric summary (MX2010 Router) on page 1009
show chassis fabric summary (MX2020 Router) on page 1009
show chassis fabric summary (MX2020 Router with MPC4E) on page 1009
show chassis fabric summary (EX8200 Switch) on page 1009
show chassis fabric summary (PTX Series Packet Transport Router) on page 1010

Output Fields

Table 148 on page 1006 lists the output fields for the show chassis fabric summary command. Output fields are listed in the approximate order in which they appear.

Table 148: show chassis fabric summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plane</td>
<td>(MX Series, MX2020 and MX2010 Routers only) Plane number.</td>
</tr>
</tbody>
</table>
### Table 148: show chassis fabric summary Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>(MX Series) State of the SIB or FPC:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>—Switch Interface Board (SIB) is operational and running.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> On the Enhanced MX SCB with Trio MPC, a maximum of 4 planes are operational and running. On all the other SCBs with Trio MPC, all the planes are operational and running.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Empty</strong>—SIB is powered down.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Check</strong>—SIB is in the <strong>Check</strong> state because of the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• SIB is not inserted properly.</td>
</tr>
<tr>
<td></td>
<td>• Some destination errors are detected on the SIB. In this case, the Packet Forwarding Engine stops using the SIB to send traffic to the affected destination Packet Forwarding Engine.</td>
</tr>
<tr>
<td></td>
<td>• Some link errors are detected on the channel between the SIB and a Packet Forwarding Engine. Link errors can be detected at initialization time or runtime:</td>
</tr>
<tr>
<td></td>
<td>• Link errors caused by a link training failure at initialization time—The Packet Forwarding Engine does not use the SIB to send traffic. The <code>show chassis fabric fpcs</code> command shows <strong>Plane disabled</strong> as status for this link.</td>
</tr>
<tr>
<td></td>
<td>• Link errors caused by CRC errors detected at runtime—The Packet Forwarding Engine continues to use the SIB to send traffic. The <code>show chassis fabric fpcs</code> command shows <strong>Link error</strong> as the status for this link.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The <strong>Check</strong> state does not apply to PTX Series Packet Transport Routers because there are no SIBs in the Check state.</td>
</tr>
<tr>
<td></td>
<td>For information about link and destination errors, issue the <code>show chassis fabric fpcs</code> commands.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Spare</strong>—SIB is redundant and will move to active state if one of the working SIBs fails.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> <strong>Spare</strong> does not apply to PTX Series Packet Transport Routers because there are no spare SIBs in the device.</td>
</tr>
<tr>
<td></td>
<td>(MX2010 and MX2020 Routers) State of the SFB.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>—Switch Fabric Board (SFB) is operational and running.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Offline</strong>—Switch Fabric Board (SFB) is powered down.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Check</strong>—Switch Fabric Board (SFB) is in the check state.</td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td>(PTX Series only) Indicates whether there is any error on the SIB.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—No errors</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link Errors</strong>—Fabric link errors were found on the SIB RX link.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cell drops</strong>—Fabric cell drops were found on the SIB ASIC.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Link, Cell drops</strong>—Both Link errors and cell drops were detected on at least one of the FPC’s fabric links.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The <strong>Errors</strong> column is empty only when the FPC or SIB is offline.</td>
</tr>
</tbody>
</table>
Table 148: show chassis fabric summary Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>(MX Series, MX2010 and MX2020 Routers) Elapsed time the plane has been online.</td>
</tr>
</tbody>
</table>

Sample Output

show chassis fabric summary (MX240 Router)

```
user@host> show chassis fabric summary
Plane  State    Uptime
 0      Online   23 hours, 26 minutes, 54 seconds
 1      Online   23 hours, 26 minutes, 54 seconds
 2      Check    18 hours, 33 minutes, 42 seconds
 3      Online   23 hours, 26 minutes, 54 seconds
 4      Spare    23 hours, 26 minutes, 54 seconds
 5      Spare    23 hours, 26 minutes, 54 seconds
 6      Spare    23 hours, 26 minutes, 54 seconds
 7      Spare    23 hours, 26 minutes, 54 seconds
```

show chassis fabric summary (MX480 Router)

```
user@host> show chassis fabric summary
Plane  State    Uptime
 0      Online   8 hours, 45 minutes, 29 seconds
 1      Online   8 hours, 45 minutes, 28 seconds
 2      Online   8 hours, 45 minutes, 28 seconds
 3      Online   8 hours, 45 minutes, 28 seconds
 4      Spare    8 hours, 45 minutes, 28 seconds
 5      Spare    8 hours, 45 minutes, 28 seconds
 6      Spare    8 hours, 45 minutes, 28 seconds
 7      Check    6 hours, 10 minutes, 12 seconds
```

show chassis fabric summary (MX480 Router with MPC4E)

```
user@host > show chassis fabric summary
Plane  State    Uptime
 0      Online   6 hours, 57 minutes, 44 seconds
 1      Online   6 hours, 57 minutes, 40 seconds
 2      Online   6 hours, 57 minutes, 39 seconds
 3      Online   6 hours, 57 minutes, 34 seconds
 4      Spare    6 hours, 57 minutes, 34 seconds
 5      Spare    6 hours, 57 minutes, 29 seconds
 6      Spare    6 hours, 57 minutes, 29 seconds
 7      Spare    6 hours, 57 minutes, 24 seconds
```

Note:
For FPC slots with MPC Type 4 or MCC:
Fabric planes 1 and 5, 3 and 7 use shared physical links.
Those slots may run in a reduced bandwidth in case both plane 1 and 5, or both 3 and 7 are active.

show chassis fabric summary (MX960 Router)

```
user@host> show chassis fabric summary
Plane  State    Uptime
 0      Online   3 hours, 7 minutes, 9 seconds
 1      Online   3 hours, 7 minutes, 4 seconds
```
show chassis fabric summary (MX2010 Router)

```
user@host> show chassis fabric summary
Plane   State       Uptime
0       Online     1 day, 13 hours, 20 minutes, 10 seconds
1       Online     1 day, 13 hours, 19 minutes, 59 seconds
2       Offline    
3       Online     1 day, 13 hours, 19 minutes, 49 seconds
4       Online     1 day, 13 hours, 19 minutes, 28 seconds
5       Check      1 day, 13 hours, 19 minutes, 17 seconds
6       Online     1 day, 13 hours, 19 minutes, 6 seconds
7       Online     1 hour, 43 minutes, 5 seconds
```

show chassis fabric summary (MX2020 Router)

```
user@host> show chassis fabric summary
Plane   State       Uptime
0       Online     8 hours, 24 minutes, 1 second
1       Online     8 hours, 47 minutes, 54 seconds
2       Online     8 hours, 47 minutes, 44 seconds
3       Online     8 hours, 47 minutes, 33 seconds
4       Online     8 hours, 47 minutes, 22 seconds
5       Online     8 hours, 47 minutes, 12 seconds
6       Online     8 hours, 47 minutes, 1 second
7       Online     8 hours, 46 minutes, 50 seconds
```

show chassis fabric summary (MX2020 Router with MPC4E)

```
user@host > show chassis fabric summary
Plane   State       Uptime
0       Online     3 days, 6 hours, 58 minutes, 29 seconds
1       Online     3 days, 6 hours, 58 minutes, 18 seconds
2       Online     3 days, 6 hours, 58 minutes, 8 seconds
3       Online     3 days, 6 hours, 57 minutes, 57 seconds
4       Online     3 days, 6 hours, 57 minutes, 46 seconds
5       Online     3 days, 6 hours, 57 minutes, 36 seconds
6       Online     3 days, 6 hours, 57 minutes, 25 seconds
7       Online     3 days, 6 hours, 57 minutes, 14 seconds
```

show chassis fabric summary (EX8200 Switch)

```
user@host> show chassis fabric summary
Plane   State       Uptime
0       Online     12 days, 50 minutes, 54 seconds
1       Online     12 days, 50 minutes, 53 seconds
2       Online     12 days, 50 minutes, 53 seconds
3       Online     12 days, 50 minutes, 52 seconds
4       Spare      12 days, 50 minutes, 49 seconds
5       Spare      12 days, 50 minutes, 47 seconds
6       Spare      12 days, 50 minutes, 47 seconds
7       Spare      12 days, 50 minutes, 46 seconds
8       Online     12 days, 50 minutes, 52 seconds
9       Online     12 days, 50 minutes, 50 seconds
10      Online     12 days, 50 minutes, 50 seconds
11      Online     12 days, 50 minutes, 49 seconds
```
## show chassis fabric summary (PTX Series Packet Transport Router)

<table>
<thead>
<tr>
<th>FRU</th>
<th>State</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIB0</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>SIB1</td>
<td>Online</td>
<td>Link Errors</td>
</tr>
<tr>
<td>SIB2</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>SIB3</td>
<td>Online</td>
<td>Cell drops</td>
</tr>
<tr>
<td>SIB4</td>
<td>Offline</td>
<td></td>
</tr>
<tr>
<td>SIB5</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>SIB6</td>
<td>Online</td>
<td>Link, Cell drops</td>
</tr>
<tr>
<td>SIB7</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>SIB8</td>
<td>Online</td>
<td>Link, Cell drops</td>
</tr>
<tr>
<td>FPC0</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>FPC1</td>
<td>Online</td>
<td>Link Errors</td>
</tr>
<tr>
<td>FPC2</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>FPC3</td>
<td>Offline</td>
<td></td>
</tr>
<tr>
<td>FPC4</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>FPC5</td>
<td>Online</td>
<td>None</td>
</tr>
<tr>
<td>FPC6</td>
<td>Empty</td>
<td></td>
</tr>
<tr>
<td>FPC7</td>
<td>Empty</td>
<td></td>
</tr>
</tbody>
</table>
show chassis fpc

Syntax
show chassis fpc
<detail <slot>> | <pic-status <slot>>

Syntax (EX Series Switches)
show chassis fpc
<detail <fpc-slot>> | <pic-status <fpc-slot>>

Syntax (T4000 Routers)
show chassis fpc
<detail <fpc-slot>>
<pic-status <fpc-slot>>

Syntax (TX Matrix and TX Matrix Plus Routers)
show chassis fpc
<detail <fpc-slot>> | <pic-status <fpc-slot>>
<slot>

Syntax (MX Series Routers and EX Series switches)
show chassis fpc
<detail <slot>> | <pic-status <slot>>
<all-members>
<local>
<member member-id>

Syntax (MX104, MX2010, and MX2020 3D Universal Edge Routers)
show chassis fpc
<slot> detail | <detail <slot>> | <pic-status <slot>>
<fpc-slot>

Syntax (QFX Series)
show chassis fpc
<detail>
<interconnect-device name <fpc-slot fpc-slot>>
<node-device name>

Syntax (PTX Series Packet Transport Routers)
show chassis fpc
<detail <fpc-slot>> | <pic-status <fpc-slot>>
<fpc-slot>

Syntax (ACX Series Universal Access Routers)
show chassis fpc
<detail <fpc-slot>> | <pic-status <fpc-slot>>
<fpc-slot>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series.
Command introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.
Command introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.
Description: Display status information about the installed Flexible PIC Concentrators (FPCs) and PICs.

Options: none—Display status information for all FPCs. On a TX Matrix router, display status information for all FPCs on the attached T640 routers in the routing matrix. On a TX Matrix Plus router, display status information for all FPCs on the attached routers in the routing matrix.

NOTE: In EX8200 switches, line cards initialize Packet Forwarding Engine during startup. If an error occurs during hardware initialization, the FPCs with bad hardware parts power down after transferring the debug information to the Routing Engine. The Routing Engine marks the FPC offline, logs the error in system log messages (/var/log/messages), and generates an alarm to inform the user.

See the following sample output:

```
user@host> show chassis fpc

Temp  CPU Utilization (%)   Memory
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap Buffer
0 Empty
1 Empty
2 Empty
3 Empty
4 Empty
5 Offline         ---Hard FPC error---
6 Empty
7 Online            26      4          0       1024        0
32

The following sample output shows the alarm raised for the failed FPCs.

user@host > show chassis alarms
4 alarms currently active
Alarm time               Class  Description
2011-03-24 00:52:51 UTC  Major  FPC 5 Hard errors
2011-03-24 00:52:31 UTC  Major  Fan Tray Failure
2011-03-24 00:52:31 UTC  Major  Fan Tray Failure
2011-03-24 00:51:26 UTC  Minor  Loss of communication with Backup RE
```
NOTE: On T4000 routers, when you include the enhanced-mode statement at the [edit chassis network-services] hierarchy level and reboot the system, only the T4000 Type 5 FPCs present on the router become online while the remaining FPCs are offline, and FPC misconfiguration alarms are generated. The show chassis alarm command output displays FPC misconfiguration (FPC fpc-slot misconfig) as the reason for the generation the alarms.

The following sample output shows the FPC status after the enhanced-mode statement is configured on the T4000 router. The T4000 Type 5 FPC present in slot 5 becomes online while the remaining FPCs are offline.

```
user@host> show chassis fpc
Temp CPU Utilization (%) Memory
Slot State (C) Total Interrupt DRAM (MB) Heap Buffer
0 offline ---FPC misconfiguration---
1 offline ---FPC misconfiguration---
2 offline ---FPC misconfiguration---
3 Empty
4 Empty
5 Online 66 50 0 2816 29
27
```

The following sample output shows FPC misconfiguration alarms.

```
user@host > show chassis alarms
3 alarms currently active
Alarm time            Class Description
2011-03-24 00:52:51 PST  Major  FPC 1 misconfig
2011-03-24 00:52:31 PST  Major  FPC 2 misconfig
2011-03-24 00:52:31 PST  Major  FPC 3 misconfig
```

detail—(Optional) Display detailed status information for all FPCs or for the FPC in the specified slot (see fpc-slot or slot).

all-members—(MX Series routers and EX Series switches only) (Optional) Display status information for all FPCs on all members of the Virtual Chassis configuration.

interconnect-device name—(QFabric systems only) (Optional) Display status information for all FPCs on the Interconnect device.

fpc-slot—(Optional) FPC slot number:
- (TX Matrix and TX Matrix Plus router only—On a TX Matrix router, if you specify the number of the T640 router (line-card chassis) by using the lcc number option (the recommended method), replace fpc-slot with a value from 0 through 7. Otherwise, replace fpc-slot with a value from 0 through 31. Likewise, on a TX Matrix Plus router, if you specify the number of the specified router (line-card chassis)
by using the lcc number option (the recommended method), replace fpc-slot with a value from 0 through 7. Otherwise, replace fpc-slot with a value from 0 through 31. For example, the following commands have the same result:

user@host> show chassis fpc detail 1 lcc 1
user@host> show chassis fpc detail 9

- M120 router—Replace fpc-slot with a value from 0 through 5.
- MX80 router—Replace fpc-slot with a value from 0 through 1.
- MX104 router—Replace fpc-slot with a value from 0 through 2.
- MX240 router—Replace fpc-slot with a value from 0 through 2.
- MX480 router—Replace fpc-slot with a value from 0 through 5.
- MX-960 router—Replace fpc-slot with a value from 0 through 11.
- MX2010 router—Replace fpc-slot-number with a value from 0 through 9.
- MX2020 router—Replace fpc-slot-number with a value from 0 through 19.
- Other routers—Replace fpc-slot with a value from 0 through 7.

- EX Series switches:
  - EX3200 switches and EX4200 standalone switches—Replace fpc-slot with 0.
  - EX4200 switches in a Virtual Chassis configuration—Replace fpc-slot with a value from 0 through 9.
  - EX6210 switches—Replace fpc-slot with a value from 0 through 9.
  - EX8208 switches—Replace fpc-slot with a value from 0 through 7.
  - EX8216 switches—Replace fpc-slot with a value from 0 through 15.

- QFX Series:
  - QFX3500 switches—Replace fpc-slot with 0.
  - QFabric systems—Replace fpc-slot with 0 through 31 on the Interconnect device.

- PTX Series Packet Transport Routers:
  - PTX5000 Packet Transport Router—Replace fpc-slot with a value from 0 through 7.

- ACX Series Universal Access Routers:
  - ACX1000 and ACX2000 Universal Access Routers—Replace fpc-slot with 0.

local—(MX Series routers and EX Series switches only) (Optional) Display status information for all FPCs on the local Virtual Chassis member.

member member-id—(MX Series routers and EX Series switches only) (Optional) Display status information for all FPCs on the specified member of the Virtual Chassis configuration. Replace member-id with a value of 0 or 1.
node-device name—(QFabric systems only) (Optional) Display status information for each Node device. Each Node device is equivalent to an FPC.

pic-status—(Optional) Display status information for all PICs or for the PIC in the specified slot (see fpc-slot).

NOTE: On T1600 routers, Type 4 FPCs with ASICs based on the SL2.0 chipset do not support the 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (10x10GE [LAN/WAN] SFPP). If you issue the show chassis fpc command with the pic-status option, the CLI displays the string “Not Supported” for 10x10GE (LAN/WAN) SFPP PICs installed on such FPCs. The following is a sample output:

```
user@host> show chassis fpc pic-status
Slot 0   Online       E2-FPC Type 1
      PIC 0  Online       1x G/E SFP, 1000 BASE
      PIC 1  Online       Adaptive Services-II
      PIC 2  Online       1x G/E IQ, 1000 BASE
      PIC 3  Online       1x G/E IQ, 1000 BASE
Slot 1   Online       FPC Type 3-ES
      PIC 0  Present      UNUSED- Not Supported
Slot 2   Online       FPC Type 4-ES
      PIC 0  Offline      4x OC-192 SONET XFP
      PIC 1  Present      10x10GE (LAN/WAN) SFPP- Not Supported
<<<<<<
Slot 4   Offline      FPC Type 1-ES
Slot 5   Offline      FPC Type 2-ES
Slot 6   Online       E2-FPC Type 3
      PIC 0  Online       1x OC-192 SONET XFP
      PIC 1  Online       4x OC-48 SONET
      PIC 2  Online       4x OC-48 SONET
      PIC 3  Online       MultiServices 500
Slot 7   Online       FPC Type 4-ES
      PIC 0  Online       4x 10GE (LAN/WAN) XFP
      PIC 1  Online       4x 10GE (LAN/WAN) XFP
```

In addition, an entry is logged in the system log messages (/var/log/messages) that the PIC is not supported. The following is a sample message logged in the system log:

```
Apr 5 08:47:36 router1 chassisd[2770]: CHASSISD_UNSUPPORTED_PIC: PIC 1 in FPC 2 (type 763, version 257) is not supported
```

If you see this issue, contact Juniper Networks Technical Assistance Center (JTAC) for a possible fix. For more information about this issue and a possible solution, see PSN-2010-03-696.
NOTE: When there is a double-bit ECC error in a network processor’s memory, the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP or Channelized E1/T1 Circuit Emulation MIC is switched to the offline state.

```
user@host> show chassis fpc pic-status
Slot 1   Online       MPC Type 2 3D Q
PIC 0  Offline      1xCOC12/4xCOC3 CH-CE- ECC error detected
```

`lcc number`—(TX Matrix router and TX Matrix Plus router only) (Optional) Line-card chassis number.

Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**Required Privilege Level**: `view`

**Related Documentation**
- `request chassis fpc` on page 749
- `show chassis fpc-feb-connectivity`
- `show chassis fabric fcps on page 916`
- `Configuring the Junos OS to Resynchronize FPC Sequence Numbers with Active FPCs when an FPC Comes Online`
- `MX960 Flexible PIC Concentrator Description`
- `ACX2000 and ACX2100 Routers Hardware and CLI Terminology Mapping`
- `enhanced-mode`

**List of Sample Output**
- `show chassis fpc (EX6210 Switch)` on page 1020
- `show chassis fpc (M10 Router)` on page 1020
- `show chassis fpc (M20 Router)` on page 1020
- `show chassis fpc detail (M Series Routers)` on page 1020
- `show chassis fpc detail (MX80 Router)` on page 1021
- `show chassis fpc (MX104 Router)` on page 1021
- `show chassis fpc detail (MX104 Router)` on page 1021
- `show chassis fpc pic-status (MX104 Router)` on page 1022
show chassis fpc (MX240 Router) on page 1022
show chassis fpc (EX Series Switch) on page 1022
show chassis fpc (MX480 Router) on page 1022
show chassis fpc (MX480 Router with 100-Gigabit Ethernet CFP) on page 1022
show chassis fpc (MX480 Router with 100-Gigabit Ethernet CFP) on page 1022
show chassis fpc pic-status (EX Series Switch) on page 1023
show chassis fpc (MX480 Router with MPC4E) on page 1023
show chassis fpc detail (MX480 Router with MPC4E) on page 1023
show chassis fpc (MX480 Router with MPC4E) on page 1024
show chassis fpc detail (MX480 Router with MPC4E) on page 1024
show chassis fpc (MX960 Router) on page 1024
show chassis fpc (MX240, MX480, MX960 Routers with Application Services Modular Line Card) on page 1025
show chassis fpc (MX240, MX480, MX960 with Application Services Modular Line Card) on page 1025
show chassis fpc (MX2010 Routers) on page 1025
show chassis fpc (MX2020 Routers) on page 1025
show chassis fpc (MX2020 Router with MPC4E) on page 1026
show chassis fpc detail (MX2020 Router with MPC4E) on page 1026
show chassis fpc detail (MX Series Routers) on page 1027
show chassis fpc detail (EX Series Switches) on page 1027
show chassis fpc (Hardware Not Supported) on page 1027
show chassis fpc detail (Hardware Not Supported) on page 1028
show chassis fpc pic-status on page 1028
show chassis fpc (M Series Routers) on page 1028
show chassis fpc pic-status (MX240, MX480, and MX960 Routers with Application Services Modular Line Card) on page 1029
show chassis fpc lcc (TX Matrix Router) on page 1029
show chassis fpc pic-status (TX Matrix Router) on page 1029
show chassis fpc pic-status lcc (TX Matrix Router) on page 1030
show chassis fpc (TX Matrix Plus Router) on page 1030
show chassis fpc lcc (TX Matrix Plus Router) on page 1031
show chassis fpc detail (TX Matrix Plus Router) on page 1031
show chassis fpc pic-status (TX Matrix Plus Router) on page 1033
show chassis fpc (TI600 Router) on page 1034
show chassis fpc detail (TI600 Router) on page 1034
show chassis fpc (EX Series Switch) on page 1035
show chassis fpc slot (TI600 Router) on page 1035
show chassis fpc pic-status (TI600 Router) on page 1035
show chassis fpc (T4000 Router) on page 1036
show chassis fpc detail (T4000 Router) on page 1036
show chassis fpc pic-status (T4000 Router) on page 1037
show chassis fpc (QFX Series) on page 1037
show chassis fpc detail (QFX3500 Switches) on page 1037
show chassis fpc pic-status (QFX3500 Switches) on page 1037
show chassis fpc interconnect-device (QFabric System) on page 1037
show chassis fpc interconnect-device (QFabric System) on page 1038
show chassis fpc interconnect-device detail (QFabric System) on page 1038
Output Fields

Table 149 on page 1018 lists the output fields for the `show chassis fpc` command. Output fields are listed in the approximate order in which they appear.

Table 149: show chassis fpc Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot or Slot State</td>
<td>Slot number and state. The state can be one of the following conditions:</td>
<td>all levels</td>
</tr>
<tr>
<td></td>
<td>• Dead—Held in reset because of errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Diag—Slot is being ignored while the FPC is running diagnostics.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dormant—Held in reset.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Empty—No FPC is present.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Offline—(PTX Series Packet Transport Routers only) One of the following two states is displayed:</td>
<td>all levels</td>
</tr>
<tr>
<td></td>
<td>• FPC offline due to unreachable destinations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FPC Offline due to degraded FPC action</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Online—FPC is online and running.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Present—FPC is detected by the chassis daemon but either is not supported by the current version of Junos OS or is inserted in the wrong slot. The output also states either Hardware Not Supported or Hardware Not In Right Slot. The FPC is coming up but not yet online.</td>
<td>all levels</td>
</tr>
<tr>
<td></td>
<td>• Probed—Probe is complete; awaiting restart of the Packet Forwarding Engine.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Probe-wait—Waiting to be probed.</td>
<td></td>
</tr>
<tr>
<td>Logical slot</td>
<td>Slot number.</td>
<td>all levels</td>
</tr>
<tr>
<td>Temp (C) or Temperature</td>
<td>Temperature of the air passing by the FPC, in degrees Celsius or in both Celsius and Fahrenheit.</td>
<td>all levels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all levels</td>
</tr>
</tbody>
</table>
Table 149: show chassis fpc Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Temperature (PTX Series)</strong></td>
<td>On PTX Series Packet Transport Routers, temperature details are provided in degrees Celsius and Fahrenheit. Output includes:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Temperature (PMB)—Temperature of the air passing by the Processor Mezzanine Board (PMB) at the bottom of the FPC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Temperature (Intake)—Temperature of the air flowing into the chassis.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Temperature (Exhaust)—Exhaust temperatures for multiple zones (Exhaust A and Exhaust B).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Temperature (TLn)—Temperature of the specified Lookup ASIC (TL) of the packet forwarding engine on the FPC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Temperature (TQn)—Temperature of the specified Queuing and Memory Interface ASIC (TQ) of the packet forwarding engine on the FPC.</td>
<td></td>
</tr>
<tr>
<td>Total CPU Utilization (%)</td>
<td>Total percentage of CPU being used by the FPC’s processor.</td>
<td>all levels</td>
</tr>
<tr>
<td>Interrupt CPU Utilization (%)</td>
<td>Of the total CPU being used by the FPC’s processor, the percentage being used for interrupts.</td>
<td>none specified</td>
</tr>
<tr>
<td>Memory DRAM (MB)</td>
<td>Total DRAM, in megabytes, available to the FPC’s processor.</td>
<td>none specified</td>
</tr>
<tr>
<td>Heap Utilization (%)</td>
<td>Percentage of heap space (dynamic memory) being used by the FPC’s processor. If this number exceeds 80 percent, there may be a software problem (memory leak).</td>
<td>none specified</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> On MX Series routers and EX Series switches in a broadband edge environment, heap utilization levels higher than 70 percent can affect unified ISSU, router stability, or scaling capability.</td>
<td></td>
</tr>
<tr>
<td>Buffer Utilization (%)</td>
<td>Percentage of buffer space being used by the FPC’s processor for buffering internal messages.</td>
<td>none specified</td>
</tr>
<tr>
<td>Total CPU DRAM</td>
<td>Amount of DRAM available to the FPC’s CPU.</td>
<td>detail</td>
</tr>
<tr>
<td>Total RLDRAM</td>
<td>Amount of reduced latency dynamic random access memory (RLDRAM) available to the FPC CPU.</td>
<td>detail</td>
</tr>
<tr>
<td>Total DDR DRAM</td>
<td>Amount of double data rate dynamic random access memory (DDR DRAM) available to the FPC CPU.</td>
<td>detail</td>
</tr>
<tr>
<td>Total SRAM</td>
<td>Amount of static RAM (SRAM) used by the FPC's CPU.</td>
<td>detail</td>
</tr>
<tr>
<td>Total SDRAM</td>
<td>Total amount of memory used for storing packets and notifications.</td>
<td>detail</td>
</tr>
<tr>
<td>I/O Manager ASICs information</td>
<td>I/O Manager version number, manufacturer, and part number.</td>
<td>detail</td>
</tr>
<tr>
<td>Start time</td>
<td>Time when the Routing Engine detected that the FPC was running.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 149: show chassis fpc Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptime</td>
<td>How long the Routing Engine has been connected to the FPC and, therefore, how long the FPC has been up and running.</td>
<td>detail</td>
</tr>
<tr>
<td>PIC type</td>
<td>(pic-status output only) Type of PIC.</td>
<td>none specified</td>
</tr>
</tbody>
</table>

Sample Output

show chassis fpc (EX6210 Switch)

```plaintext
user@switch> show chassis fpc
Slot  State     Temp (C)  CPU Utilization (%) Memory DRAM (MB) Utilization (%)
0  Empty       0      0          0         0         0          0
1  Online      7      5          0       1024        0         32
2  Empty       0      0          0         0         0          0
3  Empty       0      0          0         0         0          0
4  Online      25     17          2      2048        0         30
5  Online      25     3          0       2048        0         24
6  Online      6      5          0       1024        0         32
7  Empty       0      0          0         0         0          0
8  Empty       0      0          0         0         0          0
9  Online     8      7          0       1024        0         32
```

show chassis fpc (M10 Router)

```plaintext
user@host> show chassis fpc
FPC status:
Slot  State     Temp (C)
0  Online      27
1  Online      28
```

show chassis fpc (M20 Router)

```plaintext
user@host> show chassis fpc
FPC status:
Slot  State     Temp (C)  CPU Utilization (%) Memory DRAM (MB) Utilization (%)
0  Empty       0      0          0         0         0          0
1  Online      38     0          0         8         0          4
2  Online      35     0          0         8         0          3
3  Empty       0      0          0         0         0          0
```

show chassis fpc detail (M Series Routers)

```plaintext
user@host> show chassis fpc detail
Slot 1 information:
State               Online
Temperature          48 degrees C
Total CPU DRAM      32 MB
Total SRAM          4 MB
Total SDRAM        256 MB
I/O Manager ASIcs information      Version 2.0, Foundry IBM, Part number 0
I/O Manager ASIcs information      Version 2.0, Foundry IBM, Part number 0
```
show chassis fpc detail (MX80 Router)

user@host> show chassis fpc detail
Slot 0 information:
  State: Online
  Temperature: 47 degrees C / 116 degrees F
  Total CPU DRAM: 1024 MB
  Total SRAM: 331 MB
  Total SDRAM: 1280 MB
  Start time: 2010-02-08 12:25:33 PST
  Uptime: 2 hours, 13 minutes, 19 seconds
Slot 1 information:
  State: Online
  Temperature: 47 degrees C / 116 degrees F
  Total CPU DRAM: 1024 MB
  Total SRAM: 331 MB
  Total SDRAM: 1280 MB
  Start time: 2010-02-08 12:25:33 PST
  Uptime: 2 hours, 13 minutes, 19 seconds

show chassis fpc (MX104 Router)

user@host> show chassis fpc
Temp  CPU Utilization (%)   Memory   Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
0  Online            32     15          5       2048       22         13
1  Online            32     15          5       2048       22         13
2  Online            32     15          5       2048       22         13

show chassis fpc detail (MX104 Router)

user@host> show chassis fpc detail
Slot 0 information:
  State: Online
  Temperature: 32 (C)
  Total CPU DRAM: 2048 MB
  Total SRAM: 403 MB
  Total SDRAM: 1316 MB
  Start time: 2013-05-23 14:39:18 IST
  Uptime: 1 hour, 20 minutes, 22 seconds
Slot 1 information:
  State: Online
  Temperature: 32 (C)
  Total CPU DRAM: 2048 MB
  Total SRAM: 403 MB
  Total SDRAM: 1316 MB
  Start time: 2013-05-23 14:39:18 IST
  Uptime: 1 hour, 20 minutes, 22 seconds
Slot 2 information:
  State: Online
  Temperature: 32 (C)
  Total CPU DRAM: 2048 MB
  Total SRAM: 403 MB
  Total SDRAM: 1316 MB
  Start time: 2013-05-23 14:39:18 IST
  Uptime: 1 hour, 20 minutes, 22 seconds
show chassis fpc pic-status (MX104 Router)

    user@host> show chassis fpc pic-status
    Slot 0   Online
    Slot 1   Online
    PIC 0 Online       10x 1GE(LAN) -E SFP
    PIC 1 Online       10x 1GE(LAN) -E SFP
    Slot 2   Online
    PIC 0 Online       4x 10GE(LAN) SFP+

show chassis fpc (MX240 Router)

    user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Usage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>34</td>
<td>6</td>
<td>1024</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>33</td>
<td>9</td>
<td>1024</td>
</tr>
</tbody>
</table>

show chassis fpc (EX Series Switch)

    user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Usage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>41</td>
<td>13</td>
<td>2048</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>42</td>
<td>12</td>
<td>2048</td>
</tr>
</tbody>
</table>

show chassis fpc (MX480 Router)

    user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Usage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>36</td>
<td>9</td>
<td>1024</td>
</tr>
<tr>
<td>2</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show chassis fpc (MX480 Router with 100-Gigabit Ethernet CFP)

    user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Usage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Online</td>
<td>33</td>
<td>4</td>
<td>2048</td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>36</td>
<td>7</td>
<td>2048</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>29</td>
<td>6</td>
<td>1024</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>33</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>36</td>
<td>7</td>
<td>2048</td>
</tr>
<tr>
<td>5</td>
<td>Online</td>
<td>34</td>
<td>31</td>
<td>2048</td>
</tr>
</tbody>
</table>

show chassis fpc pic-status (MX480 Router with 100-Gigabit Ethernet CFP)

    user@host> show chassis fpc pic-status
    Slot 1   Online       MPC Type 3
    Slot 2   Online       1X100GE CFP
    Slot 2   Online       DPCE 40x 1GE R EQ
    PIC 0 Online       10x 1GE(LAN) EQ
    PIC 1 Online       10x 1GE(LAN) EQ
    PIC 2 Online       10x 1GE(LAN) EQ
PIC 3 Online       10x 1GE(LAN) EQ
Slot 3 Online       MPC Type 3
PIC 0 Online       1X100GE CFP
PIC 2 Online       1X100GE CFP
Slot 4 Online       MPC Type 3
PIC 0 Online       1X100GE CFP
PIC 2 Online       1X100GE CFP
Slot 5 Online       MPC Type 2 3D EQ
PIC 0 Online       2x 10GE XFP
PIC 1 Online       2x 10GE XFP
PIC 2 Online       10x 1GE(LAN) SFP
PIC 3 Online       10x 1GE(LAN) SFP

show chassis fpc pic-status (EX Series Switch)

user@host> show chassis fpc pic-status
Slot 1 Online       EX9200 32x10G SFP
PIC 0 Online       8X10GE SFPP
PIC 1 Online       8X10GE SFPP
PIC 2 Online       8X10GE SFPP
PIC 3 Online       8X10GE SFPP
Slot 2 Online       EX9200 32x10G SFP
PIC 0 Online       8X10GE SFPP
PIC 1 Online       8X10GE SFPP
PIC 2 Online       8X10GE SFPP
PIC 3 Online       8X10GE SFPP

show chassis fpc (MX480 Router with MPC4E)

user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>38</td>
<td>7</td>
<td>2048</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>39</td>
<td>8</td>
<td>2048</td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>39</td>
<td>7</td>
<td>2048</td>
</tr>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show chassis fpc detail (MX480 Router with MPC4E)

user@host> show chassis fpc detail
Slot 2 information:
State               Online
Temperature         38
Total CPU DRAM      2048 MB
Total RLDRAM        1016 MB
Total DDR DRAM      11264 MB
Start time:         2013-02-18 05:06:57 PST
Uptime:             17 hours, 41 minutes, 9 seconds
Max Power Consumption 610 Watts

Slot 3 information:
State               Online
Temperature         38
Total CPU DRAM      2048 MB
Total RLDRAM        1016 MB
Total DDR DRAM      11264 MB
Start time:         2013-02-18 05:07:00 PST
Uptime:             17 hours, 41 minutes, 6 seconds
Max Power Consumption 610 Watts

Slot 4 information:
State               Diagnostics
Temperature                        37
Total CPU DRAM                      0 MB
Total RLDRAM                        0 MB
Total DDR DRAM                      0 MB
Max Power Consumption             520 Watts

show chassis fpc (MX480 Router with MPC4E)

user@host> show chassis fpc

Slot  State            (C)  Temp CPU Utilization (%)   Memory    Utilization (%)
0 Empty
1 Empty
2 Online            38      7          0       2048       19         14
3 Online            39      8          0       2048       18         14
4 Online            39      7          0       2048       17         14
5 Empty

show chassis fpc detail (MX480 Router with MPC4E)

user@host> show chassis fpc detail

Slot 2 information:
State                                 Online
Temperature                        38
Total CPU DRAM                   2048 MB
Total RLDRAM                     1036 MB
Total DDR DRAM                   11264 MB
Start time:                           2013-02-18 05:06:57 PST
Uptime:                               17 hours, 41 minutes, 9 seconds
Max Power Consumption             610 Watts

Slot 3 information:
State                                 Online
Temperature                        38
Total CPU DRAM                   2048 MB
Total RLDRAM                     1036 MB
Total DDR DRAM                   11264 MB
Start time:                           2013-02-18 05:07:00 PST
Uptime:                               17 hours, 41 minutes, 6 seconds
Max Power Consumption             610 Watts

Slot 4 information:
State                                 Diagnostics
Temperature                        37
Total CPU DRAM                      0 MB
Total RLDRAM                        0 MB
Total DDR DRAM                      0 MB
Max Power Consumption             520 Watts

show chassis fpc (MX960 Router)

user@host> show chassis fpc

Slot  State            (C)  Temp CPU Utilization (%)   Memory    Utilization (%)
0 Empty
1 Empty
2 Empty
3 Online       25     19          0       1024       15         57
4 Empty
5 Online       26     27          0       1024       15         57
6 Empty
7 Empty
8 Empty
9 Empty
show chassis fpc (MX240, MX480, MX960 Routers with Application Services Modular Line Card)

```
user@host> show chassis fpc 1
            Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot  State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
 1  Online            34      5          0       3072        5         13
```

show chassis fpc (MX240, MX480, MX960 with Application Services Modular Line Card)

```
user@host> show chassis fpc 1 detail
Slot 1 information:
State                                 Online
Temperature                        34
Total CPU DRAM                     3072 MB
Total RLDRAM                       259 MB
Total DDR DRAM                     4864 MB
Start time:                           2012-06-19 10:51:43 PDT
Uptime:                               16 minutes, 48 seconds
Max Power Consumption             550 Watts
```

show chassis fpc (MX2010 Routers)

```
user@host> show chassis fpc
            Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot  State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
 0  Online            34      9          0       2048       18         13
 1  Online            32      9          0       2048       15         13
 2  Empty
 3  Empty
 4  Empty
 5  Empty
 6  Empty
 7  Empty
 8  Online            31     13          0       2048       11         13
 9  Online            33     10          0       2048       18         13
```

show chassis fpc (MX2020 Routers)

```
user@host> show chassis fpc
            Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot  State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
 0  Online            10     12          0       2048       18         13
 1  Online            10     9          0       2048       18         13
 2  Online            10     9          0       2048       18         13
 3  Online            10     9          0       2048       18         13
 4  Online            10     9          0       2048       18         13
 5  Online            10     9          0       2048       18         13
 6  Online            10     9          0       2048       18         13
 7  Online            10     9          0       2048       18         13
 8  Online            10     9          0       2048       18         13
 9  Online            10     9          0       2048       18         13
10  Online           16     8          0       2048       18         13
11  Online           11     10         0       2048       18         13
12  Online           10     10         0       2048       18         13
13  Online           11     9          0       2048       18         13
14  Online           12     10         0       2048       18         13
15  Online           13     9          0       2048       18         13
16  Online           13     9          0       2048       18         13
17  Online           12     9          0       2048       18         13
```
show chassis fpc (MX2020 Router with MPC4E)

user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Online</td>
<td>33</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Online</td>
<td>31</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Online</td>
<td>32</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Online</td>
<td>28</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Online</td>
<td>38</td>
<td>8</td>
<td>0</td>
</tr>
</tbody>
</table>

show chassis fpc detail (MX2020 Router with MPC4E)

user@host> show chassis fpc detail

Slot 0 information:
- State: Online
- Temperature: 34
- Total CPU DRAM: 2048 MB
- Total RLDRAM: 806 MB
- Total DDR DRAM: 2632 MB
- Start time: 2013-02-17 08:17:35 PST
- Uptime: 1 day, 14 hours, 50 minutes, 39 seconds
- Max Power Consumption: 368 Watts

Slot 9 information:
- State: Online
- Temperature: 32
- Total CPU DRAM: 2048 MB
- Total RLDRAM: 806 MB
- Total DDR DRAM: 2632 MB
- Start time: 2013-02-17 08:17:43 PST
- Uptime: 1 day, 14 hours, 50 minutes, 31 seconds
- Max Power Consumption: 368 Watts

Slot 10 information:
- State: Online
- Temperature: 37
- Total CPU DRAM: 2048 MB
- Total RLDRAM: 1036 MB
- Total DDR DRAM: 6656 MB
- Start time: 2013-02-17 08:17:54 PST
- Uptime: 1 day, 14 hours, 50 minutes, 20 seconds
- Max Power Consumption: 520 Watts

Slot 14 information:
- State: Online
Temperature                        32
Total CPU DRAM                   2048 MB
Total RLDRAM                     1036 MB
Total DDR DRAM                   11264 MB
Start time:                           2013-02-17 08:18:01 PST
Uptime:                               1 day, 14 hours, 50 minutes, 13 seconds
Max Power Consumption             610 Watts
Slot 19 information:
  State                                 Online
  Temperature                        38
  Total CPU DRAM                   2048 MB
  Total RLDRAM                     1324 MB
  Total DDR DRAM                   5120 MB
  Start time:                           2013-02-17 08:18:08 PST
  Uptime:                               1 day, 14 hours, 50 minutes, 6 seconds
  Max Power Consumption             440 Watts

show chassis fpc detail (MX Series Routers)

user@host> show chassis fpc detail 2
Slot 0 information:
  State                                 Online
  Temperature                        36 degrees C / 96 degrees F
  Total CPU DRAM                   1024 MB
  Total RLDRAM                      256 MB
  Total DDR DRAM                   4096 MB
  Start time:                           2009-08-11 21:20:30 PDT
  Uptime:                               2 hours, 8 minutes, 50 seconds
  Max Power Consumption             335 Watts

show chassis fpc detail (EX Series Switches)

user@host> show chassis fpc detail 2
Slot 1 information:
  State                                 Online
  Temperature                        41
  Total CPU DRAM                   2048 MB
  Total RLDRAM                     1036 MB
  Total DDR DRAM                   11264 MB
  Start time:                           2013-04-02 00:04:52 PDT
  Uptime:                               7 days, 9 hours, 47 minutes, 46 seconds
  Max Power Consumption             610 Watts
Slot 2 information:
  State                                 Online
  Temperature                        41
  Total CPU DRAM                   2048 MB
  Total RLDRAM                     1036 MB
  Total DDR DRAM                   11264 MB
  Start time:                           2013-04-02 00:04:56 PDT
  Uptime:                               7 days, 9 hours, 47 minutes, 42 seconds
  Max Power Consumption             610 Watts

show chassis fpc (Hardware Not Supported)

user@host> show chassis fpc
show chassis fpc
  Slot State    Temp  CPU Utilization (%)   Memory    Utilization (%)   (C) Total Interrupt  DRAM (MB) Heap Buffer
  0  Online  -------------------- CPU less FPC --------------------
  1  Present      ----- Hardware Not In Right Slot ------
  2  Online        0        0        0        0        0
  3  Present      ----- Hardware Not Supported ------
show chassis fpc detail (Hardware Not Supported)

user@host> show chassis fpc detail
Slot 0 information:
  State: Online
  Total CPU DRAM: ---- CPU less FPC ----
  Start time: 2006-07-07 03:21:00 UTC
  Uptime: 27 minutes, 51 seconds
Slot 1 information:
  State: Present
  Reason: --- Hardware Not In Right Slot ---
Slot 2 information:
  State: Online
  Total CPU DRAM: 32 MB
  Start time: 2006-07-07 03:20:59 UTC
  Uptime: 27 minutes, 52 seconds
Slot 3 information:
  State: Present
  Reason: --- Hardware Not Supported ---
  Total CPU DRAM: 0 MB
Slot 6 information:
  State: Online
  Total CPU DRAM: 32 MB
  Start time: 2006-07-07 03:21:01 UTC
  Uptime: 27 minutes, 50 seconds

show chassis fpc pic-status

user@host> show chassis fpc pic-status
Slot 0 Online
  PIC 1  1x OC-12 ATM, MM
  PIC 2  1x OC-12 ATM, MM
  PIC 3  1x OC-12 ATM, MM
Slot 1 Online
  PIC 0  1x OC-48 SONET, SMIR
Slot 2 Online
  PIC 0  1x OC-192 SONET, SMSR

show chassis fpc pic-status (M Series Routers)

user@host> show chassis fpc pic-status
Slot 1 Online  FPC Type 1
  PIC 0  Present  2x OC-3 ATM, MM- Hardware Error
  PIC 1  Online  4x OC-3 SONET, SMIR
Slot 2 Online  E-FPC Type 2
  PIC 0  Online  4x G/E, 1000 BASE-SX
  PIC 1  Online  2x G/E SFP, 1000 BASE
  PIC 3  Online  1x Tunnel
Slot 3 Online  E-FPC Type 1
  PIC 0  Online  1x G/E IQ, 1000 BASE
  PIC 2  Online  1x G/E SFP, 1000 BASE
Slot 4 Online  E-FPC Type 2
  PIC 0  Online  4x G/E SFP, 1000 BASE
  PIC 1  Online  4x G/E SFP, 1000 BASE
  PIC 2  Online  4x G/E SFP, 1000 BASE
  PIC 3  Online  4x G/E SFP, 1000 BASE
Slot 5  Online       FPC Type 2

show chassis fpc pic-status (M120 Router)

    user@host> show chassis fpc pic-status
    Slot 1  Online       M120 CFPC 10GE
        PIC 0  Online       1x 10GE(LAN/WAN) XFP
    Slot 3  Online       M120 FPC Type 2 (proto)
        PIC 0  Online       2x G/E IQ, 1000 BASE
        PIC 1  Online       4x OC-3 SONET, SMIR
        PIC 2  Online       2x G/E IQ, 1000 BASE
        PIC 3  Online       8x 1GE(LAN), IQ2
    Slot 4  Online       M120 FPC Type 3 (proto)
        PIC 0  Online       10x 1GE(LAN), 1000 BASE
    Slot 5  Online       M120 FPC Type 1 (proto)
        PIC 0  Present      1x G/E, 1000 BASE-LX- Not Supported
        PIC 1  Online       1x CHOC3 IQ SONET, SMLR
        PIC 2  Online       4x CHDS3 IQ
        PIC 3  Online       1x G/E SFP, 1000 BASE

show chassis fpc pic-status (MX240, MX480, and MX960 Routers with Application Services Modular Line Card)

In the following output Slot 1 and Slot 5 are the Application Services Modular Carrier Cards (AS MCC), PIC 0 is the Application Services Modular Storage Card (AS MSC), and PIC 2 is the Application Services Modular Processing Card (AS MXC).

    user@host> show chassis fpc pic-status
    Slot 2  Online       MPC Type 1 3D Q
    Slot 1  Online       AS-MCC
        PIC 0  Online       AS-MSC
        PIC 2  Online       AS-MXC
    Slot 4  Offline      MPC 3D 16x 10GE
    Slot 5  Offline      AS-MCC

show chassis fpc lcc (TX Matrix Router)

    user@host> show chassis fpc lcc 0
    lcc0-re0:
    ---------------------------------------------------------------
    Slot  State       Temp  CPU       Utilization (%)  Memory     Utilization (%)  Buffer
            (C)  Total  Interrupt     DRAM (MB)       Heap       Buffer
    0  Empty
    1  Online   27      2          0       256         8         44
    2  Online   27      3          0       256        15         44
    3  Empty
    4  Empty
    5  Empty
    6  Empty
    7  Empty

show chassis fpc pic-status (TX Matrix Router)

    user@host> show chassis fpc pic-status
    lcc0-re0:
    ---------------------------------------------------------------
    Slot 0  Online       FPC Type 3
        PIC 0  Online       1x OC-192 SM SR1
        PIC 1  Online       1x OC-192 SM SR2
        PIC 2  Online       1x OC-192 SM SR1
        PIC 3  Online       1x Tunnel
Slot 1 Online       FPC Type 2  
PIC 0 Online       1x OC-48 SONET, SMSR  
PIC 1 Online       1x OC-48 SONET, SMSR  

lcc1-re0:

-------------------------------------------------------------------------

Slot 1 Online       FPC Type 3  
PIC 0 Online       1x OC-192 SM SR1  

Slot 5 Online       FPC Type 2  
PIC 0 Online       1x OC-48 SONET, SMSR  
PIC 1 Online       2x G/E, 1000 BASE-LX  
PIC 2 Online       2x G/E, 1000 BASE-LX  
PIC 3 Online       1x OC-48 SONET, SMSR  

lcc3-re0:

show chassis fpc pic-status lcc (TX Matrix Router)

user@host> show chassis fpc pic-status lcc 0
lcc0-re0:

-------------------------------------------------------------------------

Slot 1 Online       FPC Type 2  
PIC 0 Online       1x OC-12 ATM2 IQ, MM  
PIC 1 Online       1x OC-48 SONET, SMSR  
PIC 2 Online       1x OC-48 SONET, SMSR  
PIC 3 Online       4x G/E, 1000 BASE-SX  

show chassis fpc (TX Matrix Plus Router)

user@host> show chassis fpc
lcc0-re0:

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp (C)</th>
<th>CPU Utilization (%)</th>
<th>Memory DRAM (MB)</th>
<th>Heap Utilization (%)</th>
<th>Int</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>38</td>
<td>4</td>
<td>2048</td>
<td>3</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>43</td>
<td>8</td>
<td>2048</td>
<td>6</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>43</td>
<td>6</td>
<td>2048</td>
<td>6</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Online</td>
<td>42</td>
<td>13</td>
<td>2048</td>
<td>6</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Online</td>
<td>45</td>
<td>7</td>
<td>2048</td>
<td>3</td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>

lcc2-re0:

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp (C)</th>
<th>CPU Utilization (%)</th>
<th>Memory DRAM (MB)</th>
<th>Heap Utilization (%)</th>
<th>Int</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Online</td>
<td>42</td>
<td>10</td>
<td>2048</td>
<td>6</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>42</td>
<td>11</td>
<td>2048</td>
<td>6</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>40</td>
<td>5</td>
<td>2048</td>
<td>3</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>33</td>
<td>26</td>
<td>1024</td>
<td>8</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Online</td>
<td>43</td>
<td>8</td>
<td>2048</td>
<td>6</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Online</td>
<td>46</td>
<td>6</td>
<td>2048</td>
<td>3</td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>
### lcc3-re0:

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>39</td>
<td>2048</td>
</tr>
<tr>
<td>3</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>41</td>
<td>2048</td>
</tr>
<tr>
<td>5</td>
<td>Online</td>
<td>41</td>
<td>2048</td>
</tr>
<tr>
<td>6</td>
<td>Online</td>
<td>40</td>
<td>2048</td>
</tr>
<tr>
<td>7</td>
<td>Online</td>
<td>42</td>
<td>2048</td>
</tr>
</tbody>
</table>

### show chassis fpc lcc (TX Matrix Plus Router)

**user@host> show chassis fpc lcc 0**

### lcc0-re0:

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Online</td>
<td>38</td>
<td>2048</td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>43</td>
<td>2048</td>
</tr>
<tr>
<td>3</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Online</td>
<td>43</td>
<td>2048</td>
</tr>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Online</td>
<td>42</td>
<td>2048</td>
</tr>
<tr>
<td>7</td>
<td>Online</td>
<td>45</td>
<td>2048</td>
</tr>
</tbody>
</table>

### show chassis fpc detail (TX Matrix Plus Router)

**user@host> show chassis fpc details**

### lcc0-re0:

**Slot 1 information:**
- **State:** Online
- **Temperature:** 38 degrees C / 100 degrees F
- **Total CPU DRAM:** 2048 MB
- **Total SRAM:** 64 MB
- **Total SDRAM:** 1280 MB
- **Start time:** 2010-10-04 20:06:22 PDT
- **Uptime:** 1 hour, 32 minutes, 51 seconds

**Slot 2 information:**
- **State:** Online
- **Temperature:** 43 degrees C / 109 degrees F
- **Total CPU DRAM:** 2048 MB
- **Total SRAM:** 128 MB
- **Total SDRAM:** 2560 MB
- **Start time:** 2010-10-04 20:06:37 PDT
- **Uptime:** 1 hour, 32 minutes, 36 seconds

**Slot 4 information:**
- **State:** Online
- **Temperature:** 43 degrees C / 109 degrees F
- **Total CPU DRAM:** 2048 MB
- **Total SRAM:** 128 MB
- **Total SDRAM:** 2560 MB
- **Start time:** 2010-10-04 20:06:40 PDT
- **Uptime:** 1 hour, 32 minutes, 33 seconds

**Slot 6 information:**
State                               Online
Temperature                      42 degrees C / 107 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                      128 MB
Total SDRAM                    2560 MB
Start time                          2010-10-04 20:06:42 PDT
Uptime                              1 hour, 32 minutes, 31 seconds
Slot 7 information:
State                               Online
Temperature                      45 degrees C / 113 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:06:43 PDT
Uptime                              1 hour, 32 minutes, 30 seconds
lcc2-re0:
--------------------------------------------------------------------------
Slot 0 information:
State                               Online
Temperature                      42 degrees C / 107 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                      128 MB
Total SDRAM                    2560 MB
Start time                          2010-10-04 20:06:35 PDT
Uptime                              1 hour, 32 minutes, 38 seconds
Slot 2 information:
State                               Online
Temperature                      42 degrees C / 107 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                      128 MB
Total SDRAM                    2560 MB
Start time                          2010-10-04 20:06:37 PDT
Uptime                              1 hour, 32 minutes, 36 seconds
Slot 3 information:
State                               Online
Temperature                      40 degrees C / 104 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:06:28 PDT
Uptime                              1 hour, 32 minutes, 45 seconds
Slot 4 information:
State                               Online
Temperature                      33 degrees C / 91 degrees F
Total CPU DRAM                 1024 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:08:03 PDT
Uptime                              1 hour, 31 minutes, 10 seconds
Slot 6 information:
State                               Online
Temperature                      43 degrees C / 109 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                      128 MB
Total SDRAM                    2560 MB
Start time                          2010-10-04 20:06:44 PDT
Uptime                              1 hour, 32 minutes, 29 seconds
Slot 7 information:
State                               Online
Temperature                      46 degrees C / 114 degrees F
Total CPU DRAM  2048 MB
Total SRAM     64 MB
Total SDRAM    1280 MB
Start time     2010-10-04 20:06:46 PDT
Uptime         1 hour, 32 minutes, 27 seconds

lcc3-re0:
------------------------------------------------------------------------
Slot 2 information:
State                                   Online
Temperature                      38 degrees C / 100 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:17:31 PDT
Uptime                              1 hour, 32 minutes, 27 seconds

Slot 4 information:
State                                   Online
Temperature                      41 degrees C / 105 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:17:34 PDT
Uptime                              1 hour, 31 minutes, 42 seconds

Slot 5 information:
State                                   Online
Temperature                      41 degrees C / 105 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:17:36 PDT
Uptime                              1 hour, 31 minutes, 39 seconds

Slot 6 information:
State                                   Online
Temperature                      40 degrees C / 104 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:17:39 PDT
Uptime                              1 hour, 31 minutes, 34 seconds

Slot 7 information:
State                                   Online
Temperature                      42 degrees C / 107 degrees F
Total CPU DRAM                 2048 MB
Total SRAM                       64 MB
Total SDRAM                    1280 MB
Start time                          2010-10-04 20:17:41 PDT
Uptime                              1 hour, 31 minutes, 32 seconds

show chassis fpc pic-status (TX Matrix Plus Router)
user@host> show chassis fpc pic-status
1cc0-re0:
------------------------------------------------------------------------
Slot 1 Online   FPC Type 2-ES
   PIC 0 Online   8x 1GE(LAN), IQ2
Slot 2 Online   FPC Type 4-ES
   PIC 0 Online   4x 10GE (LAN/WAN) XFP
Slot 4 Online   FPC Type 4-ES
   PIC 0 Online   4x 10GE (LAN/WAN) XFP
### show chassis fpc (T1600 Router)

**User@host> show chassis fpc**

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp (C)</th>
<th>CPU Utilization (%)</th>
<th>Memory DRAM (MB)</th>
<th>Heap</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>49</td>
<td>3</td>
<td>0</td>
<td>2048</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>46</td>
<td>6</td>
<td>0</td>
<td>2048</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Online</td>
<td>46</td>
<td>5</td>
<td>0</td>
<td>2048</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Online</td>
<td>44</td>
<td>8</td>
<td>0</td>
<td>1024</td>
<td>7</td>
</tr>
</tbody>
</table>

### show chassis fpc detail (T1600 Router)

**User@host> show chassis fpc detail**
show chassis fpc detail
Slot 2 information:
State: Online
Temperature: 49 degrees C / 120 degrees F
Total CPU DRAM: 2048 MB
Total SRAM: 64 MB
Total SDRAM: 1280 MB
Start time: 2010-10-04 21:12:52 PDT
Uptime: 32 minutes, 9 seconds
Slot 3 information:
State: Online
Temperature: 47 degrees C / 116 degrees F
Total CPU DRAM: 2048 MB
Total SRAM: 128 MB
Total SDRAM: 2560 MB
Start time: 2010-10-04 21:13:06 PDT
Uptime: 31 minutes, 55 seconds
Slot 5 information:
State: Online
Temperature: 46 degrees C / 114 degrees F
Total CPU DRAM: 2048 MB
Total SRAM: 64 MB
Total SDRAM: 1280 MB
Start time: 2010-10-04 21:12:56 PDT
Uptime: 32 minutes, 5 seconds
Slot 7 information:
State: Online
Temperature: 44 degrees C / 111 degrees F
Total CPU DRAM: 1024 MB
Total SRAM: 64 MB
Total SDRAM: 1280 MB
Start time: 2010-10-04 21:14:34 PDT
Uptime: 30 minutes, 27 seconds

show chassis fpc <fpc-slot> (EX Series Switch)

user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp (C)</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Online</td>
<td>40</td>
<td>12</td>
<td>0</td>
</tr>
</tbody>
</table>

show chassis fpc slot (T1600 Router)

user@host> show chassis fpc slot

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp (C)</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Online</td>
<td>49</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

show chassis fpc pic-status (T1600 Router)

user@host> show chassis fpc pic-status

| Slot 2 | Online | FPC Type | PIC 0 | Online | Load Type | PIC 1 | Online | 4x 1GE (LAN), IQ2E | PIC 3 | Online | 1x OC-12-3 SFP | Slot 3 | Online | FPC Type | PIC 0 | Online | 4x 10GE (LAN/WAN) XFP | PIC 1 | Online | 4x OC-192 SONET XFP |
|--------|--------|----------|-------|--------|-----------|-------|--------|--------------------|-------|--------|------------------|--------|--------|----------|-------|--------|-------------------|-------|--------|--------------------|-------|--------|------------------|
Slot 5 Online  FPC Type 2-ES
PIC 0 Online  Load Type 2
PIC 1 Online  8x 1GE(LAN), IQ2E
PIC 2 Online  8x 1GE(LAN), IQ2E
PIC 3 Online  1x OC-48-12-3 SFP
Slot 7 Online  FPC Type 4
PIC 0 Online  4x 10GE (LAN/WAN) XFP

show chassis fpc

regress@stymphalian# run show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp (°C)</th>
<th>Total CPU Utilization (%)</th>
<th>Memory DRAM (MB)</th>
<th>Heap</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Online</td>
<td>48</td>
<td>15</td>
<td>0</td>
<td>2816</td>
<td>21</td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Online</td>
<td>51</td>
<td>15</td>
<td>0</td>
<td>2816</td>
<td>21</td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Online</td>
<td>39</td>
<td>8</td>
<td>0</td>
<td>2048</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>Online</td>
<td>49</td>
<td>15</td>
<td>0</td>
<td>2816</td>
<td>21</td>
</tr>
<tr>
<td>7</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show chassis fpc detail

regress@stymphalian# run show chassis fpc detail

Slot 0 information:
State       Online
Temperature 48 degrees C / 118 degrees F
Total CPU DRAM 2816 MB
Total SRAM 1554 MB
Total SDRAM 10752 MB
Start time  2012-02-09 22:56:25 PST
Uptime      2 hours, 40 minutes, 52 seconds

Slot 3 information:
State       Online
Temperature 51 degrees C / 123 degrees F
Total CPU DRAM 2816 MB
Total SRAM 1554 MB
Total SDRAM 10752 MB
Start time  2012-02-09 22:56:22 PST
Uptime      2 hours, 40 minutes, 55 seconds

Slot 5 information:
State       Online
Temperature 39 degrees C / 102 degrees F
Total CPU DRAM 2048 MB
Total SRAM 128 MB
Total SDRAM 2560 MB
Start time  2012-02-09 22:51:27 PST
Uptime      2 hours, 45 minutes, 50 seconds

Slot 6 information:
State       Online
Temperature 49 degrees C / 120 degrees F
Total CPU DRAM 2816 MB
Total SRAM 1554 MB
Total SDRAM 10752 MB
Start time  2012-02-09 22:56:29 PST
Uptime      2 hours, 40 minutes, 48 seconds
show chassis fpc pic-status (T4000 Router)

```begin
user@host> show chassis fpc pic-status
Slot 0 Online FPC Type 5-3D
  PIC 0 Online 12x10GE (LAN/WAN) SFPP
  PIC 1 Online 12x10GE (LAN/WAN) SFPP
Slot 3 Online FPC Type 5-3D
  PIC 0 Online 1x100GE
  PIC 1 Online 12x10GE (LAN/WAN) SFPP
Slot 5 Online FPC Type 4-ES
  PIC 0 Online 100GE
  PIC 1 Online 100GE CFP
Slot 6 Online FPC Type 5-3D
  PIC 0 Online 12x10GE (LAN/WAN) SFPP
  PIC 1 Online 12x10GE (LAN/WAN) SFPP
```

show chassis fpc (QFX Series)

```begin
user@switch> show chassis fpc
Temp CPU Utilization (%) Memory Utilization (%)
Slot State (C) Total Interrupt DRAM (MB) Heap Buffer
0 Online 26 2 0 2820 0 49
```

show chassis fpc detail (QFX3500 Switches)

```begin
user@switch> show chassis fpc detail
Slot 0 information:
  State       Online
  Temperature 28 degrees C / 82 degrees F
  Total CPU DRAM 2820 MB
  Total SRAM 0 MB
  Total SDRAM 0 MB
  Start time 2010-09-20 01:34:13 PDT
  Uptime 3 days, 3 hours, 31 minutes, 48 seconds
```

show chassis fpc pic-status (QFX3500 Switches)

```begin
user@switch> show chassis fpc pic-status
Slot 0 Online QFX 48x10G 4x40G Switch
  PIC 0 Online 48x 10G-SFP+
  PIC 1 Online 15x 10G-SFP+
```

show chassis fpc interconnect-device (QFabric System)

```begin
user@switch> show chassis fpc interconnect-device interconnect1
FPC status:
Temp
Slot State (C)
0 Online 0
1 Online 0
2 Online 0
3 Online 0
4 Online 0
5 Online 0
6 Online 0
7 Online 0
8 Online 0
9 Online 0
10 Online 0
11 Online 0
12 Online 0
```
show chassis fpc interconnect-device (QFabric System)

```bash
user@switch> show chassis fpc interconnect-device interconnect1 3
FPC status:
<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Online</td>
<td>0</td>
</tr>
</tbody>
</table>
```

show chassis fpc interconnect-device detail (QFabric System)

```bash
user@switch> show chassis fpc interconnect-device interconnect1 3 detail
Slot 3 information:
<table>
<thead>
<tr>
<th>State</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>0 degrees C / 32 degrees F</td>
</tr>
<tr>
<td>Start time</td>
<td>2011-08-18 10:45:04 PDT</td>
</tr>
<tr>
<td>Uptime</td>
<td>1 minute, 49 seconds</td>
</tr>
</tbody>
</table>
```

show chassis fpc pic-status interconnect-device (QFabric System)

```bash
user@switch> show chassis fpc pic-status interconnect-device interconnect1
Slot 0 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 1 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 2 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 3 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 4 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 5 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 6 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 7 Online QFX 16-port QSFP+ Front Card
PIC 0 Online 16x 40G-QSFP+
PIC 1 Online 16x 40G-GE
Slot 8 Online QFX Fabric Rear Card
PIC 0 Online 16x 40G-GE
Slot 9 Online QFX Fabric Rear Card
PIC 0 Online 16x 40G-GE
Slot 10 Online QFX Fabric Rear Card
PIC 0 Online 16x 40G-GE
Slot 11 Online QFX Fabric Rear Card
PIC 0 Online 16x 40G-GE
Slot 12 Online QFX Fabric Rear Card
PIC 0 Online 16x 40G-GE
Slot 13 Online QFX Fabric Rear Card
PIC 0 Online 16x 40G-GE
Slot 14 Online QFX Fabric Rear Card
PIC 0 Online 16x 40G-GE
```
show chassis fpc pic-status node-device (QFabric System)

user@switch> show chassis fpc pic-status node-device node1
Slot node1 Online QFX 48x10G 4x40G Switch
PIC 0 Online 48x 10G-SFP+
PIC 1 Online 4x 40G-QSFP+

show chassis fpc (PTX5000 Packet Transport Router)

user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp (C)</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>50</td>
<td>6</td>
<td>2816</td>
</tr>
<tr>
<td>3</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Online</td>
<td>48</td>
<td>9</td>
<td>2816</td>
</tr>
<tr>
<td>6</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Online</td>
<td>49</td>
<td>8</td>
<td>2816</td>
</tr>
</tbody>
</table>

show chassis fpc detail (PTX5000 Packet Transport Router)

user@host> show chassis fpc detail

Slot 2 information:
State: Online
Temperature: 35 degrees C / 95 degrees F (PMB)
Temperature: 35 degrees C / 95 degrees F (Intake)
Temperature: 50 degrees C / 122 degrees F (Exhaust A)
Temperature: 54 degrees C / 129 degrees F (Exhaust B)
Temperature: 54 degrees C / 129 degrees F (TL0)
Temperature: 52 degrees C / 125 degrees F (TQ0)
Temperature: 61 degrees C / 141 degrees F (TL1)
Temperature: 56 degrees C / 132 degrees F (TQ1)
Temperature: 54 degrees C / 129 degrees F (TL2)
Temperature: 56 degrees C / 132 degrees F (TQ2)
Temperature: 59 degrees C / 138 degrees F (TL3)
Temperature: 60 degrees C / 140 degrees F (TQ3)
Total CPU DRAM: 2816 MB
Total SRAM: 0 MB
Total SDRAM: 0 MB
Start time: 2012-01-12 12:05:42 PST
Uptime: 3 hours, 14 minutes, 7 seconds

Slot 5 information:
State: Online
Temperature: 35 degrees C / 95 degrees F (PMB)
Temperature: 34 degrees C / 93 degrees F (Intake)
Temperature: 48 degrees C / 118 degrees F (Exhaust A)
Temperature: 53 degrees C / 127 degrees F (Exhaust B)
Temperature: 54 degrees C / 129 degrees F (TL0)
Temperature: 52 degrees C / 125 degrees F (TQ0)
Temperature: 69 degrees C / 156 degrees F (TL1)
Temperature: 56 degrees C / 132 degrees F (TQ1)
Temperature: 54 degrees C / 129 degrees F (TL2)
Temperature: 56 degrees C / 132 degrees F (TQ2)
Temperature: 59 degrees C / 138 degrees F (TL3)
Temperature: 60 degrees C / 140 degrees F (TQ3)
Total CPU DRAM: 2816 MB
Total SRAM: 0 MB
Total SDRAM: 0 MB
Start time: 2012-01-12 12:05:43 PST
Uptime: 3 hours, 14 minutes, 6 seconds

Slot 7 information:
State: Online
Temperature: 35 degrees C / 95 degrees F (PMB)
Temperature: 33 degrees C / 91 degrees F (Intake)
Temperature: 50 degrees C / 122 degrees F (Exhaust A)
Temperature: 55 degrees C / 131 degrees F (Exhaust B)
Temperature: 56 degrees C / 132 degrees F (TLO)
Temperature: 56 degrees C / 132 degrees F (TQO)
Temperature: 61 degrees C / 141 degrees F (TLO)
Temperature: 57 degrees C / 134 degrees F (TQ1)
Temperature: 55 degrees C / 131 degrees F (TQ2)
Temperature: 59 degrees C / 138 degrees F (TQ2)
Temperature: 62 degrees C / 143 degrees F (TL3)
Temperature: 62 degrees C / 143 degrees F (TQ3)
Total CPU DRAM: 2816 MB
Total SRAM: 0 MB
Total SDRAM: 0 MB
Start time: 2012-01-12 12:05:44 PST
Uptime: 3 hours, 14 minutes, 5 seconds

show chassis fpc pic-status (PTX5000 Packet Transport Router)

user@host> show chassis fpc pic-status
Slot 2  Online     FPC
  PIC 0  Online     24x 10GE(LAN) SFP+
  PIC 1  Online     24x 10GE(LAN) SFP+
Slot 5  Online     FPC
  PIC 0  Online     24x 10GE(LAN) SFP+
  PIC 1  Online     2x 40GE CFP
Slot 7  Online     FPC
  PIC 0  Online     24x 10GE(LAN) SFP+
  PIC 1  Online     2x 40GE CFP

show chassis fpc (ACX2000 Universal Access Router)

user@host> show chassis fpc

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Online</td>
<td>61</td>
<td>17 17 6</td>
<td>512 21 37</td>
</tr>
</tbody>
</table>

show chassis fpc 0 (ACX2000 Universal Access Router)

user@host> show chassis fpc 0

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Online</td>
<td>61</td>
<td>17 17 6</td>
<td>512 21 37</td>
</tr>
</tbody>
</table>

show chassis fpc detail (ACX2000 Universal Access Router)

user@host> show chassis fpc detail
Slot 0 information:
State: Online
Temperature: 61 degrees C / 141 degrees F
Total CPU DRAM: 512 MB
Start time: 2012-05-29 02:52:06 PDT
Uptime: 27 minutes, 17 seconds
show chassis fpc pic-status (ACX2000 Universal Access Router)

user@host> show chassis fpc pic-status
Slot 0  Online
  PIC 0  Online       16x CHE1T1, RJ48
  PIC 1  Online       8x 1GE(LAN) R34S
  PIC 2  Online       2x 1GE(LAN) SFP
  PIC 3  Online       2x 10GE(LAN) SFP+

show chassis FPC1 (MX Routers with Media Services Blade [MSB])

user@switch> show chassis fpc1
Temp  CPU Utilization (%)   Memory    Utilization (%)
Slot State            (C)  Total  Interrupt      DRAM (MB) Heap     Buffer
1  Online            34      5          0       3072        5         13

show chassis FPC1 detail (MX Routers with Media Services Blade [MSB])

user@switch> show chassis fpc1 detail
Slot 1 information:
State                                 Online
Temperature                        34
Total CPU DRAM                     3072 MB
Total RLDRAM                        259 MB
Total DDR DRAM                      4864 MB
Start time:                           2012-06-19 10:51:43 PDT
Uptime:                               16 minutes, 48 seconds
Max Power Consumption              550 Watts
show chassis led

| show chassis led (EX Series) | show chassis led <fpc-slot <fpc-slot-number>> |
| show chassis led (QFX Series) | show chassis led <fpc-slot <fpc-slot-number>> interconnect-device name node-device name |

Release Information
- Command introduced in Junos OS Release 10.1 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display the status and colors of the chassis LEDs on the front panel of the switch. A major alarm (red) indicates a critical error condition that requires immediate action. A minor alarm (yellow) indicates a noncritical condition that requires monitoring or maintenance. A minor alarm that is left unchecked might cause interruption in service or performance degradation.

Options
- **none**—Display the status of the chassis status LEDs (for EX4200 switches configured as a Virtual Chassis, display the information for all Virtual Chassis members).

  - **fpc-slot <fpc-slot-number>**—(Optional) (Not on EX2200 switches) Display the information as follows:
    - (EX3200, standalone EX4200, standalone QFX3500, and EX4500 switches) Display the status of the chassis status LEDs for either an FPC slot with no fpc-slot-number value specified or for the FPC slot specified by fpc-slot 0. fpc-slot refers to the switch itself and 0 is the only valid value for fpc-slot-number. Output for these options is the same as for the none option.
    - (EX4200 switches in a Virtual Chassis with two or more members) If no fpc-slot-number value is specified, display the status of the chassis status LEDs for all members of the Virtual Chassis. Output for this option is the same as for the none option. If the fpc-slot-number value is specified (it equals the member-id value), display the status of the chassis status LEDs for the specified member.
    - (EX8200 switches)—Display the status of the chassis status LEDs for the line card in the line-card slot specified by the fpc-slot-number value.

  - **interconnect-device name**—
    - (QFabric systems only) (Optional) Display the status of the chassis and interface status LEDs for the Interconnect device.

  - **node-device name**—(QFabric systems only) (Optional) Display the status of the chassis and interface status LEDs for the Node device.

Required Privilege Level
- **view**
Related Documentation

- Chassis Status LEDs in EX2200 Switches
- Chassis Status LEDs in EX3200 Switches
- Chassis Status LEDs in EX4200 Switches
- Chassis Status LEDs in EX4500 Switches
- Chassis Status LEDs in an EX8200 Switch
- Chassis Status LEDs on a QFX3500 Device
- Chassis Status LEDs in the QFX3600 and QFX3600-I Device
- Management Port LEDs on a QFX3500 Device
- Management Port LEDs in the QFX3600 and QFX3600-I Device
- Chassis Status LEDs on a QFX3008-I Interconnect Device
- Control Board LEDs on a QFX3008-I Interconnect Device

List of Sample Output

- `show chassis led (EX2200 Switch)` on page 1046
- `show chassis led` on page 1047
- `show chassis led fpc-slot 0` on page 1047
- `show chassis led (EX Series)` on page 1048
- `show chassis led node-device (QFabric System Node Device)` on page 1049
- `show chassis led interconnect-device (QFabric System - QFX3600-I Interconnect Device)` on page 1049
- `show chassis led interconnect-device (QFabric System - QFX3008-I Interconnect Device)` on page 1050

Output Fields

Table 150 on page 1043 lists the output fields for the `show chassis led` command. Output fields are listed in the approximate order in which they appear.

**Table 150: show chassis led Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front panel contents for slot</td>
<td>FPC slot number of the device whose content is being displayed. The number is always 0, except for EX4200 switches in a Virtual Chassis, where it is the member ID value.</td>
</tr>
<tr>
<td>Front panel contents (EX8200 Switches)</td>
<td>On EX8200 switches, no slot number is displayed.</td>
</tr>
<tr>
<td>Front Panel Module Information (QFabric system QFX3008-I Interconnect device)</td>
<td>On QFabric system Node devices, the name of the Node device whose content is being displayed.</td>
</tr>
<tr>
<td>Front panel contents for (QFabric system Node devices and QFX3600-I Interconnect devices)</td>
<td>(EX Series switches only) Displays status of the ALM LED:</td>
</tr>
<tr>
<td>Alarms LED</td>
<td>- Off—No alarm has been configured.</td>
</tr>
<tr>
<td></td>
<td>- Green—No alarm has been triggered.</td>
</tr>
<tr>
<td></td>
<td>- Red—Major alarm.</td>
</tr>
<tr>
<td></td>
<td>- Yellow—Minor alarm</td>
</tr>
</tbody>
</table>
### Table 150: show chassis led Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System LED</strong></td>
<td>(EX Series switches only) Displays status of the SYS LED:</td>
</tr>
<tr>
<td></td>
<td>• Off—Switch is powered off.</td>
</tr>
<tr>
<td></td>
<td>• Green—Switch is operating normally.</td>
</tr>
<tr>
<td></td>
<td>• Yellow—Switch is booting.</td>
</tr>
<tr>
<td><strong>Master LED:</strong></td>
<td>Displays status of the MST LED (on EX3200, EX4200, and EX8200 switches):</td>
</tr>
<tr>
<td></td>
<td>• Green—On an EX4200 Virtual Chassis switch, indicates the switch is the master in</td>
</tr>
<tr>
<td></td>
<td>the Virtual Chassis configuration. On other switches, indicates that the Routing</td>
</tr>
<tr>
<td></td>
<td>Engine is operational.</td>
</tr>
<tr>
<td></td>
<td>• Off</td>
</tr>
<tr>
<td></td>
<td>• On an EX4200 Virtual Chassis switch, indicates that this switch is not the master</td>
</tr>
<tr>
<td></td>
<td>in the Virtual Chassis configuration.</td>
</tr>
<tr>
<td></td>
<td>• On EX3200, standalone EX4200, and EX8200 switches, indicates that the Routing</td>
</tr>
<tr>
<td></td>
<td>Engine is not operational.</td>
</tr>
<tr>
<td><strong>Mode LED:</strong></td>
<td>(EX Series switches only) On an EX2200 switch only, displays the currently selected</td>
</tr>
<tr>
<td></td>
<td>port parameter of the Status LED:</td>
</tr>
<tr>
<td></td>
<td>• ADM—Administrative</td>
</tr>
<tr>
<td></td>
<td>• SPD—Speed</td>
</tr>
<tr>
<td></td>
<td>• DPX—Duplex</td>
</tr>
<tr>
<td></td>
<td>• POE—Power over Ethernet</td>
</tr>
<tr>
<td><strong>Status/Beacon LED</strong></td>
<td>(QFX Series only) Displays the system status as indicated by the Status LED</td>
</tr>
<tr>
<td></td>
<td>on the chassis. For more information, see:</td>
</tr>
<tr>
<td></td>
<td>• Chassis Status LEDs on a QFX3500 Device</td>
</tr>
<tr>
<td></td>
<td>• Chassis Status LEDs in the QFX3600 and QFX3600-l Device</td>
</tr>
<tr>
<td><strong>LINK/SPEED LED</strong></td>
<td>(QFX Series only) Displays the link status and speed of a management port.</td>
</tr>
<tr>
<td></td>
<td>For more information, see:</td>
</tr>
<tr>
<td></td>
<td>• Management Port LEDs on a QFX3500 Device</td>
</tr>
<tr>
<td></td>
<td>• Management Port LEDs in the QFX3600 and QFX3600-l Device</td>
</tr>
<tr>
<td><strong>ACTIVITY LED</strong></td>
<td>(QFX Series only) Displays the activity status of a management port. For more</td>
</tr>
<tr>
<td></td>
<td>information, see:</td>
</tr>
<tr>
<td></td>
<td>• Management Port LEDs on a QFX3500 Device</td>
</tr>
<tr>
<td></td>
<td>• Management Port LEDs in the QFX3600 and QFX3600-l Device</td>
</tr>
<tr>
<td><strong>STATUS LED</strong></td>
<td>(QFX Series only) Displays the link status of an interface as indicated by the ST</td>
</tr>
<tr>
<td></td>
<td>LED. For more information, see:</td>
</tr>
<tr>
<td></td>
<td>• Control Board LEDs on a QFX3008-l Interconnect Device</td>
</tr>
<tr>
<td></td>
<td>• Access Port and Uplink Port LEDs on a QFX3500 Device</td>
</tr>
<tr>
<td></td>
<td>• Access Port and Uplink Port LEDs on a QFX3600 or QFX3600-l Device</td>
</tr>
</tbody>
</table>
Table 150: show chassis led Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINK/ACTIVITY LED</td>
<td>(QFX Series only) Displays link activity or faults on an interface as indicated by the LA LED. For more information, see:</td>
</tr>
<tr>
<td></td>
<td>• Access Port and Uplink Port LEDs on a QFX3500 Device</td>
</tr>
<tr>
<td></td>
<td>• Access Port and Uplink Port LEDs on a QFX3600 or QFX3600-I Device</td>
</tr>
<tr>
<td>Status LED</td>
<td>(QFX3008-I Interconnect device only) Displays the system status as indicated by the STATUS LED on the front panel of the chassis. For more information, see Chassis Status LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td></td>
<td>• Displays the status of a Control Board as indicated by the STATUS LED on the Control Board. For more information, see Control Board LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td>Power LED</td>
<td>(QFX3008-I Interconnect device only) Displays the status of system power on the device. For more information, see Chassis Status LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td>Major Alarm LED</td>
<td>(QFX3008-I Interconnect device only) Displays whether a critical error condition that requires immediate action exists on the device. For more information, see Chassis Status LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td>Minor Alarm LED</td>
<td>(QFX3008-I Interconnect device only) Displays whether a noncritical condition that requires monitoring or maintenance exists on the device. For more information, see Chassis Status LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td>Fan 0 LED</td>
<td>(QFX3008-I Interconnect device only) Displays the status of fan trays on the device. For more information, see Chassis Status LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td>Fan 1 LED</td>
<td></td>
</tr>
<tr>
<td>Fan 2 LED</td>
<td></td>
</tr>
<tr>
<td>Fan 3 LED</td>
<td></td>
</tr>
<tr>
<td>Fan 4 LED</td>
<td></td>
</tr>
<tr>
<td>Fan 5 LED</td>
<td></td>
</tr>
<tr>
<td>Fan 6 LED</td>
<td></td>
</tr>
<tr>
<td>Fan 7 LED</td>
<td></td>
</tr>
<tr>
<td>Fan 8 LED</td>
<td></td>
</tr>
<tr>
<td>PEM 0 LED</td>
<td>(QFX3008-I Interconnect device only) Displays the status of power supplies on the device. For more information, see Chassis Status LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td>PEM 1 LED</td>
<td></td>
</tr>
<tr>
<td>PEM 2 LED</td>
<td></td>
</tr>
<tr>
<td>PEM 3 LED</td>
<td></td>
</tr>
<tr>
<td>PEM 4 LED</td>
<td></td>
</tr>
</tbody>
</table>
Table 150: show chassis led Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED info for</td>
<td>(QFX3008-I Interconnect device only) Displays the LED information for a Control Board.</td>
</tr>
<tr>
<td>Mastership LED</td>
<td>(QFX3008-I Interconnect device only) Displays status of the MASTER LED on a Control Board. For more information, see Control Board LEDs on a QFX3008-I Interconnect Device.</td>
</tr>
<tr>
<td>Interface</td>
<td>Names of the interfaces on the device.</td>
</tr>
<tr>
<td>LED (ADM/SPD/DPX/POE)</td>
<td>(EX Series switches only) State of the currently selected port parameter of the Status LED for the interface. The Status LED port parameters are:</td>
</tr>
</tbody>
</table>

**NOTE:** EX4500 and EX8200 switches do not have the POE port parameter.

- ADM—Administrative
- SPD—Speed
- DPX—Duplex
- POE—Power over Ethernet

Sample Output

**show chassis led (EX2200 Switch)**

```bash
user@switch> show chassis led
Front panel contents for slot: 0
---------------------------------
LEDs status:
  Alarms LED: Amber
  System LED: Green
  Mode LED : Duplex
Interface LED(ADM/SPD/DPX/POE)
-------------------------------------
ge-0/0/0        Off
ge-0/0/1        Full Duplex
ge-0/0/2        Full Duplex
ge-0/0/3        Off
ge-0/0/4        Off
ge-0/0/5        Full Duplex
ge-0/0/6        Full Duplex
ge-0/0/7        Full Duplex
ge-0/0/8        Full Duplex
ge-0/0/9        Full Duplex
ge-0/0/10       Full Duplex
ge-0/0/11       Full Duplex
ge-0/0/12       Full Duplex
ge-0/0/13       Full Duplex
ge-0/0/14       Full Duplex
ge-0/0/15       Full Duplex
ge-0/0/16       Full Duplex
ge-0/0/17       Full Duplex
ge-0/0/18       Full Duplex
ge-0/0/19       Full Duplex
ge-0/0/20       Full Duplex
ge-0/0/21       Full Duplex
```
show chassis led

user@switch> show chassis led

Front panel contents for slot: 0
---------------------------------
LEDs status:
  Alarms LED: Off
  System LED: Green
  Master LED: Green

Interface   LED(ADM/SPD/DPX/POE)
-------------------------------------
ge-0/0/0        Off
ge-0/0/1        Full Duplex
ge-0/0/2        Full Duplex
ge-0/0/3        Off
ge-0/0/4        Off
ge-0/0/5        Full Duplex
ge-0/0/6        Full Duplex
ge-0/0/7        Full Duplex
ge-0/0/8        Full Duplex
ge-0/0/9        Full Duplex
ge-0/0/10       Full Duplex
ge-0/0/11       Full Duplex
ge-0/0/12       Full Duplex
ge-0/0/13       Full Duplex
ge-0/0/14       Full Duplex
ge-0/0/15       Full Duplex
ge-0/0/16       Full Duplex
ge-0/0/17       Full Duplex
ge-0/0/18       Full Duplex
ge-0/0/19       Full Duplex
ge-0/0/20       Full Duplex
ge-0/0/21       Full Duplex
ge-0/0/22       Off
ge-0/0/23       Off
ge-0/0/24       Full Duplex
ge-0/0/25       Full Duplex
ge-0/0/26       Off
ge-0/0/27       Off
ge-0/0/28       Full Duplex
ge-0/0/29       Full Duplex

show chassis led fpc-slot 0

user@switch> show chassis led fpc-slot 0

Front panel contents for slot: 0
---------------------------------
LEDs status:
  Alarms LED: Red
  System LED: Green
  Master LED: Green
show chassis led (EX Series)

user@switch> show chassis led
Front panel contents for slot: 0
-------------------------------
LEDs status:
Alarms LED: Amber
Status LED: Green
Mode LED : Duplex
Interface LED(ADM/SPD/DPX/POE)
-------------------------------
ge-0/0/0 Off
ge-0/0/1 Full Duplex
ge-0/0/2 Full Duplex
ge-0/0/3 Off
ge-0/0/4 Off
ge-0/0/5 Full Duplex
ge-0/0/6 Full Duplex
ge-0/0/7 Full Duplex
ge-0/0/8 Full Duplex
ge-0/0/9 Full Duplex
ge-0/0/10 Full Duplex
ge-0/0/11 Full Duplex
ge-0/0/12 Full Duplex
ge-0/0/13 Full Duplex
ge-0/0/14 Full Duplex
ge-0/0/15 Full Duplex
ge-0/0/16 Full Duplex
ge-0/0/17 Full Duplex
ge-0/0/18 Full Duplex
ge-0/0/19 Full Duplex
ge-0/0/20 Full Duplex
ge-0/0/21 Full Duplex
ge-0/0/22 Off
show chassis led node-device (QFabric System Node Device)

user@switch> show chassis led node-device node1
Front panel contents for: node1
LEDs status:
  Status/Beacon LED: Yellow Blinking

<table>
<thead>
<tr>
<th>Interface</th>
<th>LINK/SPEED LED</th>
<th>ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1:me5</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>node1:me6</td>
<td>Green</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1:xe-0/0/8</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/10</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/12</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/24</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/25</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/26</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/27</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/28</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/29</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/30</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/31</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/32</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/33</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/34</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/35</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/36</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/37</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/38</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:ge-0/0/39</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>node1:fte-0/1/0</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
<tr>
<td>node1:fte-0/1/2</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
</tbody>
</table>

show chassis led interconnect-device (QFabric System - QFX3600-I Interconnect Device)

user@switch> show chassis led interconnect-device IC-EG0712
Front panel contents for: FPC 0
LEDs status:
  Status/Beacon LED: Yellow Blinking

<table>
<thead>
<tr>
<th>Interface</th>
<th>LINK/SPEED LED</th>
<th>ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-EG0712:me5</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-EG0712:me6</td>
<td>Green</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-EG0712:fte-0/1/0</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>IC-EG0712:fte-0/1/1</td>
<td>Green</td>
<td>Green Blinking</td>
</tr>
</tbody>
</table>
IC-EG0712:fte-0/1/2     Green           Green
IC-EG0712:fte-0/1/3     Green           Green Blinking
IC-EG0712:fte-0/1/4     Green           Green
IC-EG0712:fte-0/1/5     Green           Green Blinking
IC-EG0712:fte-0/1/6     Green           Green
IC-EG0712:fte-0/1/7     Green           Green
IC-EG0712:fte-0/1/8     Green           Green Blinking
IC-EG0712:fte-0/1/9     Green           Green Blinking
IC-EG0712:fte-0/1/10    Green           Green Blinking

show chassis led interconnect-device (QFabric System - QFX3008-I Interconnect Device)

user@switch>  show chassis led interconnect-device IC-EG0712
Front Panel Module Information
---------------------------------
LEDs status:
    Status LED: Green
    Power LED : Yellow Blinking
    Major Alarm LED: Red
    Minor Alarm LED: Yellow
    Fan 0 LED : Green
    Fan 1 LED : Green
    Fan 2 LED : Green
    Fan 3 LED : Green
    Fan 4 LED : Green
    Fan 5 LED : Green
    Fan 6 LED : Green
    Fan 7 LED : Green
    Fan 8 LED : Green
    Fan 9 LED : Green
    PEM 0 LED : Green
    PEM 1 LED : Green
    PEM 2 LED : Green
    PEM 3 LED : off
    PEM 4 LED : Yellow Blinking
    PEM 5 LED : off

    LED info for: CB - 0
---------------------------------
LEDs status:
    Status LED: Green
    Mastership LED: Green

    Interface               STATUS LED      LINK/ACTIVITY LED
    ---------------------------------
    IC-F4899:pme0 :         Green           N/A
    IC-F4899:pme1 :         off             N/A
    IC-F4899:pme2 :         off             N/A
    IC-F4899:pme3 :         off             N/A

    LED info for: CB - 1
---------------------------------
LEDs status:
    Status LED: Green
    Mastership LED: Amber

    Interface               STATUS LED      LINK/ACTIVITY LED
    ---------------------------------
    IC-F4899:pme0 :         Green           N/A
    IC-F4899:pme1 :         off             N/A
    IC-F4899:pme2 :         off             N/A
IC-F4899:pme3 :          off         N/A

LED info for: FC 0 FPC - 0
----------------------------------
LEDs status:
    Status LED: Green

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-F4899:fte-0/0/0</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/1</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/2</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/3</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/4</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/5</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/6</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/7</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/8</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/9</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/10</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/11</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/12</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/13</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/14</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-0/0/15</td>
<td>Green</td>
<td>N/A</td>
</tr>
</tbody>
</table>

LED info for: FC 1 FPC - 1
----------------------------------
LEDs status:
    Status LED: Green

<table>
<thead>
<tr>
<th>Interface</th>
<th>STATUS LED</th>
<th>LINK/ACTIVITY LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC-F4899:fte-1/0/0</td>
<td>Green</td>
<td>N/A</td>
</tr>
<tr>
<td>IC-F4899:fte-1/0/1</td>
<td>Green</td>
<td>N/A</td>
</tr>
</tbody>
</table>

LED info for: RC 2 FPC - 10
----------------------------------
LEDs status:
    Status LED: Green

LED info for: RC 3 FPC - 11
----------------------------------
LEDs status:
    Status LED: Green
show chassis location

Syntax  show chassis location
Syntax (TX Matrix Router)  show chassis location <fpc | interface (by-name name | by-slot fpc number lcc number) | lcc number | scc>
Syntax (TX Matrix Plus Router)  show chassis location <fpc | interface (by-name name | by-slot fpc number lcc number) | lcc number | sfc number>
Syntax (MX Series Router)  show chassis location <all-members>
Syntax (QFX Series)  show chassis location <interconnect-device name>
<node-device name>

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  Display the physical location of the chassis. This command can only be used on the master Routing Engine.

Options
none—Display all information about the physical location of the chassis. On a TX Matrix router, display all information about the physical location of the TX Matrix router and its attached T640 routers. On a TX Matrix Plus router, display all information about the physical location of the TX Matrix Plus router and its attached routers.
all-members—(MX Series routers only) (Optional) Display the physical location of the chassis for all the member routers in the Virtual Chassis configuration.
fpc—(TX Matrix router and TX Matrix Plus router only) (Optional) Display the physical location of all Flexible PIC Concentrators (FPCs).
interconnect-device name—(QFabric systems only) (Optional) Display the physical location of the Interconnect device.
interface by-name name—(TX Matrix and TX Matrix Plus routers only) (Optional) Display the physical location of a specified interface name. On a TX Matrix router, this option displays the FPC number and T640 router (line-card chassis) number associated with the specified interface. On a TX Matrix Plus router, this option displays the FPC number and router (line-card chassis) number associated with the specified interface.
interface by-slot fpc number lcc number—(TX Matrix and TX Matrix Plus router only) (Optional) On a TX Matrix router, display the global FPC number of an interface by specifying its local FPC number and T640 router (line-card chassis) number. On a
TX Matrix Plus router, display the global FPC number of an interface by specifying its local FPC number and router (line-card chassis) number.

- The global FPC number is the FPC slot number when all the FPC slots in the routing matrix are considered: 0 through 31. On TX Matrix Plus router with 3D SIBs, the value is 0 through 63. The local FPC number is the FPC slot number on a particular T640 router.

- For `fpc`, replace `number` with a value from 0 through 7.

- For `lcc`, replace `number` with a value from 0 through 7.

`lcc number`—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display the physical location of a specified T640 router (line-card chassis) that is connected to a TX Matrix router. On a TX Matrix Plus router, display the physical location of a specified router (line-card chassis) that is connected to a TX Matrix Plus router.

Replace `number` with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

`local`—(MX Series routers only) (Optional) Display the physical location of the chassis for the local Virtual Chassis member.

`member member-id`—(MX Series routers only) (Optional) Display the physical location of the chassis for the specified member of the Virtual Chassis configuration. Replace `member-id` with a value of 0 or 1.

`node-device name`—(QFabric systems only) (Optional) Display the physical location of the Node device.

`scc`—(TX Matrix routers only) (Optional) Display the physical location of the TX Matrix router (switch-card chassis).

`sfc`—(TX Matrix Plus routers only) (Optional) Display the physical location of the TX Matrix Plus router (or switch-fabric chassis).

**Required Privilege Level**

| Level | view |

**List of Sample Output**

- show chassis location on page 1054
- show chassis location fpc (TX Matrix Router) on page 1054
- show chassis location interface by-slot (TX Matrix Router) on page 1054
Table 151 on page 1054 lists the output fields for the `show chassis location` command. Output fields are listed in the approximate order in which they appear.

### Table 151: show chassis location Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>country-code</td>
<td>Country code information.</td>
</tr>
<tr>
<td>postal-code</td>
<td>Postal code information.</td>
</tr>
<tr>
<td>Building</td>
<td>Building information.</td>
</tr>
<tr>
<td>Floor</td>
<td>Floor information.</td>
</tr>
<tr>
<td>Global FPC</td>
<td>Global FPC number. The FPC slot number, when all FPC slots in the routing matrix are considered. The range of values is 0 through 31. On TX Matrix Plus router with 3D SIBs the value is 0 through 63.</td>
</tr>
<tr>
<td>LCC</td>
<td>Line-card chassis number. On a TX Matrix router, the number of a particular T640 router connected to the TX Matrix router. On a TX Matrix Plus router, the number of a particular router connected to the TX Matrix Plus router.</td>
</tr>
<tr>
<td>Local FPC</td>
<td>Local FPC number. On a TX Matrix router, the FPC slot number on a particular T640 router. On a TX Matrix Plus router, the FPC slot number on a particular router.</td>
</tr>
</tbody>
</table>

### Sample Output

**show chassis location**

```
user@host> show chassis location
country-code: US
postal-code: 94404
Building: Building 2, Floor: 2
```

**show chassis location fpc (TX Matrix Router)**

```
user@host> show chassis location fpc
Global FPC  LCC  Local FPC
17          2    1
21          2    5
```

**show chassis location interface by-slot (TX Matrix Router)**

```
user@host> show chassis location interface by-slot fpc1 lcc1
Global FPC: 9
```
show chassis location fpc (TX Matrix Plus Router)

user@host> show chassis location fpc
Global FPC    LCC    Local FPC
0          0        0
1          0        1

show chassis location interface by-slot (TX Matrix Plus Router)

user@host> show chassis location interface by-slot fpc 2 lcc 1
Global FPC: 10

show chassis location (QFX3500 Switches)

user@switch> show chassis location
country-code: US
postal-code: 94404
Building: Building 2, Floor: 2

show chassis location (QFabric Systems)

user@switch> show chassis location interconnect-device interconnect 1
country-code: US
postal-code: 94404
Building: Building 2, Floor: 2
show chassis pic

Syntax

show chassis pic fpc-slot slot-number pic-slot slot-number

Syntax (TX Matrix and TX Matrix Plus Routers)

show chassis pic fpc-slot slot-number pic-slot slot-number
<lcc number>

Syntax (MX Series Routers)

show chassis pic fpc-slot slot-number pic-slot slot-number
<all-members>
<local>
<member member-id>

Syntax (MX104, MX2010 and MX2020 3D Universal Edge Routers)

show chassis pic fpc-slot slot-number pic-slot slot-number

Syntax (PTX Series Packet Transport Router)

show chassis pic transport fpc-slot slot-number pic-slot slot-number

Syntax (QFX Series)

show chassis pic
<interconnect-device name (fpc-slot slot-number | pic-slot slot-number)>
<node-device name pic-slot slot-number>

Syntax (ACX Series Universal Access Routers)

show chassis pic fpc-slot slot-number pic-slot slot-number

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series.
Command introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.
Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.
Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.
Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.

Description

Display status information about the PIC installed in the specified Flexible PIC Concentrator (FPC) and PIC slot.

Options

fpc-slot slot-number—Display information about the PIC in this particular FPC slot:

- On a TX Matrix router, if you specify the number of the T640 router by using the lcc number option (the recommended method), replace slot-number with a value from 0 through 7. Otherwise, replace slot-number with a value from 0 through 31.

Likewise, on a TX Matrix Plus router, if you specify the number of the T1600 router by using the lcc number option (the recommended method), replace slot-number with a value from 0 through 7. Otherwise, replace slot-number with a value from 0 through 31. For example, the following commands have the same result:
user@host> show chassis pic fpc-slot1 lcc1 pic-slot1
user@host> show chassis pic fpc-slot9 pic-slot1

- M120 routers only—Replace `slot-number` with a value from 0 through 5.
- MX80 routers only—Replace `slot-number` with a value from 0 through 1.
- MX104 routers only—Replace `slot-number` with a value from 0 through 2.
- MX240 routers only—Replace `slot-number` with a value from 0 through 2.
- MX480 routers only—Replace `slot-number` with a value from 0 through 5.
- MX960 routers only—Replace `slot-number` with a value from 0 through 11.
- MX2010 routers only—Replace `slot-number` with a value from 0 through 9.
- MX2020 routers only—Replace `slot-number` with a value from 0 through 19.
- Other routers—Replace `slot-number` with a value from 0 through 7.
- EX Series switches:
  - EX3200 switches and EX4200 standalone switches—Replace `slot-number` with 0.
  - EX4200 switches in a Virtual Chassis configuration—Replace `slot-number` with a value from 0 through 9 (switch's member ID).
  - EX8208 switches—Replace `slot-number` with a value from 0 through 7 (line card).
  - EX8216 switches—Replace `slot-number` with a value from 0 through 15 (line card).
- QFX Series:
  - QFX3500 switches—Replace `slot-number` with 0. In the command output, FPC refers to a line card. The FPC number equals the slot number for the line card.
  - QFabric systems—Replace `slot-number` with any number between 0 and 15. In the command output, FPC refers to a line card. The FPC number equals the slot number for the line card.

**all-members**—(MX Series routers and EX Series switches only) (Optional) Display PIC information for all member routers in the Virtual Chassis configuration.

**interconnect-device name**—(QFabric systems only) (Optional) Display PIC information for a specified Interconnect device.

**lcc number**—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display PIC information for a specified T640 router (line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, display PIC information for a specified router (line-card chassis) that is connected to the TX Matrix Plus router.
Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers and EX Series switches only) (Optional) Display PIC information for the local Virtual Chassis member.

member member-id—(MX Series routers and EX Series switches only) (Optional) Display PIC information for the specified member of the Virtual Chassis configuration. Replace member-id with a value of 0 or 1.

node-device name—(QFabric systems only) (Optional) Display PIC information for a specified Node device.

pic-slot slot-number—Display information about the PIC in this particular PIC slot. For routers, replace slot-number with a value from 0 through 3. For EX3200 and EX4200 switches, replace slot-number with 0 for built-in network interfaces and 1 for interfaces on uplink modules. For EX8208 and EX8216 switches, replace slot-number with 0. For the QFX3500 standalone switch and the QFabric system, replace slot-number with 0 or 1.

transport—Display PIC information for optical transport network.

**Required Privilege Level**

- view

**Related Documentation**

- request chassis pic on page 171
- show chassis hardware
  - Configuring the PIC Type
  - 100-Gigabit Ethernet Type 4 PIC with CFP Overview

**List of Sample Output**

- show chassis pic fpc-slot pic-slot on page 1061
- show chassis pic fpc-slot pic-slot (PIC Offline) on page 1061
- show chassis pic fpc-slot pic-slot (FPC Offline) on page 1062
- show chassis pic fpc-slot pic-slot (FPC Not Present) on page 1062
- show chassis pic fpc-slot pic-slot (PIC Not Present) on page 1062
- show chassis pic fpc-slot pic-slot (M120 Router) on page 1062
- show chassis pic fpc-slot pic-slot (MX104 Router) on page 1062
- show chassis pic fpc-slot pic-slot (MX960 Router Bidirectional Optics) on page 1062
show chassis pic fpc-slot pic-slot (MX480 Router with 100-Gigabit Ethernet MIC) on page 1063
show chassis pic fpc-slot pic-slot (MX240, MX480, MX960 Routers with Application Services Modular Line Card) on page 1063
show chassis pic fpc-slot pic-slot (MX480 Router with MPC4E) on page 1063
show chassis pic fpc-slot pic-slot (MX2010 Router) on page 1064
show chassis pic fpc-slot pic-slot (MX2020 Router) on page 1064
show chassis pic fpc-slot pic-slot (MX2020 Routers with MPC4E) on page 1064
show chassis pic fpc-slot pic-slot (TT600 Router with 100-Gigabit Ethernet PIC) on page 1064
show chassis pic fpc-slot pic-slot lcc (TX Matrix Router) on page 1065
show chassis pic fpc-slot pic-slot lcc (TX Matrix Plus Router) on page 1065
show chassis pic fpc-slot pic-slot (Next-Generation SONET/SDH SFP) on page 1065
show chassis pic fpc-slot pic-slot (12-Port T1/E1) on page 1066
show chassis pic fpc-slot pic-slot (4x CHOC3 SONET CE SFP) on page 1066
show chassis pic fpc-slot pic-slot (SONET/SDH OC3/STM1 [Multi-Rate] MIC with SFP) on page 1066
show chassis pic fpc-slot pic-slot (8-port Channelized SONET/SDH OC3/STM1 [Multi-Rate] MIC with SFP) on page 1066
show chassis pic fpc-slot pic-slot (4-port Channelized SONET/SDH OC3/STM1 [Multi-Rate] MIC with SFP) on page 1067
show chassis pic fpc-slot pic-slot (1-port OC192/STM64 MIC with XFP) on page 1067
show chassis pic fpc-slot 1 pic-slot 2 (8-port DS3/E3 MIC) on page 1067
show chassis pic fpc-slot pic-slot (OTN) on page 1067
show chassis pic fpc-slot pic-slot (QFX3500 Switch) on page 1068
show chassis pic interconnect-device fpc-slot pic-slot (QFabric Systems) on page 1068
show chassis pic node-device fpc-slot pic-slot (QFabric System) on page 1068
show chassis pic fpc-slot pic-slot (ACX2000 Universal Access Router) on page 1069
show chassis pic fpc-slot pic-slot (MX Routers with Media Services Blade [MSB]) on page 1069
show chassis pic FPC slot PIC slot (MX Routers with Media Services Blade [MSB]) on page 1069
show chassis pic transport fpc-slot pic-slot (PTX Series Packet Transport Routers) on page 1069

**Output Fields** Table 152 on page 1059 lists the output fields for the `show chassis pic` command. Output fields are listed in the approximate order in which they appear.

**Table 152: show chassis pic Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>PIC type.</td>
</tr>
</tbody>
</table>

**NOTE:** On the 1-port OC192/STM64 MICs with the SDH framing mode, the type is displayed as **MIC-3D-1STM64-XFP** and with the SONET framing mode, the type is displayed as **MIC-3D-1OC192-XFP**. By default, the 1-port OC192/STM64 MICs displays the type as **MIC-3D-1OC192-XFP**.
### Table 152: show chassis pic Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Layer2 Overhead</td>
<td>(MX Series routers) Indicates whether functionality to count the Layer 2 overhead bytes in the interface statistics at the PIC level is enabled or disabled.</td>
</tr>
<tr>
<td>ASIC type</td>
<td>Type of ASIC on the PIC.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the PIC. State is displayed only when a PIC is in the slot.</td>
</tr>
<tr>
<td>State</td>
<td>• <strong>Online</strong>— PIC is online and running.</td>
</tr>
<tr>
<td>State</td>
<td>• <strong>Offline</strong>—PIC is powered down.</td>
</tr>
<tr>
<td>PIC version</td>
<td>PIC hardware version.</td>
</tr>
<tr>
<td>Uptime</td>
<td>How long the PIC has been online.</td>
</tr>
<tr>
<td>Package</td>
<td>(Multiservices PICs only) Services package supported: Layer-2 or Layer-3.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port number for the PIC.</td>
</tr>
<tr>
<td>Cable Type</td>
<td>Type of cable connected to the port: LH, LX, or SX.</td>
</tr>
<tr>
<td><strong>PIC Port Information</strong> (MX480 Router100-Gigabit Ethernet CFP)</td>
<td>Port-level information for the PIC.</td>
</tr>
<tr>
<td>Port</td>
<td>• Port—Port number</td>
</tr>
<tr>
<td>Cable type</td>
<td>• Cable type—Type of optical transceiver installed.</td>
</tr>
<tr>
<td>Fiber type</td>
<td>• Fiber type—Type of fiber. SM is single-mode.</td>
</tr>
<tr>
<td>Xcvr vendor</td>
<td>• Xcvr vendor—Transceiver vendor name.</td>
</tr>
<tr>
<td>Xcvr vendor part number</td>
<td>• Xcvr vendor part number—Transceiver vendor part number.</td>
</tr>
<tr>
<td>Fiber type</td>
<td>• Wavelength—Wavelength of the transmitted signal. Uplinks and downlinks are always 1550 nm. There is a separate fiber for each direction.</td>
</tr>
<tr>
<td><strong>PIC Port Information</strong> (MX960 Router Bidirectional Optics)</td>
<td>Port-level information for the PIC.</td>
</tr>
<tr>
<td>Port</td>
<td>• Port—Port number</td>
</tr>
<tr>
<td>Cable type</td>
<td>• Cable type—Type of small form-factor pluggable (SFP) optical transceiver installed. Uplink interfaces display -U. Down link interfaces display -D.</td>
</tr>
<tr>
<td>Fiber type</td>
<td>• Fiber type—Type of fiber. SM is single-mode.</td>
</tr>
<tr>
<td>Xcvr vendor</td>
<td>• Xcvr vendor—Transceiver vendor name.</td>
</tr>
<tr>
<td>Xcvr vendor part number</td>
<td>• Xcvr vendor part number—Transceiver vendor part number.</td>
</tr>
<tr>
<td>Fiber type</td>
<td>• BX10-10-km bidirectional optics.</td>
</tr>
<tr>
<td>Xcvr vendor part number</td>
<td>• BX40-40-km bidirectional optics.</td>
</tr>
<tr>
<td>Fiber type</td>
<td>• SFP-LX-40-km SFP optics.</td>
</tr>
<tr>
<td>Wavelength</td>
<td>• Wavelength—Wavelength of the transmitted signal. Uplinks are always 1310 nm. Downlinks are either 1490 nm or 1550 nm.</td>
</tr>
</tbody>
</table>
Table 152: show chassis pic Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PIC Port information</strong></td>
<td>Port-level information for the next-generation SONET/SDH SFP PIC.</td>
</tr>
<tr>
<td>(Next-Generation SONET/SDH SFP)</td>
<td>- Port—Port number.</td>
</tr>
<tr>
<td></td>
<td>- Cable type—Type of small form-factor pluggable (SFP) optical transceiver installed.</td>
</tr>
<tr>
<td></td>
<td>- Fiber type—Type of fiber: <strong>SM</strong> (single-mode) or <strong>MM</strong> (multimode).</td>
</tr>
<tr>
<td></td>
<td>- Xcvr vendor—Transceiver vendor name.</td>
</tr>
<tr>
<td></td>
<td>- Xcvr vendor part number—Transceiver vendor part number.</td>
</tr>
<tr>
<td></td>
<td>- Wavelength—Wavelength of the transmitted signal. Next-generation SONET/SDH SFPs use 1310 nm.</td>
</tr>
</tbody>
</table>

| **Pic port information (MX104 router)**         | Port-level information for the PIC.                                                                                                               |
|                                                 | - Port—Port number.                                                                                                                            |
|                                                 | - Cable type—Type of optical transceiver installed.                                                                                             |
|                                                 | - Fiber type—Type of fiber. **SM** is single-mode.                                                                                             |
|                                                 | - Xcvr vendor—Transceiver vendor name.                                                                                                           |
|                                                 | - Xcvr vendor part number—Transceiver vendor part number.                                                                                       |
|                                                 | - Wavelength—Wavelength of the transmitted signal.                                                                                              |
|                                                 | - Xcvr Firmware—Firmware version of the transceiver.                                                                                           |

| **Multirate Mode**                              | Rate-selectability status for the MIC: **Enabled** or **Disabled**.                                                                             |

| **Channelization**                              | Indicates whether channelization is enabled or disabled on the DS3/E3 MIC.                                                                    |

Sample Output

**show chassis pic fpc-slot pic-slot**

```
user@host> show chassis pic fpc-slot2 pic-slot0
PIC fpc slot 2 pic slot 0 information:
Type                             10x 1GE(LAN), 1000 BASE
ASIC type                        H chip
State                            Online
PIC version                      1.1
Uptime                           1 day, 50 minutes, 58 seconds
PIC Port Information:
  Port         Cable           Xcvr               Xcvr Vendor
  Number       Type            Vendor Name        Part Number
  0            GIGE 1000EX     FINISAR CORP.      FTRJ8519P1BNL-J3
  1            GIGE 1000EX     FINISAR CORP.      FTRJ-8519-7D-JUN
```

**show chassis pic fpc-slot pic-slot (PIC Offline)**

```
user@host> show chassis pic fpc-slot1 pic-slot0
PIC fpc slot 1 pic slot 0 information:
State                            Offline
```

Copyright © 2013, Juniper Networks, Inc.
show chassis pic fpc-slot pic-slot (FPC Offline)

user@host> show chassis pic fpc-slot1 pic-slot 0
FPC 1 is not online

show chassis pic fpc-slot pic-slot (FPC Not Present)

user@host> show chassis pic fpc-slot 4 pic-slot 0
FPC slot 4 is empty

show chassis pic fpc-slot pic-slot (PIC Not Present)

user@host> show chassis pic fpc-slot 5 pic-slot 2
FPC 5, PIC 2 is empty

show chassis pic fpc-slot pic-slot (M120 Router)

user@host> show chassis pic fpc-slot 3 pic-slot 0
PC slot 3, PIC slot 0 information:
  Type                             2x G/E IQ, 1000 BASE
  ASIC type                        IQ GE 2 VLAN-TAG FPGA
  State                            Online
  PIC version                 1.16
  Uptime                        3 hours, 3 minutes

PIC Port Information:

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Cable Type</th>
<th>Xcvr Vendor</th>
<th>Xcvr Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GIGE 1000SX</td>
<td>FINISAR CORP.</td>
<td>FTRJ8519P1BNL-J3</td>
</tr>
<tr>
<td>1</td>
<td>GIGE 1000SX</td>
<td>FINISAR CORP.</td>
<td>FTRJ8519P1BNL-J3</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (MX104 Router)

user@host> show chassis pic fpc-slot1 pic-slot 1
FPC slot 1, PIC slot 1 information:
  Type                             10x 1GE(LAN) -E  SFP
  State                            Online
  PIC version                  1.1
  Uptime                        1 hour, 30 minutes, 59 seconds

PIC Port Information:

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Cable Type</th>
<th>Xcvr Vendor</th>
<th>Xcvr Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>GIGE 1000T</td>
<td>Methode Elec.</td>
<td>SP7041-M1-JN</td>
</tr>
<tr>
<td>6</td>
<td>GIGE 1000LX10</td>
<td>FINISAR CORP.</td>
<td>FTLF1318P28TL-J1</td>
</tr>
<tr>
<td>8</td>
<td>GIGE 1000T</td>
<td>Methode Elec.</td>
<td>SP7041-M1-JN</td>
</tr>
<tr>
<td>9</td>
<td>GIGE 1000T</td>
<td>Methode Elec.</td>
<td>SP7041-M1-JN</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (MX960 Router Bidirectional Optics)

user@host> show chassis pic fpc-slot4 pic-slot 1
FPC slot 4, PIC slot 1 information:
  Type                             10x 1GE(LAN)
  Account Layer2 Overhead          Enabled
  State                            Online
show chassis pic fpc-slot pic-slot (MX480 Router with 100-Gigabit Ethernet MIC)

user@host> show chassis pic fpc-slot1 pic-slot2
FPC slot 1, PIC slot 2 information:
Type: 1X100GE CFP
State: Online
PIC version: 2.10
Uptime: 4 minutes, 48 seconds
PIC port information:
Fiber: Xcvr vendor
Port Cable type type Xcvr vendor part number Wavelength
0 100GBASE LR4 SM FINISAR CORP. FTLC1181RDNS-33 1310 nm

Xcvr vendor
firmware version
1.8

show chassis pic fpc-slot pic-slot (MX240, MX480, MX960 Routers with Application Services Modular Line Card)

user@host> show chassis pic fpc-slot1 pic-slot2
FPC slot 1, PIC slot 2 information:
Type: AS-MXC
State: Online
PIC version: 1.0
Uptime: 11 hours, 18 minutes, 3 seconds

show chassis pic fpc-slot pic-slot (MX480 Router with MPC4E)

user@host> show chassis pic fpc-slot3 pic-slot0
FPC slot 3, PIC slot 0 information:
Type: 4x10GE SFPP
State: Online
PIC version: 0.0
Uptime: 41 seconds
PIC port information:
Fiber: Xcvr vendor Wave- Xcvr
Port Cable type type Xcvr vendor part number length
0 10GBASE SR MM OPNEXT, INC. TRS2001EM-0014 850 nm 0.0
show chassis pic fpc-slot pic-slot (MX2010 Router)

```
user@host> show chassis pic fpc-slot 9 pic-slot 3
FPC slot 9, PIC slot 3 information:
  Type                             1X100GE CFP
  Account Layer2 Overhead          Enabled
  State                            Online
  PIC version                      0.0
  Uptime                           14 hours, 51 seconds
```

show chassis pic fpc-slot pic-slot (MX2020 Router)

```
user@host> show chassis pic fpc-slot 19 pic-slot 3
FPC slot 19, PIC slot 3 information:
  Type                             4x 10GE(LAN) SFP+
  Account Layer2 Overhead          Enabled
  State                            Online
  PIC version                      0.0
  Uptime                           1 day, 11 hours, 26 minutes, 36 seconds
```

show chassis pic fpc-slot pic-slot (MX2020 Routers with MPC4E)

```
user@host> show chassis pic fpc-slot 14 pic-slot 0
FPC slot 14, PIC slot 2 information:
  Type                             4x10GE SFPP
  State                            Online
  PIC version                      0.0
  Uptime                           1 day, 14 hours, 49 minutes, 9 seconds
```

show chassis pic fpc-slot pic-slot (TI600 Router with 100-Gigabit Ethernet PIC)

```
user@host> run show chassis pic fpc-slot 3 pic-slot 1
```
FPC slot 3, PIC slot 1 information:
- **Type**: 100GE SLOT1
- **ASIC type**: Brooklyn 100GE FPGA
- **State**: Online
- **PIC version**: 1.3
- **Uptime**: 10 minutes, 44 seconds

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>Fiber type</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100GBASE LR4</td>
<td>SM</td>
<td>Opnext Inc.</td>
<td>TRC5E20ENFSF000F</td>
<td>1310 nm</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot lcc (TX Matrix Router)

```bash
user@host> show chassis pic fpc-slot1 pic-slot1 lcc 0 lcc0-re0:
```

PIC fpc slot 1 pic slot 1 information:
- **Type**: 4x OC-3 SONET, SMIR
- **ASIC type**: D chip
- **State**: Online
- **PIC version**: 1.2
- **Uptime**: 5 days, 2 hours, 12 minutes, 8 seconds

show chassis pic fpc-slot pic-slot lcc (TX Matrix Plus Router)

```bash
user@host> show chassis pic fpc-slot 0 fpc-slot 8 lcc0-re0:
```

FPC slot 8, PIC slot 0 information:
- **Type**: 1x 10GE(LAN/WAN)
- **State**: Online
- **Uptime**: 2 hours, 46 minutes, 23 seconds

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>Fiber type</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10GBASE ZR</td>
<td>SM</td>
<td>Opnext Inc.</td>
<td>TRF7061BN-LF150</td>
<td>1550 nm</td>
</tr>
<tr>
<td>0</td>
<td>10GBASE ZR</td>
<td>SM</td>
<td>FINISAR CORP.</td>
<td>FTRX-1811-3-J2</td>
<td>1550 nm</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (Next-Generation SONET/SDH SFP)

```bash
user@host> show chassis pic fpc-slot 4 pic-slot 0
```

FPC slot 4, PIC slot 0 information:
- **Type**: 4x OC-3 1x OC-12 SFP
- **ASIC type**: D FPGA
- **State**: Online
- **PIC version**: 1.3
- **Uptime**: 1 day, 50 minutes, 4 seconds

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>Fiber type</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OC48 short reach</td>
<td>SM</td>
<td>FINISAR CORP.</td>
<td>FTRJ1321P1BTL-J2</td>
<td>1310 nm</td>
</tr>
<tr>
<td>1</td>
<td>OC3 short reach</td>
<td>MM</td>
<td>OCP</td>
<td>TRPA03MM3BAS-JE</td>
<td>1310 nm</td>
</tr>
<tr>
<td>2</td>
<td>OC3 short reach</td>
<td>MM</td>
<td>OCP</td>
<td>TRXA03MM3BAS-JW</td>
<td>1310 nm</td>
</tr>
<tr>
<td>3</td>
<td>OC12 inter reach</td>
<td>SM</td>
<td>FINISAR CORP.</td>
<td>FTLF1322P1BTR</td>
<td>1310 nm</td>
</tr>
</tbody>
</table>
show chassis pic fpc-slot pic-slot (12-Port T1/E1)

FPC slot 0, PIC slot 3 information:
- Type: 12x T1/E1 CE
- State: Online
- PIC version: 1.1
- CPU load average: 1 percent
- Interrupt load average: 0 percent
- Total DRAM size: 128 MB
- Memory buffer utilization: 100 percent
- Memory heap utilization: 4 percent
- Uptime: 1 day, 22 hours, 28 minutes, 12 seconds
- Internal Clock Synchronization: Normal

show chassis pic fpc-slot pic-slot (4x CHOC3 SONET CE SFP)

FPC slot 0, PIC slot 1 information:
- Type: 4x CHOC3 SONET CE SFP
- State: Online
- PIC version: 1.3
- CPU load average: 1 percent
- Interrupt load average: 0 percent
- Total DRAM size: 128 MB
- Memory buffer utilization: 99 percent
- Memory heap utilization: 4 percent
- Uptime: 1 day, 22 hours, 55 minutes, 37 seconds
- Internal Clock Synchronization: Normal

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>type</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OC3 short reach</td>
<td>MM</td>
<td>AVAGO</td>
<td>HFBR-57E0P-JU2</td>
<td>n/a</td>
</tr>
<tr>
<td>1</td>
<td>OC3 short reach</td>
<td>MM</td>
<td>AVAGO</td>
<td>HFBR-57E0P-JU2</td>
<td>n/a</td>
</tr>
<tr>
<td>3</td>
<td>OC3 long reach</td>
<td>SM</td>
<td>OPNEXT INC</td>
<td>TRF5456AVLB314</td>
<td>1310 nm</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (SONET/SDH OC3/STM1 [Multi-Rate] MIC with SFP)

FPC slot 0, PIC slot 0 information:
- Type: MIC-3D-8OC3OC12-4OC48
- State: Online
- PIC version: 1.8
- Uptime: 3 days, 22 hours, 3 minutes, 50 seconds

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>type</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OC12 inter reach</td>
<td>SM</td>
<td>FINISAR CORP</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>7</td>
<td>OC12 inter reach</td>
<td>SM</td>
<td>FINISAR CORP</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
</tbody>
</table>

Multirate Mode: Enabled

show chassis pic fpc-slot pic-slot (8-port Channelized SONET/SDH OC3/STM1 [Multi-Rate] MIC with SFP)

FPC slot 3, PIC slot 0 information:
- Type: MIC-3D-8CHOC3-4CHOC12
- State: Online
- PIC version: 1.9
- Uptime: 1 hour, 21 minutes, 24 seconds

Copyright © 2013, Juniper Networks, Inc.
PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>SM</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OC12 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>1</td>
<td>OC12 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>2</td>
<td>OC12 inter reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J2</td>
<td>1310 nm</td>
</tr>
<tr>
<td>4</td>
<td>OC12 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>5</td>
<td>OC12 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>6</td>
<td>OC12 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>7</td>
<td>OC12 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (4-port Channelized SONET/SDH OC3/STM1 [Multi-Rate] MIC with SFP)

user@host> show chassis pic fpc-slot 5 pic-slot 0
FPC slot 5, PIC slot 0 information:
Type                          MIC-3D-4CHOC3-2CHOC12
State                         Online
PIC version                   1.9
Uptime                       1 hour, 21 minutes

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>SM</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OC12 inter reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>2</td>
<td>OC12 inter reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
<tr>
<td>3</td>
<td>OC12 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTRJ1322P1BTR-J3</td>
<td>1310 nm</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (1-port OC192/STM64 MIC with XFP)

user@host> show chassis pic fpc-slot 1 pic-slot 0
FPC slot 1, PIC slot 0 information:
Type                          MIC-3D-1OC192-XFP
State                         Online
PIC version                   1.2
Uptime                       1 day, 11 hours, 4 minutes, 6 seconds

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>n/a</th>
<th>Xcvr vendor</th>
<th>part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OC192 short reach</td>
<td></td>
<td>FINISAR CORP.</td>
<td>FTLX1412M3BCL-J3</td>
<td>1310 nm</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (8-port DS3/E3 MIC)

user@host> show chassis pic fpc-slot 1 pic-slot 2
FPC slot 1, PIC slot 2 information:
Type                          MIC-3D-8DS3-E3
State                         Online
PIC version                   1.10
Uptime                       4 days, 1 hour, 29 minutes, 19 seconds
Channelization Mode           Disabled

show chassis pic fpc-slot pic-slot (OTN)

user@host> show chassis pic fpc-slot 5 pic-slot 0
PIC fpc slot 5 pic slot 0 information:
Type                          1x10GE(LAN),OTN
ASIC type                     H chip
State                         Online
show chassis pic fpc-slot pic-slot (QFX3500 Switch)

user@switch> show chassis pic fpc-slot 0 pic-slot 0
FPC slot 0, PIC slot 0 information:
Type 48x 10G-SFP+ Builtin
State Online
Uptime 3 days, 3 hours, 5 minutes, 20 seconds

show chassis pic interconnect-device fpc-slot pic-slot (QFabric Systems)

user@switch> show chassis pic interconnect-device interconnect1 fpc-slot 9 pic-slot 0
FPC slot 9, PIC slot 0 information:
Type 16x 40G-GE Builtin
State Online
Uptime 2 hours, 47 minutes, 40 seconds

show chassis pic node-device fpc-slot pic-slot (QFabric System)

user@switch> show chassis pic node-device node1 fpc-slot 0
FPC slot node1, PIC slot 0 information:
Type 48x 10G-SFP+Builtin
State Online
Uptime 2 hours, 52 minutes, 37 seconds

PIC port information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Cable type</th>
<th>Fiber type</th>
<th>Xcvr vendor</th>
<th>Xcvr vendor part number</th>
<th>Wavelength</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>1</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>2</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>3</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>4</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>5</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>6</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>7</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>8</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>9</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>10</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>11</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>12</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>13</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>14</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>15</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>16</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>17</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>18</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>19</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>20</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>21</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>22</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>23</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>24</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>25</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>26</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>27</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>28</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>29</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>30</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>31</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPPS101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>Slot</td>
<td>Type</td>
<td>Media</td>
<td>Vendor</td>
<td>Model</td>
<td>Wavelength</td>
</tr>
<tr>
<td>------</td>
<td>---------------</td>
<td>-------</td>
<td>-----------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>32</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>33</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>34</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>35</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>36</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>37</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>38</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>39</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>40</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>41</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>42</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>43</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>44</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>45</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>46</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
<tr>
<td>47</td>
<td>10GBASE SR</td>
<td>MM</td>
<td>SumitomoElectric</td>
<td>SPP5101SR-J3</td>
<td>850 nm</td>
</tr>
</tbody>
</table>

show chassis pic fpc-slot pic-slot (ACX2000 Universal Access Router)

```bash
user@host> show chassis pic fpc-slot 0 pic-slot 1
FPC slot 0, PIC slot 1 information:
Type                         8x 1GE(LAN) RJ45 Builtin
State                        Online
Uptime                       6 days, 2 hours, 51 minutes, 11 seconds
```

show chassis pic fpc-slot pic-slot (MX Routers with Media Services Blade [MSB])

```bash
user@switch> show chassis pic fpc-slot 1 pic-slot 0
FPC slot 1, PIC slot 0 information:
Type                         AS-MSC
State                        Online
PIC version                  1.6
Uptime                       11 hours, 17 minutes, 56 seconds
```

show chassis pic FPC slot PIC slot (MX Routers with Media Services Blade [MSB])

```bash
user@switch> show chassis pic fpc-slot 1 pic-slot 2
Type                         AS-MXC
State                        Online
PIC version                  1.0
Uptime                       11 hours, 18 minutes, 3 seconds
```

show chassis pic transport fpc-slot pic-slot (PTX Series Packet Transport Routers)

```bash
user@host> show chassis pic transport fpc-slot 2 pic-slot 0
Administrative State:       In Service
Operational State:          Normal
```
### show chassis routing-engine

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show chassis routing-engine &lt;bios</td>
<td>Display the status of the Routing Engine.</td>
</tr>
<tr>
<td>slot&gt;</td>
<td></td>
</tr>
<tr>
<td>Syntax (EX Series Switches)</td>
<td>Command introduced before Junos OS Release 7.4.</td>
</tr>
<tr>
<td>show chassis routing-engine &lt;&lt;slot&gt;&gt;</td>
<td>Command introduced in Junos OS Release 9.0 for EX Series switches.</td>
</tr>
<tr>
<td>Syntax (T Series routers)</td>
<td>sfc option introduced for the TX Matrix Plus router in Junos OS Release in 9.6.</td>
</tr>
<tr>
<td>show chassis routing-engine &lt;bios</td>
<td>Command introduced in Junos OS Release 11.1 for QFX Series.</td>
</tr>
<tr>
<td>slot&gt;</td>
<td>Command introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.</td>
</tr>
<tr>
<td>show chassis routing-engine &lt;bios</td>
<td>Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.</td>
</tr>
<tr>
<td>slot&gt;</td>
<td>Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.</td>
</tr>
<tr>
<td>Syntax (TX Matrix Plus Routers)</td>
<td></td>
</tr>
<tr>
<td>show chassis routing-engine &lt;bios</td>
<td></td>
</tr>
<tr>
<td>slot&gt;</td>
<td>Command introduced in Junos OS Release 1.2 for AFI Services Router.</td>
</tr>
<tr>
<td>Syntax (QFX Series)</td>
<td>sfc option introduced for the TX Matrix Plus router in Junos OS Release in 9.6.</td>
</tr>
<tr>
<td>show chassis routing-engine &lt;interconnect-device name&gt;</td>
<td>Command introduced in Junos OS Release 11.1 for QFX Series.</td>
</tr>
<tr>
<td>&lt;node-device name&gt;</td>
<td>Command introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.</td>
</tr>
<tr>
<td>show chassis routing-engine &lt;bios</td>
<td>Command introduced in Junos OS Release 12.3 for MX2010 3D Universal Edge Routers.</td>
</tr>
<tr>
<td>slot&gt;</td>
<td>Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.</td>
</tr>
<tr>
<td>show chassis routing-engine &lt;bios</td>
<td>Command introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.</td>
</tr>
<tr>
<td>slot&gt;</td>
<td>Command introduced in Junos OS Release 12.3 for MX2020 3D Universal Edge Routers.</td>
</tr>
<tr>
<td>show chassis routing-engine</td>
<td>Command introduced in Junos OS Release 13.2 for MX104 3D Universal Edge Routers.</td>
</tr>
<tr>
<td>Syntax (ACX Series Universal Access Routers)</td>
<td></td>
</tr>
<tr>
<td>show chassis routing-engine</td>
<td></td>
</tr>
</tbody>
</table>
Options

none—Display information about one or more Routing Engines. On a TX Matrix router, display information about all Routing Engines on the TX Matrix router and its attached T640 routers. On a TX Matrix Plus router, display information about all Routing Engines on the TX Matrix Plus router and its attached routers.

all-members—(MX Series routers only) (Optional) Display Routing Engine information for all members of the Virtual Chassis configuration.

bios—(Optional) Display the (BIOS) firmware version.

interconnect-device number—(QFabric systems only) (Optional) Display Routing Engine information for a specified Interconnect device.

lcc number—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display Routing Engine information for a specified T640 router (line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, display Routing Engine information for a specified router (line-card chassis) that is connected to the TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(MX Series routers only) (Optional) Display Routing Engine information for the local Virtual Chassis member.

member member-id—(MX Series routers only) (Optional) Display Routing Engine information for the specified member of the Virtual Chassis configuration. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

node-device number—(QFabric systems only) (Optional) Display Routing Engine information for a specified Node device.

scc—(TX Matrix routers only) (Optional) Display Routing Engine information for the TX Matrix router (switch-card chassis).

stc number—(TX Matrix Plus routers only) (Optional) Display Routing Engine information for the TX Matrix Plus router (or switch-fabric chassis). Replace number with 0.

slot—(Systems with multiple Routing Engines) (Optional) Display information for an individual Routing Engine. Replace slot with 0 or 1. For QFX3500 switches, there is only one Routing Engine, so you do not need to specify the slot number.
**Required Privilege**

- **Level**
  - view

**Related Documentation**
- request chassis routing-engine master on page 175
- Configuring Routing Engine Redundancy
- Switching the Global Master and Backup Roles in a Virtual Chassis Configuration

**List of Sample Output**
- show chassis routing-engine (M5 Router) on page 1074
- show chassis routing-engine (M10 Router) on page 1075
- show chassis routing-engine (M20 Router) on page 1075
- show chassis routing-engine (M40 Router) on page 1076
- show chassis routing-engine (M120 Router) on page 1076
- show chassis routing-engine (M160 Router) on page 1077
- show chassis routing-engine (MX104 Router) on page 1077
- show chassis routing-engine (MX240 Router) on page 1078
- show chassis routing-engine (MX480 Router) on page 1079
- show chassis routing-engine (MX960 Router) on page 1079
- show chassis routing-engine (MX2010 Router) on page 1079
- show chassis routing-engine (MX2020 Router) on page 1080
- show chassis routing-engine (T320 router) on page 1081
- show chassis routing-engine (T640 router) on page 1082
- show chassis routing-engine (T1600 router) on page 1082
- show chassis routing-engine (T4000 router) on page 1083
- show chassis routing-engine (TX Matrix Router) on page 1084
- show chassis routing-engine lcc (TX Matrix Router) on page 1085
- show chassis routing-engine bios (TX Matrix Router) on page 1085
- show chassis routing-engine lcc (TX Matrix Plus Router) on page 1086
- show chassis routing-engine bios (TX Matrix Plus Router) on page 1087
- show chassis routing-engine bios (TX Matrix Plus Router) on page 1088
- show chassis routing-engine (QFX Series) on page 1088
- show chassis routing-engine (PTX Series Packet Transport Router) on page 1088
- show chassis routing-engine (ACX2000 Universal Access Router) on page 1089
- show chassis routing-engine (ACX1000 Universal Access Router) on page 1089

**Output Fields**
Table 153 on page 1072 lists the output fields for the `show chassis routing-engine` command. Output fields are listed in the approximate order in which they appear.

### Table 153: show chassis routing-engine Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>(Systems with single and multiple Routing Engines) Slot number.</td>
</tr>
<tr>
<td>Current state</td>
<td>(Systems with multiple Routing Engines) Current state of the Routing Engine: Master, Backup, or Disabled.</td>
</tr>
<tr>
<td>Election priority</td>
<td>(Systems with multiple Routing Engines) Election priority for the Routing Engine: Master or Backup.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Temperature of the air flowing past the Routing Engine.</td>
</tr>
</tbody>
</table>
Table 153: show chassis routing-engine Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU Temperature</strong></td>
<td>Temperature of the CPU.</td>
</tr>
<tr>
<td><strong>DRAM</strong></td>
<td>Total DRAM available to the Routing Engine's processor. Starting with Junos OS Release 12.3R1, the DRAM field displays both available memory and installed memory.</td>
</tr>
<tr>
<td><strong>Memory utilization</strong></td>
<td>Percentage of Routing Engine memory being used.</td>
</tr>
<tr>
<td><strong>CPU utilization</strong></td>
<td>Information about the Routing Engine's CPU utilization:</td>
</tr>
<tr>
<td></td>
<td>• User—Percentage of CPU time being used by user processes.</td>
</tr>
<tr>
<td></td>
<td>• Background—Percentage of CPU time being used by background processes.</td>
</tr>
<tr>
<td></td>
<td>• Kernel—Percentage of CPU time being used by kernel processes.</td>
</tr>
<tr>
<td></td>
<td>• Interrupt—Percentage of CPU time being used by interrupts.</td>
</tr>
<tr>
<td></td>
<td>• Idle—Percentage of CPU time that is idle.</td>
</tr>
<tr>
<td><strong>Model</strong></td>
<td>Routing Engine model number.</td>
</tr>
<tr>
<td><strong>Serial ID</strong></td>
<td>(Systems with multiple Routing Engines) Identification number of the Routing Engine in this slot.</td>
</tr>
<tr>
<td><strong>Start time</strong></td>
<td>Time at which the Routing Engine started running.</td>
</tr>
<tr>
<td><strong>Uptime</strong></td>
<td>How long the Routing Engine has been running.</td>
</tr>
<tr>
<td><strong>Routing Engine BIOS Version</strong></td>
<td>BIOS version being run by the Routing Engine.</td>
</tr>
</tbody>
</table>
Table 153: show chassis routing-engine Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last reboot reason</td>
<td>Reason for last reboot, including:</td>
</tr>
<tr>
<td></td>
<td>• <strong>power cycle/failure</strong>—Halt of the Routing Engine using the <code>halt</code> command, powering down using the power button on the chassis or any other method (such as removal of the control board or Routing Engine), and then powering back the Routing Engine. A halt of the operating system also occurs if you enter the <code>request system halt</code> command. You can enter this command to halt the system operations on the chassis or specific Routing Engines. To restart the software, press any key on the keyboard.</td>
</tr>
<tr>
<td></td>
<td>• <strong>watchdog</strong>—Reboot due to a hardware watchdog. A watchdog is a hardware monitoring process that examines the health and performance of the router to enable the device to recover from failures. A watchdog checks for problems at certain intervals, and reboots the routing engine if a problem is encountered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>reset button reset</strong>—(Not available on the J Series router or EX Series switch) Reboot due to pressing of the reset button on the Routing Engine.</td>
</tr>
<tr>
<td></td>
<td>• <strong>power button hard power off</strong>—Reboot due to pressing of the power button on the chassis. A powering down of the software also occurs if you enter the <code>request system power-off</code> command. You can enter this command to power down the chassis or specific Routing Engines; you can then restart the software.</td>
</tr>
<tr>
<td></td>
<td>• <strong>misc hardware reason</strong>—Reboot due to miscellaneous hardware reasons.</td>
</tr>
<tr>
<td></td>
<td>• <strong>thermal shutdown</strong>—Reboot due to the router or switch reaching a critical temperature at which point it is unsafe to continue operations.</td>
</tr>
<tr>
<td></td>
<td>• <strong>hard disk failure</strong>—Reboot due to a hard disk or solid-state drive (SSD) failure.</td>
</tr>
<tr>
<td></td>
<td>• <strong>reset from debugger</strong>—Reboot due to reset from the debugger.</td>
</tr>
<tr>
<td></td>
<td>• <strong>chassis control reset</strong>—Restart the chassis process that manages PICs, FPCs, and other hardware components. The chassis control module that runs the Routing Engine performs management and monitoring functions, and it provides a single access point for operational and maintenance functions. A reset of the chassis management process occurs when you enter the <code>restart chassis-control</code> command.</td>
</tr>
<tr>
<td></td>
<td>• <strong>bios auto recovery reset</strong>—Reboot due to a BIOS auto-recovery reset.</td>
</tr>
<tr>
<td></td>
<td>• <strong>could not be determined</strong>—Reboot due to an undetermined reason.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Router rebooted after a normal shutdown</strong>—Reboot due to a normal shutdown. This reason is displayed if the Routing Engine is powered down by pushing and holding the online/offline button on the Routing Engine faceplate for 30 seconds, and then powered back. A reboot of the software also occurs if you enter the <code>request system reboot</code> command. You can enter this command to reboot the chassis or specific Routing Engines.</td>
</tr>
<tr>
<td>Load averages</td>
<td>Routing Engine load averages for the last 1, 5, and 15 minutes.</td>
</tr>
</tbody>
</table>

**Sample Output**

**show chassis routing-engine (M5 Router)**

```
user@host> show chassis routing-engine
Routing Engine status:
  Temperature                  25 degrees C / 77 degrees F
  DRAM                        768 MB
  Memory utilization          21 percent
  CPU utilization:
    User                      0 percent
    Background                0 percent
    Kernel                    0 percent
    Interrupt                 0 percent
```
show chassis routing-engine (M10 Router)

user@host> show chassis routing-engine
Routing Engine status:
  Temperature                 25 degrees C / 77 degrees F
  DRAM                       768 MB
  Memory utilization          21 percent
  CPU utilization:
    User                       0 percent
    Background                 0 percent
    Kernel                     0 percent
    Interrupt                  0 percent
    Idle                      100 percent

Model                          RE-2.0
Serial ID                      31000007349bf701
Start time                     2003-12-04 09:42:17 PST
Uptime                         26 days, 1 hour, 12 minutes, 27 seconds
Last reboot reason             Router rebooted after a normal shutdown
Load averages:                 1 minute   5 minute  15 minute
                                0.00       0.01       0.00

show chassis routing-engine (M20 Router)

user@host> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 29 degrees C / 84 degrees F
    DRAM                       768 MB
    Memory utilization          20 percent
    CPU utilization:
      User                       1 percent
      Background                 0 percent
      Kernel                     2 percent
      Interrupt                  0 percent
      Idle                      97 percent

Model                          RE-2.0
Serial ID                      58000007348d9a01
Start time                     2003-12-30 07:05:47 PST
Uptime                        3 hours, 41 minutes, 14 seconds
Last reboot reason             Router rebooted after a normal shutdown
Load averages:                 1 minute   5 minute  15 minute
                                0.00       0.02       0.00

Routing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 29 degrees C / 84 degrees F
    DRAM                       768 MB
    Memory utilization          0 percent
    CPU utilization:
show chassis routing-engine (M40 Router)

```
user@host> show chassis routing-engine
Routing Engine status:
    Temperature                 25 degrees C / 77 degrees F
    DRAM                       768 MB
    Memory utilization          21 percent
    CPU utilization:
        User                       0 percent
        Background                 0 percent
        Kernel                     0 percent
        Interrupt                  0 percent
        Idle                     100 percent
    Model                          RE-2.0
    Serial ID                      d800000734745701
    Start time                     2003-06-17 16:37:33 PDT
    Uptime                        195 days, 18 hours, 47 minutes, 9 seconds
    Last reboot reason             Router rebooted after a normal shutdown
```

show chassis routing-engine (M120 Router)

```
user@host> show chassis routing-engine
Routing Engine status:
    Slot 0:
        Current state                  Master
        Election priority              Master (default)
        Temperature                 46 degrees C / 114 degrees F
        CPU temperature             44 degrees C / 111 degrees F
        DRAM                      2048 MB
        Memory utilization          18 percent
        CPU utilization:
            User                       0 percent
            Background                 0 percent
            Kernel                     5 percent
            Interrupt                  0 percent
            Idle                      95 percent
        Model                          RE-A-1000
        Serial ID                      1000621154
        Start time                     2006-10-31 17:10:05 PST
        Uptime                         14 minutes, 31 seconds
        Last reboot reason             Router rebooted after a normal shutdown
        Load averages:                 1 minute   5 minute  15 minute
                                      0.02       0.07       0.07
    Slot 1:
        Current state                  Backup
        Election priority              Backup (default)
        Temperature                 45 degrees C / 113 degrees F
```
CPU temperature             42 degrees C / 107 degrees F
DRAM                      2048 MB
Memory utilization          15 percent
CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     0 percent
  Interrupt                  0 percent
  Idle                     100 percent
Model                          RE-A-1000
Serial ID                      1000621151
Start time                     2006-10-31 17:10:04 PST
Uptime                         14 minutes, 30 seconds
Last reboot reason             Router rebooted after a normal shutdown

show chassis routing-engine (M160 Router)

user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state                  Master
  Election priority              Master (default)
  Temperature                 43 degrees C / 109 degrees F
DRAM                      2048 MB
Memory utilization          11 percent
CPU utilization:
  User                       1 percent
  Background                 0 percent
  Kernel                     2 percent
  Interrupt                  0 percent
  Idle                      97 percent
Model                          RE-3.0
Serial ID                      210865700403
Start time                     2003-12-23 12:25:55 PST
Uptime                        6 days, 22 hours, 33 minutes, 24 seconds
Last reboot reason             Router rebooted after a normal shutdown
Load averages:                 1 minute   5 minute  15 minute
  0.24       0.13       0.04
Routing Engine status:
Slot 1:
  Current state                  Backup
  Election priority              Backup (default)
  Temperature                 40 degrees C / 104 degrees F
DRAM                      2048 MB
Memory utilization           9 percent
CPU utilization:
  User                       0 percent
  Background                 0 percent
  Kernel                     0 percent
  Interrupt                  0 percent
  Idle                     100 percent
Model                          RE-3.0
Serial ID                      210865700332
Start time                     2003-12-23 12:25:55 PST
Uptime                        6 days, 22 hours, 33 minutes, 21 seconds
Last reboot reason             Router rebooted after a normal shutdown

show chassis routing-engine (MX104 Router)

user@host> show chassis routing-engine
### Routing Engine status:

**Slot 0:**
- **Current state:** Master
- **Election priority:** Master (default)
- **Temperature:** 32 degrees C / 89 degrees F
- **CPU temperature:** 42 degrees C / 107 degrees F
- **DRAM:** 3840 MB (3840 MB installed)
- **Memory utilization:** 18 percent
- **CPU utilization:**
  - User: 0 percent
  - Background: 0 percent
  - Kernel: 3 percent
  - Interrupt: 2 percent
  - Idle: 94 percent
- **Model:** RE-MX-104
- **Serial ID:** CAAR5925
- **Start time:** 2013-06-05 13:17:08 IST
- **Uptime:** 1 hour, 15 minutes, 8 seconds
- **Last reboot reason:** 0x200: normal shutdown
- **Load averages:**
  - 1 minute: 0.87
  - 5 minute: 0.90
  - 15 minute: 0.41

**Routing Engine status:**

**Slot 1:**
- **Current state:** Backup
- **Election priority:** Backup (default)
- **Temperature:** 32 degrees C / 89 degrees F
- **CPU temperature:** 38 degrees C / 100 degrees F
- **DRAM:** 3840 MB (3840 MB installed)
- **Memory utilization:** 13 percent
- **CPU utilization:**
  - User: 0 percent
  - Background: 0 percent
  - Kernel: 1 percent
  - Interrupt: 2 percent
  - Idle: 97 percent
- **Model:** RE-MX-104
- **Serial ID:** CAAM6369
- **Start time:** 2013-06-05 13:07:37 IST
- **Uptime:** 1 hour, 24 minutes, 34 seconds
- **Last reboot reason:** 0x200: normal shutdown
- **Load averages:**
  - 1 minute: 0.19
  - 5 minute: 0.15
  - 15 minute: 0.06

---

**show chassis routing-engine (MX240 Router)**

```
user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
- **Current state:** Backup
- **Election priority:** Master (default)
- **Temperature:** 40 degrees C / 104 degrees F
- **CPU temperature:** 47 degrees C / 116 degrees F
- **DRAM:** 3584 MB
- **Memory utilization:** 7 percent
- **CPU utilization:**
  - User: 0 percent
  - Background: 0 percent
  - Kernel: 0 percent
  - Interrupt: 0 percent
  - Idle: 100 percent
- **Model:** RE-S-2000
```
<table>
<thead>
<tr>
<th>Serial ID</th>
<th>1000703522</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>2007-12-19 10:35:40 PST</td>
</tr>
<tr>
<td>Uptime</td>
<td>16 days, 3 hours, 15 minutes, 23 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>Router rebooted after a normal shutdown</td>
</tr>
</tbody>
</table>

**show chassis routing-engine (MX480 Router)**

```
user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state    Master
  Election priority Master (default)
  Temperature      41 degrees C / 105 degrees F
  CPU temperature  38 degrees C / 100 degrees F
  DRAM              2048 MB
  Memory utilization 13 percent
  CPU utilization:
    User               0 percent
    Background        0 percent
    Kernel            2 percent
    Interrupt         0 percent
    Idle              98 percent
  Model              RE-S-1300
  Serial ID          1000697044
  Start time         2008-01-04 06:46:08 PST
  Uptime             8 hours, 17 minutes, 16 seconds
  Last reboot reason  Router rebooted after a normal shutdown
```

<table>
<thead>
<tr>
<th>Serial ID</th>
<th>1000617944</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>2006-10-26 12:37:13 PDT</td>
</tr>
<tr>
<td>Uptime</td>
<td>6 days, 4 hours, 59 minutes, 40 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>Router rebooted after a normal shutdown</td>
</tr>
</tbody>
</table>

**show chassis routing-engine (MX960 Router)**

```
user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state    Master
  Election priority Master (default)
  Temperature      37 degrees C / 98 degrees F
  CPU temperature  37 degrees C / 98 degrees F
  DRAM              2048 MB
  Memory utilization 18 percent
  CPU utilization:
    User               0 percent
    Background        0 percent
    Kernel            4 percent
    Interrupt         0 percent
    Idle              96 percent
  Model              RE-S-1300
  Serial ID          1000617944
  Start time         2006-10-26 12:37:13 PDT
  Uptime             6 days, 4 hours, 59 minutes, 40 seconds
  Last reboot reason  Router rebooted after a normal shutdown
  Load averages:     1 minute   5 minute  15 minute
                      0.16       0.08       0.02
```

**show chassis routing-engine (MX2010 Router)**

```
user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state    Master
  Election priority Master (default)
  Temperature      3 degrees C / 37 degrees F
```

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU temperature</td>
<td>3 degrees C / 37 degrees F</td>
</tr>
<tr>
<td>DRAM</td>
<td>17152 MB</td>
</tr>
<tr>
<td>Memory utilization</td>
<td>13 percent</td>
</tr>
<tr>
<td>CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>0 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>4 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>2 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>95 percent</td>
</tr>
<tr>
<td>Model</td>
<td>RE-S-1800x4</td>
</tr>
<tr>
<td>Serial ID</td>
<td>9009099704</td>
</tr>
<tr>
<td>Start time</td>
<td>2012-10-02 14:33:32 PDT</td>
</tr>
<tr>
<td>Uptime</td>
<td>14 hours, 39 minutes, 39 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>Router rebooted after a normal shutdown.</td>
</tr>
<tr>
<td>Load averages:</td>
<td></td>
</tr>
<tr>
<td>1 minute</td>
<td>0.06</td>
</tr>
<tr>
<td>5 minute</td>
<td>0.05</td>
</tr>
<tr>
<td>15 minute</td>
<td>0.01</td>
</tr>
</tbody>
</table>

Routing Engine status:

**Slot 1:**

- **Current state:** Backup
- **Election priority:** Backup (default)
- **Temperature:** 1 degrees C / 33 degrees F
- **CPU temperature:** 2 degrees C / 35 degrees F
- **DRAM:** 17152 MB
- **Memory utilization:** 11 percent
- **CPU utilization:**
  - User: 0 percent
  - Background: 0 percent
  - Kernel: 0 percent
  - Interrupt: 0 percent
  - Idle: 100 percent
- **Model:** RE-S-1800x4
- **Serial ID:** 9009099706
- **Start time:** 2012-10-02 10:36:06 PDT
- **Uptime:** 18 hours, 36 minutes, 57 seconds
- **Last reboot reason:** Router rebooted after a normal shutdown.
- **Load averages:**
  - 1 minute: 0.01
  - 5 minute: 0.00
  - 15 minute: 0.00

**show chassis routing-engine (MX2020 Router)**

```
user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state: Master
  Election priority: Master (default)
  Temperature: 6 degrees C / 42 degrees F
  CPU temperature: 6 degrees C / 42 degrees F
  DRAM: 17152 MB
  Memory utilization: 14 percent
  CPU utilization:
    User: 1 percent
    Background: 0 percent
    Kernel: 7 percent
    Interrupt: 2 percent
    Idle: 91 percent
  Model: RE-S-1800x4
  Serial ID: 9009099704
  Start time: 2012-10-02 11:05:24 PDT
  Uptime: 2 days, 15 hours, 49 minutes, 13 seconds
  Last reboot reason: Router rebooted after a normal shutdown.
  Load averages:
    1 minute: 0.01
    5 minute: 0.00
    15 minute: 0.00
```
Routing Engine status:

<table>
<thead>
<tr>
<th>Slot 1:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Current state</td>
<td>Backup</td>
<td>Backup</td>
</tr>
<tr>
<td>Election priority</td>
<td>Backup (default)</td>
<td>Backup (default)</td>
</tr>
<tr>
<td>Temperature</td>
<td>7 degrees C / 44 degrees F</td>
<td>45 degrees C / 113 degrees F</td>
</tr>
<tr>
<td>CPU temperature</td>
<td>5 degrees C / 41 degrees F</td>
<td>48 degrees C / 118 degrees F</td>
</tr>
<tr>
<td>DRAM</td>
<td>17152 MB</td>
<td>3584 MB</td>
</tr>
<tr>
<td>Memory utilization</td>
<td>12 percent</td>
<td>9 percent</td>
</tr>
<tr>
<td>CPU utilization:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>99 percent</td>
<td>97 percent</td>
</tr>
<tr>
<td>Model</td>
<td>RE-S-1800x4</td>
<td>RE-A-2000</td>
</tr>
<tr>
<td>Serial ID</td>
<td>9009094138</td>
<td>9009010618</td>
</tr>
<tr>
<td>Start time</td>
<td>2012-10-02 11:09:57 PDT</td>
<td>2012-10-10 01:24:05 PDT</td>
</tr>
<tr>
<td>Uptime</td>
<td>2 days, 15 hours, 44 minutes, 27 seconds</td>
<td>5 days, 10 hours, 49 minutes, 23 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>Router rebooted after a normal shutdown.</td>
<td>0x1:power cycle/failure</td>
</tr>
<tr>
<td>Load averages:</td>
<td>1 minute 5 minute 15 minute</td>
<td>1 minute 5 minute 15 minute</td>
</tr>
<tr>
<td></td>
<td>0.00 0.05 0.04</td>
<td>0.00 0.05 0.04</td>
</tr>
</tbody>
</table>

show chassis routing-engine (T320 router)

**user@host> show chassis routing-engine**

Slot 0:

<table>
<thead>
<tr>
<th>Current state</th>
<th>Master</th>
</tr>
</thead>
<tbody>
<tr>
<td>Election priority</td>
<td>Master (default)</td>
</tr>
<tr>
<td>Temperature</td>
<td>51 degrees C / 123 degrees F</td>
</tr>
<tr>
<td>CPU temperature</td>
<td>55 degrees C / 131 degrees F</td>
</tr>
<tr>
<td>DRAM</td>
<td>3584 MB</td>
</tr>
<tr>
<td>Memory utilization</td>
<td>11 percent</td>
</tr>
<tr>
<td>CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>0 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>2 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>97 percent</td>
</tr>
<tr>
<td>Model</td>
<td>RE-A-2000</td>
</tr>
<tr>
<td>Serial ID</td>
<td>9009010618</td>
</tr>
<tr>
<td>Start time</td>
<td>2012-10-10 01:24:05 PDT</td>
</tr>
<tr>
<td>Uptime</td>
<td>5 days, 10 hours, 49 minutes, 23 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>0x1:power cycle/failure</td>
</tr>
<tr>
<td>Load averages:</td>
<td>1 minute 5 minute 15 minute</td>
</tr>
<tr>
<td></td>
<td>0.00 0.05 0.04</td>
</tr>
</tbody>
</table>

Routing Engine status:

<table>
<thead>
<tr>
<th>Slot 1:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Current state</td>
<td>Backup</td>
<td>Backup</td>
</tr>
<tr>
<td>Election priority</td>
<td>Backup (default)</td>
<td>Backup (default)</td>
</tr>
<tr>
<td>Temperature</td>
<td>45 degrees C / 113 degrees F</td>
<td></td>
</tr>
<tr>
<td>CPU temperature</td>
<td>48 degrees C / 118 degrees F</td>
<td></td>
</tr>
<tr>
<td>DRAM</td>
<td>3584 MB</td>
<td>3584 MB</td>
</tr>
<tr>
<td>Memory utilization</td>
<td>9 percent</td>
<td>9 percent</td>
</tr>
<tr>
<td>CPU utilization:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>100 percent</td>
<td>97 percent</td>
</tr>
<tr>
<td>Model</td>
<td>RE-A-2000</td>
<td></td>
</tr>
</tbody>
</table>
show chassis routing-engine (T640 router)

user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state                  Master
  Election priority              Master (default)
  Temperature                 50 degrees C / 122 degrees F
  CPU temperature             58 degrees C / 136 degrees F
  DRAM                      3584 MB
  Memory utilization          14 percent
  CPU utilization:
    User                       1 percent
    Background                 0 percent
    Kernel                     4 percent
    Interrupt                  1 percent
    Idle                      95 percent

  Model                          RE-A-2000
  Serial ID                      1000686556
  Start time                     2012-10-10 01:24:02 PDT
  Uptime                         5 days, 10 hours, 50 minutes, 27 seconds
  Last reboot reason             0x1:power cycle/failure

Routing Engine status:
Slot 1:
  Current state                  Backup
  Election priority              Backup (default)
  Temperature                 44 degrees C / 111 degrees F
  CPU temperature             49 degrees C / 120 degrees F
  DRAM                      3584 MB
  Memory utilization          12 percent
  CPU utilization:
    User                       0 percent
    Background                 0 percent
    Kernel                     0 percent
    Interrupt                  1 percent
    Idle                      99 percent

  Model                          RE-A-2000
  Serial ID                      1000702739
  Start time                     2012-10-10 01:24:02 PDT
  Uptime                         5 days, 10 hours, 50 minutes, 26 seconds
  Last reboot reason             0x1:power cycle/failure

show chassis routing-engine (T1600 router)

user@host> show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state                  Master
  Election priority              Master (default)
  Temperature                 48 degrees C / 118 degrees F
  CPU temperature             58 degrees C / 136 degrees F
  DRAM                      3584 MB
  Memory utilization          13 percent
  CPU utilization:
show chassis routing-engine (T4000 router)

user@host> show chassis routing-engine

Routing Engine status:
Slot 0:
  Current state      Master
  Election priority  Master (default)
  Temperature        33 degrees C / 91 degrees F
  CPU temperature    50 degrees C / 122 degrees F
  DRAM               8960 MB
  Memory utilization 18 percent
  CPU utilization:
    User              0 percent
    Background        0 percent
    Kernel            4 percent
    Interrupt         1 percent
    Idle              95 percent
  Model              RE-DUO-1800
  Serial ID          P737F-002248
  Start time         2012-02-09 22:49:53 PST
  Uptime             2 hours, 21 minutes, 35 seconds
  Last reboot reason  Router rebooted after a normal shutdown.
  Load averages:     1 minute 5 minute 15 minute
                      0.00  0.04  0.00

Routing Engine status:
Slot 1:
  Current state      Backup
  Election priority  Backup (default)
  Temperature        32 degrees C / 89 degrees F
CPU temperature             46 degrees C / 114 degrees F
DRAM                      8960 MB
Memory utilization          24 percent
CPU utilization:
    User                       0 percent
    Background                 0 percent
    Kernel                     0 percent
    Interrupt                  0 percent
    Idle                      99 percent
Model                          RE-DUO-1800
Serial ID                      P737F-002653
Start time                     2012-02-08 20:12:51 PST
Uptime                         1 day, 4 hours, 58 minutes, 28 seconds
Last reboot reason             Router rebooted after a normal shutdown.

show chassis routing-engine (TX Matrix Router)

user@host> show chassis routing-engine
scc-re0:
--------------------------------------------------------------------------
Routing Engine status:
Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 34 degrees C / 93 degrees F
    CPU temperature             33 degrees C / 91 degrees F
    DRAM                      2048 MB
    Memory utilization          12 percent
    CPU utilization:
        User                       0 percent
        Background                 0 percent
        Kernel                     2 percent
        Interrupt                  0 percent
        Idle                      98 percent
    Model                          RE-4.0
    Serial ID                      P11123900153
    Start time                     2004-08-05 18:42:05 PDT
    Uptime                        9 days, 22 hours, 49 minutes, 50 seconds
    Last reboot reason             Router rebooted after a normal shutdown
    Load averages:                 1 minute   5 minute  15 minute
                                    0.00       0.08       0.07

lcc0-re0:
--------------------------------------------------------------------------
Routing Engine status:
Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 33 degrees C / 91 degrees F
    CPU temperature             30 degrees C / 86 degrees F
    DRAM                      2048 MB
    Memory utilization          12 percent
    CPU utilization:
        User                       0 percent
        Background                 0 percent
        Kernel                     1 percent
        Interrupt                  0 percent
        Idle                      98 percent
    Model                          RE-3.0
    Serial ID                      210865700363
    Start time                     2004-08-05 18:42:05 PDT
Uptime: 9 days, 22 hours, 48 minutes, 20 seconds
Last reboot reason: Router rebooted after a normal shutdown
Load averages:

<table>
<thead>
<tr>
<th></th>
<th>1 minute</th>
<th>5 minute</th>
<th>15 minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
</tr>
</tbody>
</table>

lcc2-re0:

Routing Engine status:
Slot 0:
Current state: Master
Election priority: Master (default)
Temperature: 34 degrees C / 93 degrees F
CPU temperature: 35 degrees C / 95 degrees F
DRAM: 2048 MB
Memory utilization: 12 percent
CPU utilization:
User: 0 percent
Background: 0 percent
Kernel: 2 percent
Interrupt: 0 percent
Idle: 98 percent
Model: RE-4.0
Serial ID: P11123900126
Start time: 2004-08-05 18:42:05 PDT
Uptime: 9 days, 22 hours, 49 minutes, 4 seconds
Last reboot reason: Router rebooted after a normal shutdown
Load averages:

<table>
<thead>
<tr>
<th></th>
<th>1 minute</th>
<th>5 minute</th>
<th>15 minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>0.01</td>
<td>0.01</td>
<td>0.00</td>
</tr>
</tbody>
</table>

show chassis routing-engine lcc (TX Matrix Router)

user@host> show chassis routing-engine 0 lcc 0
lcc0-re0:

Routing Engine status:
Slot 0:
Current state: Master
Election priority: Master (default)
Temperature: 34 degrees C / 91 degrees F
CPU temperature: 35 degrees C / 95 degrees F
DRAM: 2048 MB
Memory utilization: 12 percent
CPU utilization:
User: 0 percent
Background: 0 percent
Kernel: 2 percent
Interrupt: 0 percent
Idle: 98 percent
Model: RE-4.0
Serial ID: P110865700363
Start time: 2004-08-05 18:42:05 PDT
Uptime: 7 days, 22 hours, 49 minutes, 6 seconds
Last reboot reason: Router rebooted after a normal shutdown
Load averages:

<table>
<thead>
<tr>
<th></th>
<th>1 minute</th>
<th>5 minute</th>
<th>15 minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

show chassis routing-engine bios (TX Matrix Router)

user@host> show chassis routing-engine bios
scc-re0:
Routing Engine BIOS Version: V1.0.0
lcc0-re0:
-------------------------------------------------------------------------------------
Routing Engine BIOS Version: V1.0.17
lcc2-re0:
-------------------------------------------------------------------------------------
Routing Engine BIOS Version: V1.0.0

show chassis routing-engine (TX Matrix Plus Router)

user@host> show chassis routing-engine
sfc0-re0:
-------------------------------------------------------------------------------------
Routing Engine status:
Slot 0:
  Current state                  Master
  Election priority              Master (default)
  Temperature                 27 degrees C / 80 degrees F
  CPU temperature             42 degrees C / 107 degrees F
  DRAM                      3327 MB
  Memory utilization          12 percent
  CPU utilization:
    User                       0 percent
    Background                 0 percent
    Kernel                     2 percent
    Interrupt                  0 percent
    Idle                     98 percent
  Model                          RE-TXP-SFC
  Serial ID                      737A-1024
  Start time                     2009-05-11 17:39:49 PDT
  Uptime                         3 hours, 45 minutes, 25 seconds
  Last reboot reason             Router rebooted after a normal shutdown.
  Load averages:                 1 minute   5 minute  15 minute
                                   0.00       0.00       0.00
Routing Engine status:
Slot 1:
  Current state                  Backup
  Election priority              Backup (default)
  Temperature                 29 degrees C / 84 degrees F
  CPU temperature             43 degrees C / 109 degrees F
  DRAM                      3327 MB
  Memory utilization          11 percent
  CPU utilization:
    User                       0 percent
    Background                 0 percent
    Kernel                     0 percent
    Interrupt                  0 percent
    Idle                     100 percent
  Model                          RE-TXP-SFC
  Serial ID                      737A-1024
  Start time                     2009-05-11 17:08:54 PDT
  Uptime                         4 hours, 16 minutes, 52 seconds
  Last reboot reason             0x1:power cycle/failure
lcc0-re0:
-------------------------------------------------------------------------------------
Routing Engine status:
Slot 0:
  Current state                  Master
  Election priority              Master (default)
  Temperature                 30 degrees C / 86 degrees F
show chassis routing-engine lcc (TX Matrix Plus Router)

user@host> show chassis routing-engine 0 lcc 0
lcc0-re0:

Routing Engine status:
Slot 0:
    Current state                  Master
    Election priority              Master (default)
    Temperature                 30 degrees C / 86 degrees F
    CPU temperature             43 degrees C / 109 degrees F
    DRAM                        3327 MB
    Memory utilization         9 percent
    CPU utilization:
        User                       0 percent
        Background                 0 percent
        Kernel                     2 percent
        Interrupt                 0 percent
        Idle                      98 percent
    Model                          RE-TXP-LCC
    Serial ID                      737F-1024
    Start time                     2009-05-06 17:31:32 PDT
    Uptime                         5 days, 3 hours, 54 minutes, 19 seconds
    Last reboot reason             Router rebooted after a normal shutdown.
    Load averages:
        1 minute 5 minute 15 minute
        0.00 0.00 0.00

Routing Engine status:
Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
    Temperature                 30 degrees C / 86 degrees F
    CPU temperature             43 degrees C / 109 degrees F
    DRAM                        3327 MB
    Memory utilization         9 percent
    CPU utilization:
        User                       0 percent
        Background                 0 percent
        Kernel                     0 percent
        Interrupt                 0 percent
        Idle                     100 percent
    Model                          RE-TXP-LCC
    Serial ID                      737F-1024
    Start time                     2009-05-11 17:40:32 PDT
    Uptime                         3 hours, 45 minutes, 26 seconds
    Last reboot reason             Router rebooted after a normal shutdown.
    Load averages:
        1 minute 5 minute 15 minute
        0.00 0.00 0.00
Routing Engine status:
Slot 1:
  Current state                  Backup
  Election priority              Backup (default)
  Temperature                 30 degrees C / 86 degrees F
  CPU temperature             43 degrees C / 109 degrees F
  DRAM                      3327 MB
  Memory utilization           9 percent
  CPU utilization:
    User                       0 percent
    Background                 0 percent
    Kernel                     0 percent
    Interrupt                  0 percent
    Idle                     100 percent
  Model                          RE-TXP-LCC
  Serial ID                      737F-1024
  Start time                     2009-05-06 17:31:32 PDT
  Uptime                         5 days, 3 hours, 54 minutes, 59 seconds
  Last reboot reason             Router rebooted after a normal shutdown.

show chassis routing-engine bios (TX Matrix Plus Router)

user@host>  show chassis routing-engine bios
sfc0-re0:
---------------------------------------------------------------------
Routing Engine BIOS Version: V0.0.Z
---------------------------------------------------------------------

lcc0-re0:
---------------------------------------------------------------------
Routing Engine BIOS Version: V0.0.N

show chassis routing-engine (QFX Series)

user@switch>  show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state Master
  Election priority Master (default)
  DRAM 2820 MB
  Memory utilization 49 percent
  CPU utilization:
    User 1 percent
    Background 0 percent
    Kernel 1 percent
    Interrupt 0 percent
    Idle 97 percent
  Model QFX3500-48S4Q
  Serial ID S/N ED3709
  Uptime 3 days, 4 hours, 29 minutes, 42 seconds
  Last reboot reason 0x200:chassis control reset
  Load averages: 1 minute 5 minute 15 minute
  0.37 0.26 0.19

show chassis routing-engine (PTX Series Packet Transport Router)

user@switch>  show chassis routing-engine
Routing Engine status:
Slot 0:
  Current state                  Master
  Election priority              Master (default)
  Temperature                 60 degrees C / 140 degrees F
show chassis routing-engine (ACX2000 Universal Access Router)

user@host> show chassis routing-engine
Routing Engine status:
  Temperature 53 degrees C / 127 degrees F
  DRAM 1536 MB
  Memory utilization 25 percent
  CPU utilization:
    User 0 percent
    Background 0 percent
    Kernel 0 percent
    Interrupt 0 percent
    Idle 99 percent
  Model RE-ACX-2000
  Serial ID P737A-002438
  Start time 2012-05-09 00:57:07 PDT
  Uptime 5 days, 3 hours, 16 minutes, 15 seconds
  Last reboot reason Router rebooted after a normal shutdown.
  Load averages:
    1 minute 5 minute 15 minute
    0.00 0.03 0.05

show chassis routing-engine (ACX1000 Universal Access Router)

user@host> show chassis routing-engine
Routing Engine status:
  Temperature 36 degrees C / 96 degrees F

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAM</td>
<td>768 MB</td>
</tr>
<tr>
<td>Memory utilization</td>
<td>50 percent</td>
</tr>
<tr>
<td>CPU utilization:</td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>3 percent</td>
</tr>
<tr>
<td>Background</td>
<td>0 percent</td>
</tr>
<tr>
<td>Kernel</td>
<td>6 percent</td>
</tr>
<tr>
<td>Interrupt</td>
<td>0 percent</td>
</tr>
<tr>
<td>Idle</td>
<td>91 percent</td>
</tr>
<tr>
<td>Model</td>
<td>RE-ACX-1000</td>
</tr>
<tr>
<td>Start time</td>
<td>2012-05-10 07:12:23 PDT</td>
</tr>
<tr>
<td>Uptime</td>
<td>4 days, 10 hours, 46 minutes, 53 seconds</td>
</tr>
<tr>
<td>Last reboot reason</td>
<td>Router rebooted after a normal shutdown.</td>
</tr>
<tr>
<td>Load averages:</td>
<td>1 minute   5 minute 15 minute</td>
</tr>
<tr>
<td></td>
<td>0.00        0.00        0.00</td>
</tr>
</tbody>
</table>
**Syntax**

```
show log
<filename | user <username>>
```

**Syntax (QFabric System)**

```
show log filename
<device-type (device-id | device-alias)>
```

**Syntax (TX Matrix Routers)**

```
show log
<all-lcc | lcc number | scc>
<filename | user <username>>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
- Option `device-type (device-id | device-alias)` is introduced in Junos OS Release 13.1 for the QFX Series.

**Description**

List log files, display log file contents, or display information about users who have logged in to the router or switch.

**Options**

- `none`—List all log files.

  - `<all-lcc | lcc number | scc>`—(TX Matrix routers only) (Optional) Display logging information about all T640 routers (or line-card chassis) or a specific T640 router (replace `number` with a value from 0 through 3) connected to a TX Matrix router. Or, display logging information about the TX Matrix router (or switch-card chassis).

- `device-type`—(QFabric system only) (Optional) Display log messages for only one of the following device types:
  - `director-device`—Display logs for Director devices.
  - `interconnect-device`—Display logs for Interconnect devices.
  - `node-device`—Display logs for Node devices.

---

**NOTE:** If you specify the `device-type` optional parameter, you must also specify either the `device-id` or `device-alias` optional parameter.

- `(device-id | device-alias)`—If a device type is specified, display logs for a device of that type. Specify either the device ID or the device alias (if configured).
filename—(Optional) Display the log messages in the specified log file. For the routing matrix, the filename must include the chassis information.

NOTE: The filename parameter is mandatory for the QFabric system. If you did not configure a syslog filename, specify the default filename of messages.

user <username>—(Optional) Display logging information about users who have recently logged in to the router or switch. If you include username, display logging information about the specified user.

Required Privilege Level
trace

List of Sample Output
show log on page 1092
show log filename on page 1092
show log filename (QFabric System) on page 1093
show log user on page 1093

Sample Output
show log

user@host> show log
total 57518
-rw-r--r-- 1 root bin 211663 Oct 1 19:44 dcd
-rw-r--r-- 1 root bin 999947 Oct 1 19:41 dcd.0
-rw-r--r-- 1 root bin 999994 Oct 1 17:48 dcd.1
-rw-r--r-- 1 root bin 238815 Oct 1 19:44 rpd
-rw-r--r-- 1 root bin 1049098 Oct 1 18:00 rpd.0
-rw-r--r-- 1 root bin 1061095 Oct 1 12:13 rpd.1
-rw-r--r-- 1 root bin 1052026 Oct 1 06:08 rpd.2
-rw-r--r-- 1 root bin 1056309 Sep 30 18:21 rpd.3
-rw-r--r-- 1 root bin 1056371 Sep 30 14:36 rpd.4
-rw-r--r-- 1 root bin 1056301 Sep 30 10:50 rpd.5
-rw-r--r-- 1 root bin 1056350 Sep 30 07:04 rpd.6
-rw-r--r-- 1 root bin 1048876 Sep 30 03:21 rpd.7
-rw-r--r-- 1 root bin 19656 Oct 1 19:37 wtmp

show log filename

user@host> show log rpd
Oct 1 18:00:18 trace_on: Tracing to /var/log/rpd? started
Oct 1 18:00:18 EVENT <MTU> ds-5/2/0.0 index 24 <Broadcast PointToPoint Multicast
Oct 1 18:00:18
Oct 1 18:00:19 KRT recv len 56 V9 seq 148 op add Type route/if af 2 addr 13.13.13.21 nhop type local nhop 13.13.13.21
Oct 1 18:00:19 KRT recv len 56 V9 seq 149 op add Type route/if af 2 addr 13.13.13.22 nhop type unicast nhop 13.13.13.22
Oct 1 18:00:19 KRT recv len 48 V9 seq 150 op add Type ifaddr index 24 devindex 43
Oct 1 18:00:19 KRT recv len 144 V9 seq 151 op chnge Type ifdev devindex 44
Oct 1 18:00:19 KRT recv len 144 V9 seq 152 op chnge Type ifdev devindex 45
Oct 1 18:00:19 KRT recv len 144 V9 seq 153 op chnge Type ifdev devindex 46
Oct 1 18:00:19 KRT recv len 1272 V9 seq 154 op chnge Type ifdev devindex 47
...

show log filename (QFabric System)

show log messages
user@qfabric> show log messages
Mar 28 18:00:06 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:06 ED1486
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2159)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1486
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC:  @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)
Mar 28 18:00:07 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:07 ED1492
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 2, jnxFruL3Index 0,
jnxFruName PIC:  @ 0/1/*, jnxFruType 11, jnxFruSlot 0, jnxFruOfflineReason 2,
jnxFruLastPowerOff 0, jnxFruLastPowerOn 2191)
Mar 28 18:00:16 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:16 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:27 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:27 ED1486
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
__DCF_default___NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:50 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:50
__DCF_default___NW-INE-0_RE0_ file: UI_COMMIT: User 'root' requested 'commit'
operation (comment: none)
Mar 28 18:00:55 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:00:55 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:01:10 qfabric file: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:01:10 ED1492
file: UI_COMMIT: User 'root' requested 'commit' operation (comment: none)
Mar 28 18:02:37 qfabric chassisd: QFABRIC_INTERNAL_SYSLOG: Mar 28 18:02:37 ED1491
chassisd: CHASSISD_SNMP_TRAP10: SNMP trap generated: FRU power on
(jnxFruContentsIndex 8, jnxFruL1Index 1, jnxFruL2Index 1, jnxFruL3Index 0,
jnxFruName PIC: 48x 10G-SFP+ @ 0/0/*, jnxFruType 11, jnxFruSlot 0,
jnxFruOfflineReason 2, jnxFruLastPowerOff 0, jnxFruLastPowerOn 33809)

show log user

user@host> show log user
darius   mg2546                    Thu Oct  1 19:37   still logged in
darius   mg2529                    Thu Oct  1 19:08 - 19:36  (00:28)
darius   mg2518                    Thu Oct  1 18:53 - 18:58  (00:04)
root     mg1575                    Wed Sep 30 18:39 - 18:41  (00:02)
root     ttyp2    jun.site.per    Wed Sep 30 18:39 - 18:41  (00:02)
alex     ttyp1    192.168.1.2      Wed Sep 30 01:03 - 01:22  (00:19)
show pfe next-hop

Syntax

```
show pfe next-hop
  <interface interface-name>
```  

Syntax (TX Matrix and TX Matrix Plus Routers)

```
show pfe next-hop
  <fpc slot>
  <interface interface-name>
  <lcc number>
```  

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display Packet Forwarding Engine next-hop information.

Options

- **none**—Display all Packet Forwarding Engine next-hop information.

  - **fpc slot**—(TX Matrix and TX Matrix Plus routers only) (Optional) Show the next hops for a Flexible PIC Concentrator (FPC) slot.
    - On a TX Matrix router, if you specify the number of a T640 router by using the **lcc number** option (the recommended method), replace **slot** with a value from 0 through 7. Otherwise, replace **slot** with a value from 0 through 31.
    - On a TX Matrix Plus router, if you specify the number of a T1600 router by using the **lcc number** option (the recommended method), replace **slot** with a value from 0 through 7. Otherwise, replace **slot** with a value from 0 through 31.
    - On a TX Matrix Plus router in the TXP-T1600-3D, TXP-T4000-3D, or TXP-Mixed-LCC-3D configuration, if you specify the number of a T1600 or T4000 router by using the **lcc number** option (the recommended method), replace **slot** with a value from 0 through 7. Otherwise, replace **slot** with a value from 0 through 63.

  For example, the following commands have the same result:

  ```
  user@host> show pfe next-hop fpc 1 lcc 1
  user@host> show pfe next-hop fpc 9
  ```

- **interface interface-name**—(Optional) Display the Packet Forwarding Engine next-hop interface.

- **lcc number**—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display Packet Forwarding Engine next-hop interface for a specific T640 router (or line-card chassis) that is connected to a TX Matrix router. On a TX Matrix Plus router, display Packet Forwarding Engine next-hop interface for the router (or line-card chassis) that is connected to a TX Matrix Plus router.
Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**Required Privilege Level**

admin

**Related Documentation**

- Routing Matrix with TXP-T1600 Configuration
- Routing Matrix with TXP-T1600-3D Configuration
- Routing Matrix with TXP-T4000-3D Configuration
- Overview of a Routing Matrix with TXP-Mixed-LCC-3D Configuration

**List of Sample Output**

show pfe next-hop on page 1096
show pfe next-hop fpc (TX Matrix Router) on page 1096
show pfe next-hop fpc (TX Matrix Plus Router) on page 1096
Sample Output

**show pfe next-hop**

```bash
user@host> show pfe next-hop
Nexthop Info:
<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Interface</th>
<th>Protocol</th>
<th>Encap</th>
<th>Next Hop Addr</th>
<th>MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Mcast</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Bcast</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>Discard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>MDiscard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>Reject</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>192.168.4.60</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>Resolve</td>
<td>fxp0.0</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>127.0.0.1</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>Unicast</td>
<td>fxp0.0</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>11.1.0.1</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>Unicast</td>
<td>at-0/1/0.0</td>
<td>IPv4</td>
<td>ATM SNAP</td>
<td>-</td>
<td>4482</td>
</tr>
</tbody>
</table>

```

**show pfe next-hop fpc (TX Matrix Router)**

```bash
user@host> show pfe next-hop fpc1
Slot 1
Nexthop Info:
<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Interface</th>
<th>Next Hop Addr</th>
<th>Protocol</th>
<th>Encap</th>
<th>MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Mcast</td>
<td>default</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>Bcast</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>Discard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>MDiscard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>Mcast</td>
<td>default</td>
<td>IPv6</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>MDiscard</td>
<td>-</td>
<td>IPv6</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>Reject</td>
<td>-</td>
<td>IPv6</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>Discard</td>
<td>-</td>
<td>None</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>68</td>
<td>Local</td>
<td>192.168.66.113</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>69</td>
<td>Resolve</td>
<td>fxp0.0</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>70</td>
<td>Unicast</td>
<td>fxp0.0</td>
<td>192.168.71.254</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>0</td>
</tr>
<tr>
<td>256</td>
<td>Local</td>
<td>10.71.71.1</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>257</td>
<td>Local</td>
<td>127.0.0.1</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>258</td>
<td>Mcast.local..1</td>
<td>default</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>259</td>
<td>Bcast.local..1</td>
<td>-</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>261</td>
<td>Discard.local..1</td>
<td>-</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>262</td>
<td>MDiscard.local..1</td>
<td>-</td>
<td>IPv4</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>269</td>
<td>Mcast.local..1</td>
<td>default</td>
<td>IPv6</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>271</td>
<td>Discard.local..1</td>
<td>-</td>
<td>IPv6</td>
<td>Unspecified</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**show pfe next-hop fpc (TX Matrix Plus Router)**

```bash
user@host> show pfe next-hop fpc 0
Slot 0
<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Interface</th>
<th>Next Hop Addr</th>
<th>Protocol</th>
<th>Encap</th>
<th>MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Mcast</td>
<td>default</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>32</td>
<td>Bcast</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>34</td>
<td>Discard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>35</td>
<td>MDiscard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Line</th>
<th>Action</th>
<th>Address</th>
<th>Protocol</th>
<th>Interface</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>Reject</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>39</td>
<td>Mcast</td>
<td>default</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>42</td>
<td>Discard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>43</td>
<td>MDiscard</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>44</td>
<td>Reject</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>49</td>
<td>Receive</td>
<td>-</td>
<td>MPLS</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>50</td>
<td>Discard</td>
<td>-</td>
<td>MPLS</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>111</td>
<td>Mcast</td>
<td>.local..1</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>112</td>
<td>Bcast</td>
<td>.local..1</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>114</td>
<td>Discard</td>
<td>.local..1</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>115</td>
<td>MDiscard</td>
<td>.local..1</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>116</td>
<td>Reject</td>
<td>.local..1</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>119</td>
<td>Mcast</td>
<td>.local..1</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>122</td>
<td>Discard</td>
<td>.local..1</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>123</td>
<td>MDiscard</td>
<td>.local..1</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>124</td>
<td>Reject</td>
<td>.local..1</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>191</td>
<td>Mcast</td>
<td>.local..2</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>192</td>
<td>Bcast</td>
<td>.local..2</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>194</td>
<td>Discard</td>
<td>.local..2</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>195</td>
<td>MDiscard</td>
<td>.local..2</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>196</td>
<td>Reject</td>
<td>.local..2</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>322</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>323</td>
<td>Resolve</td>
<td>bcm0.0</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>326</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>327</td>
<td>Resolve</td>
<td>bcm0.0</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>328</td>
<td>Local</td>
<td>-</td>
<td>IPv6</td>
<td>fe80::201:ff:fe01:5</td>
<td>0</td>
</tr>
<tr>
<td>329</td>
<td>Receive</td>
<td>bcm0.0</td>
<td>IPv6</td>
<td>ff02::1:ff01:5</td>
<td>0</td>
</tr>
<tr>
<td>330</td>
<td>Receive</td>
<td>bcm0.0</td>
<td>IPv6</td>
<td>fe80::</td>
<td>0</td>
</tr>
<tr>
<td>331</td>
<td>Resolve</td>
<td>bcm0.0</td>
<td>IPv6</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>332</td>
<td>Local</td>
<td>-</td>
<td>IPv6</td>
<td>fec0::a:1:0:5</td>
<td>0</td>
</tr>
<tr>
<td>333</td>
<td>Receive</td>
<td>bcm0.0</td>
<td>IPv6</td>
<td>ff02::1:ff00:5</td>
<td>0</td>
</tr>
<tr>
<td>334</td>
<td>Receive</td>
<td>bcm0.0</td>
<td>IPv6</td>
<td>fec0::</td>
<td>0</td>
</tr>
<tr>
<td>335</td>
<td>Resolve</td>
<td>bcm0.0</td>
<td>IPv6</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>348</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>192.168.178.4</td>
<td>0</td>
</tr>
<tr>
<td>349</td>
<td>Resolve</td>
<td>em0.0</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>350</td>
<td>Unicast</td>
<td>em0.0</td>
<td>IPv4</td>
<td>192.168.178.126</td>
<td>0</td>
</tr>
<tr>
<td>357</td>
<td>Local</td>
<td>-</td>
<td>IPv6</td>
<td>fe80::201:ff:fe01:5</td>
<td>0</td>
</tr>
<tr>
<td>512</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>10.255.178.11</td>
<td>0</td>
</tr>
<tr>
<td>513</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>127.0.0.1</td>
<td>0</td>
</tr>
<tr>
<td>515</td>
<td>Local</td>
<td>-</td>
<td>IPv6</td>
<td>abcd::10:255:178:11</td>
<td>0</td>
</tr>
<tr>
<td>516</td>
<td>Local</td>
<td>-</td>
<td>IPv6</td>
<td>fe80::200:ff:fe00:0</td>
<td>0</td>
</tr>
<tr>
<td>517</td>
<td>Local</td>
<td>-</td>
<td>IPv6</td>
<td>127.0.0.1</td>
<td>0</td>
</tr>
<tr>
<td>518</td>
<td>Mcast</td>
<td>.local..3</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>519</td>
<td>Bcast</td>
<td>.local..3</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>521</td>
<td>Discard</td>
<td>.local..3</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>522</td>
<td>MDiscard</td>
<td>.local..3</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>523</td>
<td>Reject</td>
<td>.local..3</td>
<td>IPv4</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>531</td>
<td>Mcast</td>
<td>.local..3</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>533</td>
<td>Discard</td>
<td>.local..3</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>534</td>
<td>MDiscard</td>
<td>.local..3</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>535</td>
<td>Reject</td>
<td>.local..3</td>
<td>IPv6</td>
<td>unspecified</td>
<td>0</td>
</tr>
<tr>
<td>539</td>
<td>Mgroup</td>
<td>-</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>540</td>
<td>Bcast</td>
<td>ge-15/0/3.0</td>
<td>IPv4</td>
<td>Ethernet</td>
<td>0</td>
</tr>
<tr>
<td>541</td>
<td>Receive</td>
<td>ge-15/0/3.0</td>
<td>IPv4</td>
<td>14.2.1.0</td>
<td>0</td>
</tr>
<tr>
<td>542</td>
<td>Local</td>
<td>-</td>
<td>IPv4</td>
<td>14.2.1.1</td>
<td>0</td>
</tr>
<tr>
<td>543</td>
<td>Resolve</td>
<td>ge-15/0/3.0</td>
<td>IPv4</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>544</td>
<td>Bcast</td>
<td>ge-31/0/4.0</td>
<td>IPv4</td>
<td>Ethernet</td>
<td>0</td>
</tr>
<tr>
<td>Line</td>
<td>Action</td>
<td>Interface</td>
<td>Address</td>
<td>Protocol</td>
<td>Type</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----------</td>
<td>----------</td>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>545</td>
<td>Receive</td>
<td>ge-31/0/4.0</td>
<td>14.1.1.0</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>546</td>
<td>Local</td>
<td>-</td>
<td>14.1.1.1</td>
<td>IPv4</td>
<td>-</td>
</tr>
<tr>
<td>547</td>
<td>Resolve</td>
<td>ge-31/0/4.0</td>
<td>-</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>548</td>
<td>Unicast</td>
<td>ge-31/0/4.0</td>
<td>14.1.1.2</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>549</td>
<td>Unicast</td>
<td>ge-15/0/3.0</td>
<td>14.2.1.2</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>550</td>
<td>Bcast</td>
<td>ael.0</td>
<td>-</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>551</td>
<td>Receive</td>
<td>ael.0</td>
<td>11.1.1.0</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>552</td>
<td>Local</td>
<td>-</td>
<td>11.1.1.1</td>
<td>IPv4</td>
<td>-</td>
</tr>
<tr>
<td>553</td>
<td>Resolve</td>
<td>ael.0</td>
<td>-</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>554</td>
<td>Aggreg.</td>
<td>ael.0</td>
<td>-</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>555</td>
<td>Unicast</td>
<td>ge-23/0/8.0</td>
<td>11.1.1.2</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>556</td>
<td>Unicast</td>
<td>ge-7/0/9.0</td>
<td>11.1.1.2</td>
<td>IPv4</td>
<td>Ethernet</td>
</tr>
<tr>
<td>557</td>
<td>Aggreg.</td>
<td>ael.0</td>
<td>-</td>
<td>MPLS</td>
<td>Ethernet</td>
</tr>
<tr>
<td>558</td>
<td>Unicast</td>
<td>ge-23/0/8.0</td>
<td>-</td>
<td>MPLS</td>
<td>Ethernet</td>
</tr>
<tr>
<td>559</td>
<td>Unicast</td>
<td>ge-7/0/9.0</td>
<td>-</td>
<td>MPLS</td>
<td>Ethernet</td>
</tr>
<tr>
<td>560</td>
<td>Aggreg.</td>
<td>ael.0</td>
<td>-</td>
<td>MPLS</td>
<td>Ethernet</td>
</tr>
<tr>
<td>561</td>
<td>Unicast</td>
<td>ge-23/0/8.0</td>
<td>-</td>
<td>MPLS</td>
<td>Ethernet</td>
</tr>
<tr>
<td>562</td>
<td>Unicast</td>
<td>ge-7/0/9.0</td>
<td>-</td>
<td>MPLS</td>
<td>Ethernet</td>
</tr>
</tbody>
</table>
### show pfe route

**Syntax**

```plaintext
show pfe route <<inet6 | ip | iso> <prefix prefix> | <table <table-name> | <index index> | <prefix prefix> | <mpls> | <summary>
```

**Syntax (EX Series Switch and QFX Series)**

```plaintext
show pfe route <<inet6 | ip> <prefix prefix> | <table <table-name> | <index index> | <prefix prefix> | <mpls> | <summary>
```

**Syntax (TX Matrix and TX Matrix Plus Routers)**

```plaintext
show pfe route <<fpc slot> <<inet6 | ip | iso> <prefix prefix> | <table <table-name> | <index index> | <prefix prefix> | <lcc number> | <mpls> | <summary>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display the routes in the Packet Forwarding Engine forwarding table. The Packet Forwarding Engine forwards packets between input and output interfaces.

**Options**

- `none`—Display all Packet Forwarding Engine forwarding table information.
- `fpc slot`—(TX Matrix and TX Matrix Plus routers only) (Optional) Show the next hops for a Flexible PIC Concentrator (FPC) slot.
  - On a TX Matrix router, if you specify the number of a T640 router by using the `lcc number` option (the recommended method), replace `slot` with a value from 0 through 7. Otherwise, replace `slot` with a value from 0 through 31.
  - On a TX Matrix Plus router, if you specify the number of a T1600 router by using the `lcc number` option (the recommended method), replace `slot` with a value from 0 through 7. Otherwise, replace `slot` with a value from 0 through 31.
  - On a TX Matrix Plus router in the TXP-T1600-3D, TXP-T4000-3D, or TXP-Mixed-LCC-3D configuration, if you specify the number of a T1600 or T4000 router by using the `lcc number` option (the recommended method), replace `slot`
with a value from 0 through 7. Otherwise, replace slot with a value from 0 through 63.

For example, the following commands have the same result:

```
user@host> show pfe route fpc 1 lcc 1
user@host> show pfe route fpc 9
```

**index** *(Optional)* Display table index.

**inet6** *(Optional)* Display Packet Forwarding Engine IPv6 routes.

**ip** *(Optional)* Display Packet Forwarding Engine IPv4 routes.

**iso** *(Optional)* Display ISO version routing tables.

**lcc number** *(TX Matrix and TX Matrix Plus routers only) *(Optional)* On a TX Matrix router, the slot number of the T640 router (or line-card chassis) that houses the FPC. On a TX Matrix Plus router, the slot number of the router (line-card chassis) that houses the FPC.

Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**mpls** *(Optional)* Display Packet Forwarding Engine MPLS information.

**prefix prefix** *(Optional)* IPv4 or IPv6 prefix for which to show table entries.

**summary** *(Optional)* Display summary of Packet Forwarding Engine information.

**table <table-name>** *(Optional)* Display table information.

**Required Privilege Level**

`admin`

**Related Documentation**

- `Routing Matrix with TXP-T1600 Configuration`
- `Routing Matrix with TXP-T1600-3D Configuration`
- `Routing Matrix with TXP-T4000-3D Configuration`
- `Overview of a Routing Matrix with TXP-Mixed-LCC-3D Configuration`

**List of Sample Output**

`show pfe route ip on page 1101`
Sample Output

show pfe route ip

user@host> show pfe route ip

IPv4 Route Table 0, default.0, 0x0:

<table>
<thead>
<tr>
<th>Destination</th>
<th>NH IP Addr</th>
<th>Type</th>
<th>NH ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td>Discard</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>127.0.0.1</td>
<td>Local</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>172.16/12</td>
<td>192.168.71.254</td>
<td>Unicast</td>
<td>68</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>192.168.0/18</td>
<td>192.168.71.254</td>
<td>Unicast</td>
<td>68</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>192.168.40/22</td>
<td>192.168.71.254</td>
<td>Unicast</td>
<td>68</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>192.168.64/18</td>
<td>192.168.71.254</td>
<td>Unicast</td>
<td>68</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>192.168.64/21</td>
<td></td>
<td>Resolve</td>
<td>67</td>
<td>fxp0.0</td>
</tr>
<tr>
<td>192.168.71.249</td>
<td>192.168.71.249</td>
<td>Local</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>192.168.220.0/30</td>
<td></td>
<td>Resolve</td>
<td>303</td>
<td>fe-0/0/0.0</td>
</tr>
<tr>
<td>192.168.220.0</td>
<td>192.168.220.0</td>
<td>Receive</td>
<td>301</td>
<td>fe-0/0/0.0</td>
</tr>
<tr>
<td>224.0.0.1</td>
<td></td>
<td>Mcast</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>255.255.255.255</td>
<td></td>
<td>Bcast</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

...

show pfe route iso

user@host# show pfe route iso

CLNS Route Table 0, CLNP.0, 0x0:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>NH ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Reject</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>47.0005.80ff.f800.0000.0108.0001.0102.5508.2159/152</td>
<td>Local</td>
<td>514</td>
<td></td>
</tr>
<tr>
<td>49.0001.00a0.c96b.c491/72</td>
<td>Local</td>
<td>536</td>
<td></td>
</tr>
</tbody>
</table>

show pfe route lcc summary (TX Matrix Router)

user@host> show pfe route lcc 2 summary

Slot 0

IPv4 Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>43</td>
<td>3081</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>281</td>
</tr>
</tbody>
</table>

MPLS Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td>68</td>
</tr>
</tbody>
</table>

IPV6 Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>9</td>
<td>717</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>389</td>
</tr>
</tbody>
</table>
### Slot 1

**IPv4 Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>43</td>
<td>3081</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>281</td>
</tr>
</tbody>
</table>

**MPLS Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td>68</td>
</tr>
</tbody>
</table>

**IPV6 Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>9</td>
<td>717</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>389</td>
</tr>
</tbody>
</table>

### Slot 16

**IPv4 Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>41</td>
<td>2938</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>281</td>
</tr>
</tbody>
</table>

**MPLS Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td>68</td>
</tr>
</tbody>
</table>

**IPV6 Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>9</td>
<td>717</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>389</td>
</tr>
</tbody>
</table>

### Slot 17

**IPv4 Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>41</td>
<td>2938</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>281</td>
</tr>
</tbody>
</table>

**MPLS Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td>68</td>
</tr>
</tbody>
</table>

**IPV6 Route Tables:**

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show pfe route lcc summary (TX Matrix Plus Router)

user@host> show pfe route lcc 2 summary

Slot 0

IPv4 Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>25</td>
<td>2266</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>815</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>545</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>453</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>1371</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>453</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
<td>1187</td>
</tr>
</tbody>
</table>

MPLS Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td>88</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>452</td>
</tr>
</tbody>
</table>

IPv6 Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>7</td>
<td>697</td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>1305</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>385</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>385</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>385</td>
</tr>
<tr>
<td>6</td>
<td>18</td>
<td>1833</td>
</tr>
</tbody>
</table>

Slot 6

IPv4 Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>25</td>
<td>2266</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>815</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>545</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>453</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>1371</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>453</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
<td>1187</td>
</tr>
</tbody>
</table>

MPLS Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
<td>88</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>452</td>
</tr>
</tbody>
</table>

IPv6 Route Tables:

<table>
<thead>
<tr>
<th>Index</th>
<th>Routes</th>
<th>Size(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>7</td>
<td>697</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1</td>
<td>13</td>
<td>1305</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>385</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>385</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>385</td>
</tr>
<tr>
<td>6</td>
<td>18</td>
<td>1833</td>
</tr>
</tbody>
</table>

...
**show pfe terse**

**Syntax**

```
show pfe terse
```

**Syntax (TX Matrix and TX Matrix Plus Router)**

```
show pfe terse
<lcc number | scc>
<sfc number>
```

**Syntax (MX Series Router)**

```
show pfe terse
<all-members>
<local>
<member member-id>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display Packet Forwarding Engine status information.

**Options**

- `none`—Display brief information about the Packet Forwarding Engine.

- `all-members`—(MX Series routers only) (Optional) Display Packet Forwarding Engine status information for all members in the Virtual Chassis configuration.

- `lcc number`—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display Packet Forwarding Engine information for a T640 router (or line-card chassis) that is connected to a TX Matrix router. On a TX Matrix Plus router, display Packet Forwarding Engine information for the router (or line-card chassis) that is connected to a TX Matrix Plus router.

  Replace `number` with the following values depending on the LCC configuration:

  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

- `local`—(MX Series routers only) (Optional) Display Packet Forwarding Engine status information for the local Virtual Chassis member.

- `member member-id`—(MX Series routers only) (Optional) Display Packet Forwarding Engine status information for the specified member of the Virtual Chassis configuration. Replace `member-id` with a value of 0 or 1.

- `scc`—(TX Matrix routers only) (Optional) Display Packet Forwarding Engine information for the TX Matrix router (or switch-card chassis).
**sfc**—(TX Matrix Plus routers only) (Optional) Display Packet Forwarding Engine information for the TX Matrix Plus router (or switch-fabric chassis).

**Required Privilege Level**

- **admin**

**List of Sample Output**

- `show pfe terse (TX Matrix Router) on page 1106`
- `show pfe terse (TX Matrix Plus Router) on page 1106`
- `show pfe terse sfc (TX Matrix Plus Router) on page 1106`

**Sample Output**

**show pfe terse (TX Matrix Router)**

```
user@host> show pfe terse
Slot Type Slot    State   Flags Uptime
0  SFM  Present Online  0x0bf 01:25:42
2  SFM  Present Online  0x0bf 01:25:40
0  FPC  Present Online  0x102 01:25:57
1  FPC  Present Online  0x102 01:25:55
2  FPC  Present Online  0x102 01:25:53
```

**show pfe terse (TX Matrix Plus Router)**

```
user@host> show pfe terse
sfc0-re0:
--------------------------------------------------------------------------
Slot Type Slot      State     Uptime
0   LCC  Present   Online    2d 05:26
lcc0-re0:
--------------------------------------------------------------------------
Slot Type Slot      State     Uptime
0   GFPC Present   Online    2d 05:25
1   GFPC Present   Online    2d 05:25
```

**show pfe terse sfc (TX Matrix Plus Router)**

```
user@host> show pfe terse sfc 0
sfc0-re0:
--------------------------------------------------------------------------
Slot Type Slot      State     Uptime
0   LCC  Present   Online    2d 05:25
```
show system alarms

Syntax

show system alarms

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display active system alarms.

Options

This command has no options.

Additional Information

System alarms are preset. They include a configuration alarm that appears when no rescue configuration alarm is set and a license alarm that appears when a software feature is configured and no valid license is configured for the feature. For more information about system alarms, see the Junos OS Administration Library for Routing Devices.

In Junos OS release 11.1 and later, alarms for fans also show the slot number of the fans in the CLI output.

Starting with Junos OS Release 13.2, you can view degraded fabric alarms on a routing matrix based on TX Matrix Plus router with 3D SIBs. The alarm indicates that the source FPC is running with a degraded fabric condition. This alarm is an early warning of a possible fabric black-hole condition. When the degraded fabric alarm is raised on the source FPC, you can take remedial action to avoid a fabric black-hole condition. The degraded fabric alarm is raised on the source FPC if both the following conditions are met:

- The active Packet Forwarding Engine destinations are reachable on one or no active switching planes.
- At least one of the inactive switching planes has a fault that causes the destination Packet Forwarding Engine to become unreachable.

Required Privilege

admin

List of Sample Output

show system alarms on page 1107
show system alarms (Fan Tray) on page 1108
show system alarms (QFX Series) on page 1108
show system alarms (TX Matrix Plus router with 3D SIBs) on page 1108

Sample Output

show system alarms

user@host> show system alarms
2 alarms currently active

<table>
<thead>
<tr>
<th>Alarm time</th>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-02-24 17:29:34 UTC</td>
<td>Minor</td>
<td>IPsec VPN tunneling usage requires a</td>
</tr>
</tbody>
</table>
show system alarms (Fan Tray)

```plaintext
user@host> show system alarms
4 alarms currently active
Alarm time               Class  Description
2010-11-11 20:27:38 UTC  Major  Side Fan Tray 7 Failure
2010-11-11 20:27:13 UTC  Minor  Side Fan Tray 7 Overspeed
2010-11-11 20:27:13 UTC  Major  Side Fan Tray 5 Failure
2010-11-11 20:27:13 UTC  Major  Side Fan Tray 0 Failure
```

show system alarms (QFX Series)

```plaintext
user@switches> show system alarms
2 alarms currently active
Alarm time Class Description
2005-02-24 17:29:34 UTC Minor Rescue configuration is not sent
```

show system alarms (TX Matrix Plus router with 3D SIBs)

```plaintext
user@router> show system alarms
sfc0-re0:
-------------------------------------------------------------------------
2 alarms currently active
Alarm time               Class  Description
2013-05-08 18:13:58 UTC  Major  LCC 0 Major Errors
2013-05-08 17:48:46 UTC  Major  LCC 7 Major Errors
lcc0-re1:
-------------------------------------------------------------------------
1 alarm currently active
Alarm time               Class  Description
2013-05-08 18:19:24 UTC  Major  FPC 1 degraded fabric condition detected
lcc7-re0:
-------------------------------------------------------------------------
1 alarm currently active
Alarm time               Class  Description
2013-05-08 18:19:24 UTC  Major  FPC 7 degraded fabric condition detected
```
show system audit

Syntax

show system audit
<root-only>

Syntax (EX Series Switch and MX Series Router)

show system audit
<all-members>
<local>
<member member-id>
<root-only>

Syntax (TX Matrix Router)

show system audit
<all-lcc | lcc number | scc>
<root-only>

Syntax (TX Matrix Plus Router)

show system audit
<all-chassis | all-lcc | lcc number | sfc number>
<root-only>

Syntax (QFX Series)

show system audit
<infrastructure name | interconnect-device name | node-group name | root-only>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display the state and checksum values for file systems.

Options

none—Display the state and checksum values for all file systems.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display file system MD5 hash and permissions information for all of the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display file system MD5 hash and permissions information for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display file system MD5 hash and permissions information for all T1600 or T4000 routers connected to the TX Matrix Plus router.

all-members—(EX4200 switch, QFX Series, and MX Series routers only) (Optional) Display file system MD5 hash and permissions information on all members of the Virtual Chassis configuration.

lcc number—(TX Matrix and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display file system MD5 hash and permissions information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display file system MD5 hash and permissions information for a specific router that is connected to the TX Matrix Plus router.
Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**infrastructure name**—(QFabric systems only) (Optional) Display file system MD5 hash and permissions information for a fabric control Routing Engine or a fabric control Routing Engine.

**interconnect-device name**—(QFabric systems only) (Optional) Display file system MD5 hash and permissions information for the Interconnect device.

**local**—(EX4200 switch, QFX Series, and MX Series routers only) (Optional) Display file system MD5 hash and permissions information on the local Virtual Chassis member.

**member-member-id**—(EX4200 switch, QFX Series, and MX Series routers only) (Optional) Display file system MD5 hash and permissions information on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace **member-id** with a value from 0 through 9. For an MX Series Virtual Chassis, replace **member-id** with a value of 0 or 1.

**node-group name**—(QFabric systems only) (Optional) Display file system MD5 hash and permissions information for the Node group

**root-only**—(Optional) Check only the root (/) file system. On a QFabric system, you can check the root (/) file system on the infrastructure (fabric manager Routing Engine and fabric control Routing Engine), Interconnect device, or Node group.

**scc**—(TX Matrix routers only) (Optional) Display file system MD5 hash and permissions information for the TX Matrix router (or switch-card chassis).

**sfc number**—(TX Matrix Plus routers only) (Optional) Display file system MD5 hash and permissions information for the TX Matrix Plus router (or switch-fabric chassis). Replace number with 0.

**Additional Information**

To redirect the output to a file, issue the following command:

```
ssh device-name 'show system audit root-only' > output-file
```

If you save the output of the **show system audit root-only** command to a file, you can compare it to subsequent output from the command to determine whether anything has changed.
By default, when you issue the `show system audit` command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

**Required Privilege Level**

- admin

**List of Sample Output**

- `show system audit root-only` on page 1111
- `show system audit lcc (TX Matrix Router)` on page 1111
- `show system audit lcc (TX Matrix Plus Router)` on page 1113
- `show system audit root-only (QFX3500 Switch)` on page 1115

**Sample Output**

**show system audit root-only**

```
user@host> show system audit root-only
#
#   user: root
#   machine: my-host
#   tree: /
#date: Fri Feb 11 21:21:46 2000
#
./  /set type=file uid=0 gid=0 mode=0775 nlink=1
  .  /set type=dir uid=0 gid=0 mode=07455 nlink=1
  .cshrc  /set type=file uid=0 gid=0 mode=0755 nlink=1
  ./md5digest=f414e06feaa6bd646244bb98e13d6e6226
  ./kernel.jkernel.backup  /set type=file uid=0 gid=0 mode=0755
  ./md5digest=2c343cf0bd9fae8f04f78604feed7aa4
  ./profile  /set type=file uid=0 gid=0 mode=0755 nlink=1
  ./md5digest=55a1e3c6c67789c9d31c2113f670
COPYRIGHT  /set type=file uid=0 gid=0 mode=0444 nlink=1
  ./md5digest=7df8bc77dce71382ea73eb0e9a9243
boot.config  /set type=file uid=0 gid=0 mode=0755 nlink=1
  ./md5digest=939182975.0
boot.help  /set type=file uid=0 gid=0 mode=0755 nlink=1
  ./md5digest=939182975.0
compat  /set type=link uid=0 gid=0 mode=0777 nlink=1
  ./link=/usr/compat
kernel  /set type=file uid=0 gid=0 mode=0755 nlink=1
  ./md5digest=1a2a8aff2f678a918ba099e2f8427e
kernel.avr  /set type=file uid=0 gid=0 mode=0755 nlink=1
  ./md5digest=2c343cf0bd9fae8f04f78604feed7aa4
kernel.config  /set type=file uid=0 gid=0 mode=0755 nlink=1
  ./md5digest=939182975.0
sys  /set type=link uid=0 gid=0 mode=0777 nlink=1
  ./link=/usr/src/sys
```

**show system audit lcc (TX Matrix Router)**

```
user@host> show system audit lcc
lcc2-re0:

--------------------------------------------------------------------------
#   user: root
--------------------------------------------------------------------------
```
# machine: rodin-lcc2
# tree: /
# date: Mon Sep 13 11:55:33 2004

# .
/set type=file uid=0 gid=0 mode=0555 nlink=1 flags=None
  type=dir nlink=20 size=512 time=1094982121.0
  COPYRIGHT mode=0644 size=4735 time=986012708.0 \ 
  md5digest=78396df1404ad742e6eb1be28f0cd63b
/kernel type=link mode=0700 size=17 time=1090266262.0 \ 
  link=/packages/jkernel

# ./altconfig
altconfig type=dir nlink=2 size=512 time=1089801320.0
# ./altconfig
..   

# ./altroot
altroot type=dir nlink=2 size=512 time=1089801320.0
# ./altroot
..

# ./b
b type=dir mode=0755 nlink=2 size=512 time=1093961429.0
# ./b
..

# ./bin
/set type=file uid=0 gid=0 mode=0700 nlink=1 flags=None
/bin type=dir mode=0755 nlink=2 size=512 time=1089843059.0
  [ link=/packages/mnt/jbase/bin/test
  cat type=link size=28 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/cat
  chmod type=link size=29 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/chmod
  cp type=link size=26 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/cp
  csh type=link size=27 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/csh
  date type=link size=28 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/date
  dd type=link size=26 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/dd
  df type=link size=26 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/df
  echo type=link size=28 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/echo
  ed type=link size=26 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/ed
  expr type=link size=28 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/expr
  hostname type=link size=32 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/hostname
  kill type=link size=28 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/kill
  ln type=link size=26 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/ln
  ls type=link size=26 time=1090266270.0 \ 
    link=/packages/mnt/jbase/bin/ls
mkdir       type=link size=29 time=1090266270.0 \
link=/packages/mnt/jbase/bin/mkdir
mv          type=link size=26 time=1090266270.0 \
link=/packages/mnt/jbase/bin/mv
ps          type=link size=26 time=1090266270.0 \
link=/packages/mnt/jbase/bin/ps
pwd         type=link size=27 time=1090266270.0 \
link=/packages/mnt/jbase/bin/pwd
rcp         type=link size=27 time=1090266270.0 \
link=/packages/mnt/jbase/bin/rcp
red         type=link size=26 time=1090266270.0 \
link=/packages/mnt/jbase/bin/ed
rm          type=link size=26 time=1090266270.0 \
link=/packages/mnt/jbase/bin/rm
rmdir       type=link size=29 time=1090266270.0 \
link=/packages/mnt/jbase/bin/rmdir
sh          type=link size=26 time=1090266270.0 \
link=/packages/mnt/jbase/bin/sh
sleep       type=link size=29 time=1090266270.0 \
link=/packages/mnt/jbase/bin/sleep
stty        type=link size=28 time=1090266270.0 \
link=/packages/mnt/jbase/bin/stty
sync        type=link size=28 time=1090266270.0 \
link=/packages/mnt/jbase/bin/sync
tcsh        type=link size=27 time=1090266270.0 \
link=/packages/mnt/jbase/bin/tcsh
test        type=link size=28 time=1090266270.0 \
link=/packages/mnt/jbase/bin/test

# ./bin
...

# ./boot

boot            type=dir mode=0555 nlink=3 size=512 time=1094978286.0 \
md5digest=6f780822dd4ae482a20462b66e542cca
boot1          mode=0555 size=512 time=1094978294.0 \
md5digest=8d112b09df342cd0b60fadbdcde8e07
boot2          mode=0555 size=7680 time=1094978294.0 \
md5digest=28eb58c4068c6b8571e1484f9e028e4
kgzldr.o      size=5996 time=1094982121.0 \
md5digest=c53dc948eb07e2adeb0413ec4634a3
loader        mode=0555 size=163840 time=1094978298.0 \
md5digest=82d9dc23d1033476bbfb61bb7264c4fed
loader.4th    size=9237 time=986013631.0 \
md5digest=43144391465ad50267d31e0a320be1de

show system audit lcc (TX Matrix Plus Router)

user@host>  show system audit all-chassis

sfc0-re0:  
-------------------------------------------------------------------------
  # user: root
  # machine: finalfive
  # tree: /
# date: Mon May 18 00:13:16 2009

# .
/set type=file uid=0 gid=0 mode=0755 nlink=1 flags=none
  type=dir nlink=23 size=512 time=1242347096.0
/COPYRIGHT mode=0644 size=6196 time=1168587741.0  \\md5digest=bbad415ec29bbed9b383537100412c
/kernel type=link size=17 time=1242347011.0 link=/packages/jkernel
/staging type=link mode=0777 size=8 time=1242346935.0 link=/var/tmp
# ../.snap
./.snap           type=dir mode=0775 nlink=2 size=512 time=1242346922.0
# ../.snap
  ..

# ./altconfig
/altconfig       type=dir mode=0775 nlink=2 size=512 time=1242346922.0
# ./altconfig
  ..

# ./altroot
/altroot         type=dir mode=0775 nlink=2 size=512 time=1242346922.0
# ./altroot
  ..

# ./bin
/bin             type=dir nlink=2 size=512 time=1242346944.0
  133 type=link size=28 time=1242346942.0  \\link=/packages/mnt/jbase/bin/test
  cat type=link size=27 time=1242346941.0  \\link=/packages/mnt/jbase/bin/cat
  chflags type=link size=31 time=1242346941.0  \\link=/packages/mnt/jbase/bin/chflags
  chmod type=link size=29 time=1242346941.0  \\link=/packages/mnt/jbase/bin/chmod
  cp type=link size=26 time=1242346941.0  \\link=/packages/mnt/jbase/bin/cp
  csh type=link size=27 time=1242346941.0  \\link=/packages/mnt/jbase/bin/csh
  date type=link size=28 time=1242346941.0  \\link=/packages/mnt/jbase/bin/date
  dd type=link size=26 time=1242346941.0  \\link=/packages/mnt/jbase/bin/dd
  df type=link size=26 time=1242346941.0  \\link=/packages/mnt/jbase/bin/df
  echo type=link size=28 time=1242346941.0  \\link=/packages/mnt/jbase/bin/echo
  ed type=link size=26 time=1242346941.0  \\link=/packages/mnt/jbase/bin/ed
  expr type=link size=28 time=1242346941.0  \\link=/packages/mnt/jbase/bin/expr
  hostname type=link size=32 time=1242346941.0  \\link=/packages/mnt/jbase/bin/hostname
  kill type=link size=28 time=1242346941.0  \\link=/packages/mnt/jbase/bin/kill
  ln type=link size=26 time=1242346941.0  \\link=/packages/mnt/jbase/bin/ln
  ls type=link size=26 time=1242346941.0  \\link=/packages/mnt/jbase/bin/ls
mkdir type=link size=29 time=1242346941.0 \\
link=/packages/mnt/jbase/bin/ls

mv type=link size=26 time=1242346941.0 \\
link=/packages/mnt/jbase/bin/mv

pax type=link size=27 time=1242346944.0 \\
link=/packages/mnt/jbase/bin/pax

ps type=link size=26 time=1242346941.0 \\
link=/packages/mnt/jbase/bin/ps

pwd type=link size=27 time=1242346941.0 \\
link=/packages/mnt/jbase/bin/pwd

cp type=link size=27 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/cp

red type=link size=26 time=1242346941.0 \\
link=/packages/mnt/jbase/bin/red

cast type=link size=26 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/cast

rm type=link size=26 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/rm

csr type=link size=27 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/csr

sh type=link size=26 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/sh

sleep type=link size=29 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/sleep

stty type=link size=28 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/stty

sync type=link size=28 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/sync
	
tcsh type=link size=27 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/csh

test type=link size=28 time=1242346942.0 \\
link=/packages/mnt/jbase/bin/test

# ./bin

show system audit root-only (QFX3500 Switch)

user@switch> show system audit root-only
#       user: root
#    machine: my-host
#     tree: /
#       date: Fri Feb 11 21:21:46 2000
# .
/.set type=file uid=0 gid=0 mode=0755 nlink=1
  .type=dir nlink=23 time=1024 time=950252640.0
  .cshrc uid=3 gid=7 mode=0644 size=177 time=939182975.0 \ 
    md5digest=f414e06f8d64624b89de136e6226
  .kernel.jkernel.backup \ 
    mode=0744 time=1934552 time=944688902.0 \ 
    md5digest=2c343cf0b9f8e8f04f78604feed7a4
  .profile uid=3 gid=7 mode=0644 nlink=2 time=137 time=939182975.0 \ 
    md5digest=55a1e3c6e67789c9d5acccelara39f670
COPYRIGHT uid=3 gid=7 mode=0444 size=3425 time=939182975.0 \ 
    md5digest=7df8b77dceee71382e7a80a3e69243
  boot.config mode=0644 size=3 time=945902618.0 \ 
    md5digest=93d229393ed36777333aa4053d2cbb40
  boot.help uid=3 gid=7 mode=0444 size=411 time=939182876.0 \ 
    md5digest=9b712635734caee753f4179ab59988e
  compat type=link mode=0777 size=11 time=915249058.0 \ 
    link=/usr/compat
  kernel mode=0444 size=1947607 time=950230892.0 \ 

md5digest=1a2a8aff2fec678a918ba0d6bf063980
kernel.avr uid=1112 size=1947642 time=950252597.0 \ md5digest=82e1637682d58ec28964dfee7fccc62e
kernel.config \ mode=0644 size=0 time=915149058.0 \ md5digest=d41d8cd98f00b204e9800998e882652e
sys type=link mode=0777 size=11 time=915149029.0 \ link=usr/src/sys
show system buffers

Syntax  
show system buffers

Syntax (EX Series)  
show system buffers
<all-members>
<local>
<member member-id>

Syntax (TX Matrix Router)  
show system buffers
<all-chassis | all-lcc | lcc number | scc>

Syntax (TX Matrix Plus Router)  
show system buffers
<all-chassis | all-lcc | lcc number | sfc number>

Syntax (MX Series Router)  
show system buffers
<all-members>
<local>
<member member-id>

Syntax (QFX Series)  
show system buffers
<infrastructure name | interconnect-device name | node-group name | root-only (infrastructure name | interconnect-device name | node-group name)>

Release Information  
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Display information about the buffer pool that the Routing Engine uses for local traffic. Local traffic is the routing and management traffic that is exchanged between the Routing Engine and the Packet Forwarding Engine within the router or switch, as well as the routing and management traffic from IP (that is, from OSPF, BGP, SNMP, ping operations, and so on).

Options  
none—Show all buffer statistics.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show buffer statistics for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, show buffer statistics for all routers connected to the TX Matrix Plus router.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Show buffer statistics for all of the chassis.

all-members—(EX4200 switches and MX Series routers only) (Optional) Show buffer statistics for all members of the Virtual Chassis configuration.

infrastructure name—(QFabric systems only) (Optional) Show buffer statistics for a fabric control Routing Engine or a fabric control Routing Engine.
**interconnect-device name**—(QFabric systems only) (Optional) Show buffer statistics for the Interconnect device.

**lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, show buffer statistics for a specific T640 router (or line-card chassis) that is connected to the TX Matrix router. On a TX Matrix Plus router, show buffer statistics for a specific router (line-card chassis) that is connected to the TX Matrix Plus router.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

**local**—(EX4200 switches and MX Series routers only) (Optional) Show buffer statistics for the local Virtual Chassis member.

**member member-id**—(EX4200 switches and MX Series routers only) (Optional) Show buffer statistics for the specified member of the Virtual Chassis configuration. For EX4200 switches, replace *member-id* with a value from 0 through 9. For an MX Series Virtual Chassis, replace *member-id* with a value of 0 or 1.

**node-group name**—(QFabric systems only) (Optional) Show buffer statistics for the Node group

**sfc**—(TX Matrix Plus routers only) (Optional) Show buffer statistics for the TX Matrix Plus router. Replace *number* with 0.

**Additional Information**

By default, when you issue the `show system buffers` command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.

A special type of memory buffer called a *cluster* is 2 KB in size. For more information, see *The Design and Implementation of the 4.4BSD Operation System* by McKusic, Bostic, Karels, and Quarterman.

**Required Privilege Level**

`view`
List of Sample Output

- show system buffers on page 1120
- show system buffers scc (TX Matrix Router) on page 1121
- show system buffers sfc (TX Matrix Plus Router) on page 1121
- show system buffers all-chassis (TX Matrix Plus Router) on page 1121
- show system buffers node-group (QFabric System) on page 1122

Output Fields

Table 154 on page 1120 describes the output fields for the show system buffers command. Output fields are listed in the approximate order in which they appear.
Table 154: show system buffers Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mbufs in use</td>
<td>Memory buffers (mbufs) are 128-byte buffers that are used for various purposes inside the kernel. Each memory buffer has a type, and the output itemizes the amount allocated for each type. Types with no memory buffers allocated are not displayed.</td>
</tr>
<tr>
<td>mbufs allocated to packet headers</td>
<td>Number of memory buffers currently holding packet headers</td>
</tr>
<tr>
<td>mbufs allocated to control blocks</td>
<td>Number of memory buffers currently holding the state for sockets.</td>
</tr>
<tr>
<td>mbufs allocated to send data</td>
<td>Number of memory buffers currently holding socket send data.</td>
</tr>
<tr>
<td>mbufs allocated to pfe refill data</td>
<td>Number of memory buffers currently holding Packet Forwarding Engine refill data.</td>
</tr>
<tr>
<td>mbufs allocated to fxp data</td>
<td>Number of memory buffers currently holding fxp data.</td>
</tr>
<tr>
<td>mbufs allocated to socket names and addresses</td>
<td>Number of memory buffers currently holding addresses for sockets.</td>
</tr>
<tr>
<td>mbuf clusters in use</td>
<td>Allocation statistics for memory buffer clusters.</td>
</tr>
<tr>
<td>allocated to network</td>
<td>Total amount of memory in use by the networking and interprocess communication (IPC) code.</td>
</tr>
<tr>
<td>requests for memory denied</td>
<td>Number of times a memory allocation request within the IPC and networking code failed.</td>
</tr>
<tr>
<td>requests for memory delayed</td>
<td>Number of times a memory allocation request within the IPC and networking code was postponed.</td>
</tr>
<tr>
<td>calls to protocol drain routines</td>
<td>Number of times a memory allocation request within the IPC and networking code triggered a memory reclamation attempt.</td>
</tr>
</tbody>
</table>

Sample Output

show system buffers

user@host> show system buffers
397/893/1290 mbufs in use (current/cache/total)
395/331/726/30000 mbuf clusters in use (current/cache/total/max)
384/256 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
889K/885K/1774K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0/5/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines

**show system buffers scc (TX Matrix Router)**

```
user@host> show system buffers scc
213 mbufs in use:
   11 mbufs allocated to packet headers
   26 mbufs allocated to socket names and addresses
   2 mbufs allocated to socket options
   17 mbufs allocated to socket send data
   2 mbufs allocated to pfe data
   155 mbufs allocated to fxp data (rx)
   511 mbufs allocated to <mbuf type 86>
   256 mbufs allocated to <mbuf type 92>
924/1162 mbuf clusters in use
2788 Kbytes allocated to network (75% in use)
0 requests for memory denied
0 requests for memory delayed
0 calls to protocol drain routines
```

**show system buffers sfc (TX Matrix Plus Router)**

```
user@host> show system buffers sfc 0

sfc0-re0:

--------------------------------------------------------------------------
4363/2807/7170 mbufs in use (current/cache/total)
4358/1968/6326/30000 mbuf clusters in use (current/cache/total/max)
256/128 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
9806K/4637K/14444K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0/10/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines
```

**show system buffers all-chassis (TX Matrix Plus Router)**

```
user@host> show system buffers all-chassis

sfc0-re0:

--------------------------------------------------------------------------
4363/2807/7170 mbufs in use (current/cache/total)
4358/1968/6326/30000 mbuf clusters in use (current/cache/total/max)
256/128 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
9806K/4637K/14444K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0/10/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
```
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines

lcc0-re0:

772/2558/3330 mbufs in use (current/cache/total)
772/598/1370/30000 mbuf clusters in use (current/cache/total/max)
768/512 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
1737K/1835K/3572K bytes allocated to network (current/cache/total)
0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0 requests for jumbo clusters denied (4k/9k/16k)
0/4/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines

lcc1-re0:

773/2437/3210 mbufs in use (current/cache/total)
773/453/1226/30000 mbuf clusters in use (current/cache/total/max)
768/384 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
1739K/1515K/3254K bytes allocated to network (current/cache/total)
0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0 requests for jumbo clusters denied (4k/9k/16k)
0/7/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines

lcc2-re0:

816/2514/3330 mbufs in use (current/cache/total)
816/554/1370/30000 mbuf clusters in use (current/cache/total/max)
768/512 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
1836K/1736K/3572K bytes allocated to network (current/cache/total)
0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0 requests for jumbo clusters denied (4k/9k/16k)
0/4/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile

show system buffers node-group (QFabric System)
Chapter 24: Administration

0/0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0/0 16k jumbo clusters in use (current/cache/total/max)
4K/3714K/3719K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0/6/6656 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines

re0:

--------------------------------------------------------------------------
516/639/1155 mbufs in use (current/cache/total)
515/147/662/30000 mbuf clusters in use (current/cache/total/max)
512/128 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
1159K/453K/1612K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0/4/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines

re1:

--------------------------------------------------------------------------
519/771/1290 mbufs in use (current/cache/total)
518/176/694/30000 mbuf clusters in use (current/cache/total/max)
512/128 mbuf+clusters out of packet secondary zone in use (current/cache)
0/0/0 4k (page size) jumbo clusters in use (current/cache/total/max)
0/0/0 9k jumbo clusters in use (current/cache/total/max)
0/0/0 16k jumbo clusters in use (current/cache/total/max)
1165K/544K/1710K bytes allocated to network (current/cache/total)
0/0/0 requests for mbufs denied (mbufs/clusters/mbuf+clusters)
0/0/0 requests for jumbo clusters denied (4k/9k/16k)
0/4/1024 sfbufs in use (current/peak/max)
0 requests for sfbufs denied
0 requests for sfbufs delayed
0 requests for I/O initiated by sendfile
0 calls to protocol drain routines
**show system connections**

**Syntax**

```
show system connections
<extensive>
<all-chassis | all-lcc | lcc number | scc>
<inet | inet6>
<show-routing-instances>
```

**Syntax (EX Series)**

```
show system connections
<extensive>
<all-members>
<inet | inet6>
<local>
<member member-id>
<show-routing-instances>
```

**Syntax (TX Matrix Router)**

```
show system connections
<extensive>
<all-chassis | all-lcc | lcc number | scc>
<inet | inet6>
<show-routing-instances>
```

**Syntax (TX Matrix Plus Router)**

```
show system connections
<extensive>
<all-chassis | all-lcc | lcc number | sfc number>
<inet | inet6>
<show-routing-instances>
```

**Syntax (MX Series Router)**

```
show system connections
<extensive>
<all-members>
<inet | inet6>
<local>
<member member-id>
<show-routing-instances>
```

**Syntax (QFX Series)**

```
show system connections
<extensive>
<inet>
<infrastructure name>
<interconnect-device name>
<node-group name>
<show-routing-instances>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `sfc` option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display information about the active IP sockets on the Routing Engine. Use this command to verify which servers are active on a system and what connections are currently in progress.
Options

none—Display information about all active IP sockets on the Routing Engine.

extensive—(Optional) Display exhaustive system process information, which, for TCP connections, includes the TCP control block. This option is useful for debugging TCP connections.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display system connection activity for all the routers in the chassis.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system connection activity for all T640 routers connected to the TX Matrix router. On a TX Matrix Plus router, display system connection activity for all connected T1600 or T4000 LCCs.

all-members—(EX4200 switches and MX Series routers only) (Optional) Display system connection activity for all members of the Virtual Chassis configuration.

inet | inet6—(Optional) Display IPv4 connections or IPv6 connections, respectively.

infrastructure name—(QFabric systems only) (Optional) Display system connection activity for the fabric control Routing Engines or fabric manager Routing Engines.

interconnect-device name—(QFabric systems only) (Optional) Display system connection activity for the Interconnect device.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display system connection activity for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display system connection activity for a specific router that is connected to the TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Display system connection activity for the local Virtual Chassis member.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Display system connection activity for the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

node-group name—(QFabric systems only) (Optional) Display system connection activity for the Node group.
scc—(TX Matrix routers only) (Optional) Display system connection activity for the
TX Matrix router (or switch-card chassis).

sfc—(TX Matrix routers only) (Optional) Display system connection activity for the
TX Matrix Plus router.

show-routing-instances—(Optional) Display routing instances.

Additional Information
By default, when you issue the show system connections command on the master Routing
Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all
the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise,
if you issue the same command on the backup Routing Engine of a TX Matrix or a TX
Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs
that are connected to it in the routing matrix.

Required Privilege
view

Related Documentation
• Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output
show system connections on page 1127
show system connections extensive on page 1127
show system connections lcc (TX Matrix Router) on page 1128
show system connections show-routing-instances on page 1129
show system connections (TX Matrix Plus Router) on page 1130
show system connections sfc (TX Matrix Plus Router) on page 1133
show system connections show-routing-instances (TX Matrix Plus Router) on page 1135
show system connections (QFX3500 Switch) on page 1140

Output Fields
Table 155 on page 1126 describes the output fields for the show system connections
command. Output fields are listed in the approximate order in which they appear.

Table 155: show system connections Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proto</td>
<td>Protocol of the socket: IP, TCP, or UDP for IPv4 or IPv6.</td>
</tr>
<tr>
<td>Recv-Q</td>
<td>Number of input packets received by the protocol and waiting to be processed by the application.</td>
</tr>
<tr>
<td>Send-Q</td>
<td>Number of output packets sent by the application and waiting to be processed by the protocol.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Local address and port of the socket, separated by a period. An asterisk (*) indicates that the bound address is the wildcard address. Server sockets typically have the wildcard address and a well-known port bound to them.</td>
</tr>
<tr>
<td>Foreign Address</td>
<td>Foreign address and port of the socket, separated by a period. An asterisk (*) indicates that the address or port is a wildcard.</td>
</tr>
</tbody>
</table>
Table 155: show system connections Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Routing Instance</strong></td>
<td>(Displayed only when the <strong>show-routing-instance</strong> option is used.) Routing instances associated with active IP sockets on the Routing Engine.</td>
</tr>
<tr>
<td>(state)</td>
<td>For TCP, the protocol state of the socket.</td>
</tr>
</tbody>
</table>

Sample Output

show system connections

```
user@host> show system connections
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp 0 0 192.168.168.10.23 208.197.169.195.945 ESTABLISHED
```

show system connections extensive

```
user@host> show system connections extensive
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp 0 0 192.168.168.10.23 208.197.169.195.945 ESTABLISHED
```

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRS</td>
<td>236981199</td>
</tr>
<tr>
<td>RCVUP</td>
<td>236981325</td>
</tr>
<tr>
<td>RCVNXT</td>
<td>236981327</td>
</tr>
<tr>
<td>RCVADV</td>
<td>237046862</td>
</tr>
<tr>
<td>Rcvwnd</td>
<td>66640</td>
</tr>
<tr>
<td>RTT</td>
<td>140058623</td>
</tr>
<tr>
<td>SRRT</td>
<td>15519</td>
</tr>
<tr>
<td>RTTv</td>
<td>908</td>
</tr>
<tr>
<td>RXTCUR</td>
<td>1200</td>
</tr>
<tr>
<td>RTXSHIFT</td>
<td>0</td>
</tr>
<tr>
<td>RTSEQ</td>
<td>2566994941</td>
</tr>
<tr>
<td>RTTMIN</td>
<td>1360</td>
</tr>
<tr>
<td>Flags</td>
<td>SACK_PERMIT [0x2000200]</td>
</tr>
<tr>
<td>TCP4</td>
<td>10.255.165.203.65141 ESTABLISHED</td>
</tr>
<tr>
<td>Sndsbcc</td>
<td>0</td>
</tr>
<tr>
<td>Sndsbmbcnt</td>
<td>0</td>
</tr>
<tr>
<td>Sndsbmbmax</td>
<td>131072</td>
</tr>
<tr>
<td>Proc id</td>
<td>0</td>
</tr>
<tr>
<td>Proc name</td>
<td>rpd</td>
</tr>
<tr>
<td>ISS</td>
<td>2555995917</td>
</tr>
<tr>
<td>Sndduna</td>
<td>2555995917</td>
</tr>
<tr>
<td>Snddntx</td>
<td>2555995917</td>
</tr>
<tr>
<td>Snddwnd</td>
<td>16384</td>
</tr>
<tr>
<td>Sndmax</td>
<td>2555995910</td>
</tr>
<tr>
<td>Sndcwnd</td>
<td>1000</td>
</tr>
<tr>
<td>Sndsthresh</td>
<td>1073725440</td>
</tr>
<tr>
<td>IRS</td>
<td>2123825753</td>
</tr>
<tr>
<td>Rcvup</td>
<td>2555995917</td>
</tr>
<tr>
<td>Rcvnxt</td>
<td>2555995917</td>
</tr>
<tr>
<td>Rcvadv</td>
<td>2556012301</td>
</tr>
<tr>
<td>Rcvwnd</td>
<td>16384</td>
</tr>
<tr>
<td>Rtt</td>
<td>0</td>
</tr>
<tr>
<td>SRRT</td>
<td>3309</td>
</tr>
<tr>
<td>RTTMIN</td>
<td>72</td>
</tr>
<tr>
<td>RXTCUR</td>
<td>1200</td>
</tr>
<tr>
<td>RTXSHIFT</td>
<td>0</td>
</tr>
<tr>
<td>RTSEQ</td>
<td>2555995989</td>
</tr>
<tr>
<td>TCP4</td>
<td>10.255.165.93.179 ESTABLISHED</td>
</tr>
<tr>
<td>Sndsbcc</td>
<td>0</td>
</tr>
<tr>
<td>Sndsbmbcnt</td>
<td>0</td>
</tr>
<tr>
<td>Sndsbmbmax</td>
<td>131072</td>
</tr>
<tr>
<td>Proc id</td>
<td>5022</td>
</tr>
<tr>
<td>Proc name</td>
<td>rpd</td>
</tr>
<tr>
<td>ISS</td>
<td>2555995917</td>
</tr>
<tr>
<td>Sndduna</td>
<td>2555995917</td>
</tr>
<tr>
<td>Snddntx</td>
<td>2555995917</td>
</tr>
<tr>
<td>Snddwnd</td>
<td>16384</td>
</tr>
<tr>
<td>Sndmax</td>
<td>2555995910</td>
</tr>
<tr>
<td>Sndcwnd</td>
<td>1000</td>
</tr>
<tr>
<td>Sndsthresh</td>
<td>1073725440</td>
</tr>
<tr>
<td>Rtt</td>
<td>0</td>
</tr>
<tr>
<td>SRRT</td>
<td>3279</td>
</tr>
<tr>
<td>RTTMIN</td>
<td>22</td>
</tr>
<tr>
<td>RXTCUR</td>
<td>1200</td>
</tr>
<tr>
<td>RTXSHIFT</td>
<td>0</td>
</tr>
<tr>
<td>RTSEQ</td>
<td>2123860662</td>
</tr>
<tr>
<td>TCP4</td>
<td>10.255.165.113.52404 ESTABLISHED</td>
</tr>
<tr>
<td>Sndsbcc</td>
<td>0</td>
</tr>
<tr>
<td>Sndsbmbcnt</td>
<td>0</td>
</tr>
<tr>
<td>Sndsbmbmax</td>
<td>131072</td>
</tr>
<tr>
<td>Proc id</td>
<td>110932118</td>
</tr>
<tr>
<td>Proc name</td>
<td>rpd</td>
</tr>
<tr>
<td>ISS</td>
<td>110932118</td>
</tr>
<tr>
<td>Sndduna</td>
<td>110932118</td>
</tr>
<tr>
<td>Snddntx</td>
<td>110932118</td>
</tr>
<tr>
<td>Snddwnd</td>
<td>16384</td>
</tr>
<tr>
<td>Sndmax</td>
<td>110932118</td>
</tr>
<tr>
<td>Sndcwnd</td>
<td>1000</td>
</tr>
<tr>
<td>Sndsthresh</td>
<td>1073725440</td>
</tr>
<tr>
<td>Rtt</td>
<td>0</td>
</tr>
<tr>
<td>SRRT</td>
<td>18</td>
</tr>
<tr>
<td>RTTMIN</td>
<td>18</td>
</tr>
<tr>
<td>RXTCUR</td>
<td>1200</td>
</tr>
<tr>
<td>RTXSHIFT</td>
<td>0</td>
</tr>
<tr>
<td>RTSEQ</td>
<td>110932109</td>
</tr>
</tbody>
</table>

show system connections lcc (TX Matrix Router)

user@host> show system connections lcc 2
### Active Internet connections (including servers)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.66.131.1342</td>
<td>192.168.66.130.23</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.66.131.2059</td>
<td>192.168.66.130.23</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.66.131.4571</td>
<td>192.168.66.130.23</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.66.131.2496</td>
<td>192.168.66.130.23</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.3221</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.23</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.22</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.21</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.79</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6234</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.6333</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

### show system connections show-routing-instances

```
user@host> show system connections show-routing-instances
Active Internet connections (including servers) (including routing-instances)
<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>Routing Instance</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.69.204.23</td>
<td>172.17.28.19.4267</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.69.204.58540</td>
<td>10.209.7.138.23</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.69.204.23</td>
<td>172.17.28.19.1098</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.7.1.57668</td>
<td>192.168.9.1.179</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.7.1.179</td>
<td>192.168.8.1.49209</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>128.0.0.1.6234</td>
<td>128.0.3.17.1024</td>
<td>128.0.0.1.6234</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>128.0.0.4.9000</td>
<td>128.0.0.4.59103</td>
<td>128.0.0.4.9000</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>128.0.0.4.9000</td>
<td>128.0.0.4.59103</td>
<td>128.0.0.4.9000</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.32012</td>
<td><em>.</em></td>
<td>*.32012</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.9000</td>
<td><em>.</em></td>
<td>*.9000</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33007</td>
<td><em>.</em></td>
<td>*.33007</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6154</td>
<td><em>.</em></td>
<td>*.6154</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6153</td>
<td><em>.</em></td>
<td>*.6153</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.7000</td>
<td><em>.</em></td>
<td>*.7000</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6152</td>
<td><em>.</em></td>
<td>*.6152</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6156</td>
<td><em>.</em></td>
<td>*.6156</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33005</td>
<td><em>.</em></td>
<td>*.33005</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33007</td>
<td><em>.</em></td>
<td>*.33007</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>
```

Copyright © 2013, Juniper Networks, Inc.
```
tcp4  0  0  *.31343       *. *
__juniper_private1__ LISTEN

tcp4  0  0  *.31341       *. *
__juniper_private1__ LISTEN

tcp4  0  0  *.32003       *. *
__juniper_private2__ LISTEN

tcp4  0  0  *.666         *. *
__juniper_private1__ LISTEN

tcp4  0  0  *.38          *. *
__juniper_private1__ LISTEN

tcp4  0  0  *.3221        *. *
__juniper_private1__ LISTEN

LISTEN
```

**show system connections (TX Matrix Plus Router)**

```shell
user@host> show system connections
sfc0-re0:
```

---

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>3</td>
<td>192.168.178.11.23</td>
<td>172.17.28.19.3565</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.23</td>
<td>172.17.28.204.62719</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.23</td>
<td>192.168.69.199.51255</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.23</td>
<td>172.24.26.227.42860</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6156</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.32012</td>
<td>162.0.0.5.58935</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.32012</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33007</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.666</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.6161</td>
<td>162.0.0.5.62026</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33005</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.9000</td>
<td>162.0.0.4.51611</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.51611</td>
<td>162.0.0.4.9000</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6151</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6154</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6153</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.31343</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.31341</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.9000</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6152</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

---

**Copyright © 2013, Juniper Networks, Inc.**
Active Internet connections (including servers)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.32003</td>
<td><em>..</em></td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33009</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.3221</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.23</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.22</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.21</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.79</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6234</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>127.0.0.1.123</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>10.255.178.11</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.123</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.62027</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.59363</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.31342</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.161</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.161</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.31340</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.31340</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.49152</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.49152</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.4784</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.49152</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.4784</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.3784</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.6333</td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>ip4</td>
<td>0</td>
<td>0</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>ip4</td>
<td>0</td>
<td>0</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.3221</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.23</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.22</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.21</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.79</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td>*.59924</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.59412</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td>*.161</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.31342</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.6333</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

---

lcc1-re0:

Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address (state) Foreign Address
---
<p>| tcp4 | 0 | 0 | *.6234 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.7000 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.9000 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.3221 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.23  | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.22  | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.514 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.513 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.21  | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.79  | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.514 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.513 | LISTEN | <em>.</em> |
| tcp4 | 0 | 0 | *.33009| LISTEN | <em>.</em> |
| udp46| 0 | 0 | *.514 | LISTEN | <em>.</em> |
| udp4 | 0 | 0 | *.514 | LISTEN | <em>.</em> |
| udp46| 0 | 0 | *.59924| LISTEN | <em>.</em> |</p>
<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6234</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.7000</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.9000</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33009</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.3221</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.23</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.22</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6156</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.9000</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.666</td>
<td><em>.</em></td>
</tr>
</tbody>
</table>

show system connections sfc (TX Matrix Plus Router)

```
user@host> show system connections sfc
sfc0-re0:
```

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.514</td>
<td>132.0.0.4.952</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.514</td>
<td>131.0.0.4.694</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.514</td>
<td>130.0.0.4.860</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.514</td>
<td>129.0.0.4.716</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.996</td>
<td>132.0.0.4.514</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.798</td>
<td>131.0.0.4.514</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.995</td>
<td>130.0.0.4.514</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.895</td>
<td>129.0.0.4.514</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.21</td>
<td>172.168.178.11.21</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.21</td>
<td>172.168.178.5162</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6156</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.9000</td>
<td><em>.</em></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.666</td>
<td><em>.</em></td>
</tr>
</tbody>
</table>
```plaintext
show system connections show-routing-instances (TX Matrix Plus Router)

user@host> show system connections show-routing-instances
sfc0-re0:

Active Internet connections (including servers) (including routing-instances)

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>Routing Instance</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6156</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.9000</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.666</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>2</td>
<td>192.168.178.11.23</td>
<td>172.168.178.11.23</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.23</td>
<td>192.168.178.11.23</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.23</td>
<td>192.168.178.11.23</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.11.23</td>
<td>192.168.178.11.23</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.32012</td>
<td>162.0.0.5.58935</td>
<td><strong>juniper_private1</strong></td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.32012</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33007</td>
<td><em>.</em></td>
<td><strong>juniper_private2</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.6161</td>
<td>162.0.0.5.62026</td>
<td><strong>juniper_private1</strong></td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33005</td>
<td><em>.</em></td>
<td><strong>juniper_private2</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.9000</td>
<td>162.0.0.4.51611</td>
<td><strong>juniper_private1</strong></td>
<td>FIN_WAIT_2</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>162.0.0.4.51611</td>
<td>162.0.0.4.9000</td>
<td><strong>juniper_private1</strong></td>
<td>CLOSE_WAIT</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6151</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6154</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>
```

Copyright © 2013, Juniper Networks, Inc.
 tcp4  0   0   *.6153       __juniper_private1__ LISTEN   *.*
tcp4  0   0   *.31343      __juniper_private1__ LISTEN   *.*
tcp4  0   0   *.31341      __juniper_private1__ LISTEN   *.*
tcp4  0   0   *.6152       __juniper_private1__ LISTEN   *.*
tcp4  0   0   *.32003      __juniper_private1__ LISTEN   *.*
tcp4  0   0   *.33009      __juniper_private2__ LISTEN   *.*
tcp4  0   0   *.3221       default       LISTEN   *.*
tcp4  0   0   *.23          default       LISTEN   *.*
tcp4  0   0   *.22          default       LISTEN   *.*
tcp4  0   0   *.514         default       LISTEN   *.*
tcp4  0   0   *.513         default       LISTEN   *.*
tcp4  0   0   *.21          default       LISTEN   *.*
tcp4  0   0   *.79          default       LISTEN   *.*
tcp4  0   0   *.514         __juniper_private1__ LISTEN   *.*
tcp4  0   0   *.513         __juniper_private1__ LISTEN   *.*
tcp4  0   0   *.6234        __juniper_private1__ LISTEN   *.*
udp4  0   0   127.0.0.1.123 default       LISTEN   *.*
udp4  0   0   10.255.178.11.123 default       LISTEN   *.*
udp4  0   0   *.123         default       LISTEN   *.*
udp46 0   0   *.514         default       LISTEN   *.*
udp4  0   0   *.514         default       LISTEN   *.*
udp46 0   0   *.50895       default       LISTEN   *.*
udp4  0   0   *.50794       default       LISTEN   *.*
udp4  0   0   *.31342      __juniper_private1__ LISTEN   *.*
udp46 0   0   *.161         __juniper_private1__ LISTEN   *.*
udp4  0   0   *.161         default       LISTEN   *.*
udp4  0   0   *.31340      __juniper_private2__ LISTEN   *.*
udp4  0   0   *.31340      __juniper_private2__ LISTEN   *.*
udp46 0   0   *.49152       __juniper_private1__ LISTEN   *.*
udp46 0   0   *.4784        default       LISTEN   *.*
udp46 0   0   *.3784        default       LISTEN   *.*
<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>Routing Instance</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.7000</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>192.168.178.3.23</td>
<td>172.24.26.227.50399</td>
<td>default</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.3221</td>
<td><em>.</em></td>
<td><strong>juniper_private2</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.23</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.22</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.21</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.79</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.59924</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.59412</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td>*.161</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.161</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>
### lcc1-re0:

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>Routing Instance</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.7000</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.6234</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.9000</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.3221</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.23</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.22</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.514</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.513</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.21</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.79</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.514</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.513</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.33009</td>
<td><em>.</em></td>
<td><strong>juniper_private2</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.514</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.514</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.59924</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.59412</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.31342</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.161</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.161</td>
<td><em>.</em></td>
<td>default</td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.6333</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>

### lcc2-re0:

<table>
<thead>
<tr>
<th>Proto</th>
<th>Recv-Q</th>
<th>Send-Q</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>Routing Instance</th>
<th>(state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.7000</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td><em>.</em>.6234</td>
<td><em>.</em></td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN</td>
</tr>
<tr>
<td>Proto</td>
<td>Recv-Q</td>
<td>Send-Q</td>
<td>Local Address</td>
<td>Routing Instance</td>
<td>Foreign Address</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>--------</td>
<td>---------------</td>
<td>------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.7000</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.6234</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.9000</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.33009</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.3221</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.23</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.22</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.21</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.79</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>0</td>
<td>*.513</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.514</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.31342</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.62103</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.59924</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.161</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.161</td>
<td>default</td>
<td>LISTEN e.*</td>
<td></td>
</tr>
<tr>
<td>udp4</td>
<td>0</td>
<td>0</td>
<td>*.6333</td>
<td><strong>juniper_private1</strong></td>
<td>LISTEN e.*</td>
<td></td>
</tr>
</tbody>
</table>
### Active Internet connections (including servers)

**Proto** | **Recv-Q** | **Send-Q** | **Local Address** | **Foreign Address** | **(state)**
---|---|---|---|---|---
tcp4 | 0 | 0 | 10.94.204.110.23 | 172.17.28.19.1308 | ESTABLISHED
tcp4 | 0 | 0 | 128.0.0.1.6234 | 128.0.0.1.615142 | ESTABLISHED
tcp4 | 0 | 0 | 128.0.0.1.65142 | 128.0.0.1.61234 | ESTABLISHED
tcp4 | 0 | 0 | 128.0.0.1.61441 | 128.0.0.1.33003 | ESTABLISHED
tcp4 | 0 | 0 | 128.0.0.1.61441 | 128.0.0.1.33003 | ESTABLISHED
tcp4 | 0 | 0 | 128.0.0.1.59437 | 128.0.0.1.33001 | ESTABLISHED
tcp4 | 0 | 0 | 128.0.0.1.59437 | 128.0.0.1.33001 | ESTABLISHED
<table>
<thead>
<tr>
<th>Name</th>
<th>Flags</th>
<th>Local Address</th>
<th>Remote Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.33023</td>
<td>128.0.0.1.63605</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.63605</td>
<td>128.0.0.1.33023</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.33001</td>
<td>128.0.0.1.63830</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.63830</td>
<td>128.0.0.1.33001</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.667</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.6156</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.7000</td>
<td>128.0.0.1.51580</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.51580</td>
<td>128.0.0.1.7000</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.6234</td>
<td>128.0.0.1.53646</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.33001</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.33003</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.53646</td>
<td>128.0.0.1.6234</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.6.9000</td>
<td>128.0.0.1.6.3454</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>128.0.0.1.6.3454</td>
<td>128.0.0.1.6.9000</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.666</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.7000</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.51627</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.3492</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.33023</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.33013</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.7202</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.6151</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.9000</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.6161</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.6011</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.3221</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.23</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.22</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.513</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td>0</td>
<td>*.21</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>Proto</td>
<td>Flags</td>
<td>Local Address</td>
<td>Remote Address</td>
<td>State</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>---------------</td>
<td>----------------</td>
<td>-------</td>
</tr>
<tr>
<td>tcp4</td>
<td></td>
<td>*.79</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td></td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td></td>
<td>*.513</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td></td>
<td>*.1127</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td></td>
<td>*.1129</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td></td>
<td>*.1128</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>tcp4</td>
<td></td>
<td>*.6234</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.514</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>128.0.0.1.123</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td></td>
<td>*.53344</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.54261</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td></td>
<td>*.161</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.161</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.31342</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.59137</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.49152</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp46</td>
<td></td>
<td>*.4784</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.3784</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.49152</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.4784</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.3784</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>10.255.204.110.123</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.123</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.67</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.6333</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>udp4</td>
<td></td>
<td>*.2293</td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>ip4</td>
<td></td>
<td><em>..</em></td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>ip4</td>
<td></td>
<td><em>..</em></td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
<tr>
<td>ip4</td>
<td></td>
<td><em>..</em></td>
<td><em>.</em></td>
<td>LISTEN</td>
</tr>
</tbody>
</table>
show system core-dumps

Syntax

```
show system core-dumps
    <brief | detail>
    <core-filename>
    <core-file-info>
```

Syntax (EX Series Switches)

```
show system core-dumps
    <all-members>
    <brief | detail>
    <core-filename>
    <core-file-info>
    <local>
    <member member-id>
```

Syntax (TX Matrix Router)

```
show system core-dumps
    <all-chassis | all-lcc | lcc number | scc>
    <brief | detail>
    <core-filename>
    <core-file-info>
```

Syntax (TX Matrix Plus Router)

```
show system core-dumps
    <all-chassis | all-lcc | lcc number | sfc number>
    <brief | detail>
    <core-filename>
    <core-file-info>
```

Syntax (QFX Series)

```
show system core-dumps
    <brief | detail>
    <component (UUID | serial number | all)>
    <core-file-info component (UUID | serial number) core-file-name>
    <display-period (hours | minutes | seconds)>
    <display-order>
    <kernel-crashinfo component (UUID | serial number)>
    <repository (core | log)>
```

Release Information

Command introduced before Junos OS Release 8.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Show core files on all routers or switches running Junos OS. You can use the `show system core-dumps` command to show a list of system core files created when the router or switch has failed. This command can be useful for diagnostic purposes. Each list item includes the file permissions, number of links, owner, group, size, modification date, and path and filename. On a QFabric system, you can view core-dump files on individual QFabric system devices as well as on the entire QFabric system.

You can use the option `core-filename` and its options `core-file-info`, `brief`, and `detail` to display more information about the specified core-dump files.

Options

```
none—Display a list of all existing core-dump files.
```
**all-chassis**—(TX Matrix and TX Matrix Plus routers only) (Optional) On a routing matrix based on a TX Matrix router, display system core files for the TX Matrix router switch-card chassis [SCC] and all the T640 routers [LCCs] connected to the TX Matrix router.

On a routing matrix based on a TX Matrix Plus router, display system core files for the TX Matrix Plus router (switch-fabric chassis [SFC]) and all the T1600 routers [LCCs] connected to the TX Matrix Plus router.

**<all-lcc | lcc number>**—(TX Matrix and TX Matrix Plus routers only) (Optional) On a routing matrix based on the TX Matrix router, display core dump files for all T640 routers (line-card chassis [LCCs]) or a specific T640 router [LCC] connected to the TX Matrix router.

On a routing matrix based on the TX Matrix Plus router, display logging information for all T1600 routers (line-card chassis [LCCs]) or a specific T1600 router (LCC) connected to the TX Matrix Plus router. When using the `lcc number` option, replace `number` with a value from 0 through 3.

**NOTE:** The all-chassis option displays system core files for the SCC or SFC and the LCCs connected to the SCC or SFC in the routing matrix while the all-lcc option only displays system core files for the LCCs in the routing matrix.

**all-members**—(EX4200 switches) (Optional) Display system core files on all members of the Virtual Chassis configuration.

**brief**—(Optional) View details of a binary file.

**component (UUID | serial number | all)**—(QFabric systems only) (Optional) Display a list of core-dump files located on individual QFabric system device or on the entire QFabric system.

**core-file-info**—(Optional) Display the stack trace of a core file.

**core-filename**—(Optional) Name of a specific core file to display.

**detail**—(Optional) View stack trace with details of the binary file.

**display-order (timestamp-sort | alphanumeric-sort)**—(QFabric systems only) (Optional) Display list of debug artifacts generated within the specified period—for example, within the last hour, within the last 20 minutes, or within the last 32 seconds—or according to their filename.

**display-period (hours | minutes | seconds)**—(QFabric systems only) (Optional) Display core-dump files generated within the specified period—for example, within the last hour, within the last 20 minutes, or within the last 32 seconds.

**kernel-crashinfo component (UUID | serial number)**—(QFabric systems only) (Optional) Display kernel crash information from the EEPROM on a QFabric system device.
local—(EX4200 switches only) (Optional) Display system core files on the local Virtual Chassis member.

member member-id—(EX4200 switches only) (Optional) Display system core files on the specified member of the Virtual Chassis configuration. Replace member-id with a value from 0 through 9.

repository (core | log)—(QFabric systems only) (Optional) Specify either the core or log repository in which to view core-dump files.

scc—(TX Matrix routers only) (Optional) Display system core files on the TX Matrix router (or switch-card chassis).

sfc—(TX Matrix Plus routers only) (Optional) Display system core files on the TX Matrix Plus router (or switch-fabric chassis).

Required Privilege view

List of Sample Output

show system core-dumps on page 1147
show system core-dumps on page 1147
show system core-dumps (TX Matrix Plus Router) on page 1147
show system core-dumps (QFX3500 Switch) on page 1149
show system core-dumps (QFabric Systems) on page 1149
show system core-dumps core-file-info component serial number core-file-name (QFabric Systems) on page 1150
show system core-dumps component serial number display-order alphanumeric-sort repository core (QFabric Systems) on page 1150
show system core-dumps display-period (QFabric Systems) on page 1150
show system core-dumps kernel-crashinfo component serial number (QFabric Systems) on page 1152
show system core-dumps repository core (QFabric Systems) on page 1154
show system core-dumps repository log (QFabric Systems) on page 1154

Output Fields

Table 156 on page 1145 describes the output fields for the show system core-dumps command. Output fields are listed in the approximate order in which they appear.

Table 156: show system core-dumps Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permissions</td>
<td>Read/write permissions for the file named.</td>
</tr>
<tr>
<td>Links</td>
<td>Number of links to the file.</td>
</tr>
<tr>
<td>Owner</td>
<td>Name of the file owner.</td>
</tr>
<tr>
<td>Group</td>
<td>Name of the group with file access.</td>
</tr>
<tr>
<td>File size</td>
<td>File size in bytes.</td>
</tr>
<tr>
<td>Modified</td>
<td>Last file modification date and time.</td>
</tr>
</tbody>
</table>
### Table 156: show system core-dumps Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Path/filename</strong></td>
<td>File path where the file resides and the filename.</td>
</tr>
<tr>
<td><strong>Repository scope:</strong></td>
<td>Repository where core-dump files and log files are stored. The core-dump files are located in the <em>core</em> repository, and the log files are located in the <em>log</em> repository. The default <strong>Repository scope</strong> is shared since both the <em>core</em> and <em>log</em> repositories are shared by all of the QFabric system devices.</td>
</tr>
<tr>
<td><strong>Repository head:</strong></td>
<td>Path to the top-level repository location.</td>
</tr>
<tr>
<td><strong>Repository name:</strong></td>
<td>Name of the repository: <em>core</em> or <em>log</em>.</td>
</tr>
<tr>
<td><strong>List of nodes for core repository:</strong></td>
<td>List of core-dump files associated with a particular QFabric system device located in the core repository.</td>
</tr>
<tr>
<td><strong>Node Group</strong></td>
<td>Name of the QFabric system device.</td>
</tr>
<tr>
<td><strong>Node Identifier</strong></td>
<td>UUID or serial number of the QFabric system device.</td>
</tr>
<tr>
<td><strong>Num</strong></td>
<td>Number of core-dump and log files.</td>
</tr>
<tr>
<td><strong>Model</strong></td>
<td>Model number of the QFabric system device.</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td>Usage of the repository in megabytes.</td>
</tr>
<tr>
<td><strong>Total usage of core repository:</strong></td>
<td>Total usage of core-dump files associated with a particular QFabric system device located in the core repository. Usage is specified in megabytes and as a percentage.</td>
</tr>
<tr>
<td><strong>Total usage of log repository:</strong></td>
<td>Total usage of log files associated with a particular QFabric system device located in the log repository. Usage is specified in megabytes and as a percentage.</td>
</tr>
<tr>
<td><strong>List of nodes for core repository:</strong></td>
<td>List of core-dump files associated with a particular QFabric system device located in the core repository.</td>
</tr>
<tr>
<td><strong>List of nodes for log repository:</strong></td>
<td>List of log files associated with a particular QFabric system device located in the log repository.</td>
</tr>
<tr>
<td><strong>Filename</strong></td>
<td>Name of the core-dump file.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>Last core-dump file modification date and time.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>Size of the core-dump file.</td>
</tr>
<tr>
<td><strong>Core filename</strong></td>
<td>Filename of the core-dump file.</td>
</tr>
<tr>
<td><strong>Process name</strong></td>
<td>Name of the process that is generating a core-dump file or log file.</td>
</tr>
</tbody>
</table>
Table 156: show system core-dumps Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Junos OS release.</td>
</tr>
<tr>
<td>Build server</td>
<td>Junos OS build server.</td>
</tr>
<tr>
<td>Build date</td>
<td>Junos OS build date.</td>
</tr>
<tr>
<td>Stack trace</td>
<td>Stack trace of the core-dump file.</td>
</tr>
</tbody>
</table>

Sample Output

show system core-dumps

This example shows the command output if core files exist.

```
user@switcht> show system core-dumps
-rw------- 1 root wheel 268369920 Jun 18 17:59 /var/crash/vmcore.0
-rw-rw----- 1 root field 3371008 Jun 18 17:53 /var/tmp/rpd.core.0
-rw-r--r-- 1 root wheel 27775914 Jun 18 17:59 /var/crash/kernel.0
```

show system core-dumps

This example shows the command output if core files do not exist.

```
user@host> show system core-dumps
/var/crash/*/core*: No such file or directory
/var/tmp/*/core*: No such file or directory
/var/crash/kernel.*: No such file or directory
```

show system core-dumps (TX Matrix Plus Router)

```
user@host> show system core-dumps
sfc0-re0:
--------------------------------------------------------------------------
/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*/core*: No such file or directory

/var/crash/cores:
total 8

/var/tmp/cores:
total 1627592
  -rw-r--r-- 1 root field 535346090 May 15 07:36 rpd.core-tarball.0.090515.0736.tgz
  -rw-r--r-- 1 root field 105632057 May 15 07:37 rpd.core-tarball.1.090515.0737.tgz
  -rw-r--r-- 1 root field 101981681 May 15 07:38 rpd.core-tarball.2.090515.0738.tgz
  -rw-r--r-- 1 root field 85854573 May 15 07:40 rpd.core-tarball.3.090515.0740.tgz
  -rw-r--r-- 1 root field 4157845 May 15 08:18 rpd.core-tarball.4.090515.0818.tgz
lcc0-re0:--------------------------------------------------------------------------
```

Copyright © 2013, Juniper Networks, Inc.
/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory

/var/crash/cores:
total 8

/var/tmp/cores:
total 12

lcc1-re0:

/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory

/var/crash/cores:
total 8

/var/tmp/cores:
total 10024
-rw-r--r--  1 root  field    187594 Apr 22 15:47 chassisd.core-tarball.0.090422.1547.tgz
-rw-r--r--  1 root  field    1894183 Apr 22 19:02 chassisd.core-tarball.0.090422.1902.tgz
-rw-r--r--  1 root  field    1290240 Apr 26 16:01 ksyncd_1558.core.0.090426.1601

lcc2-re0:

/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory

/var/crash/cores:
total 21124008
-rw-r--r--  1 root  field    1022376528 May 2  06:43 core-LCC2-EGFPC7.core.0.090502.0643
-rw-r--r--  1 root  field    1022376528 May 2  08:13 core-LCC2-EGFPC7.core.0.090502.0813
-rw-r--r--  1 root  field    1022376544 May 5  06:15 core-LCC2-EGFPC7.core.0.090505.0615
-rw-r--r--  1 root  field    1022376544 May 6  10:59 core-LCC2-EGFPC7.core.0.090506.1059
-rw-r--r--  1 root  field    1022376528 May 2  06:58 core-LCC2-EGFPC7.core.1.090502.0658
-rw-r--r--  1 root  wheel  754271232 May 5  06:33 core-LCC2-EGFPC7.core.1.090505.0633
-rw-r--r--  1 root  wheel  264897536 May 6  11:12 core-LCC2-EGFPC7.core.1.090506.1112
-rw-r--r--  1 root  wheel  1022376528 May 2  07:22 core-LCC2-EGFPC7.core.2.090502.0722
-rw-r--r--  1 root  wheel  163633152 May 5  06:52 core-LCC2-EGFPC7.core.2.090505.0652
-rw-r--r--  1 root  wheel  171312128 May 6  12:13 core-LCC2-EGFPC7.core.2.090506.1213
-rw-r--r--  1 root  wheel  1022376528 May 2  07:39 core-LCC2-EGFPC7.core.3.090502.0739
-rw-r--r--  1 root  wheel  1022376528 May 2  07:55 core-LCC2-EGFPC7.core.4.090502.0755
-rw-r--r--  1 root  wheel  427277312 May 7  04:47 core-LCC2-STFPC4.core.0.090507.0447
-rw-r--r--  1 root  wheel  419609600 May 7  04:47 core-LCC2-STFPC5.core.0.090507.0447
-rw-r--r--  1 root  wheel  432356352 May 7  04:47
show system core-dumps (QFX3500 Switch)

```
showsystemcore-dumps(QFX3500Switch)
user@switch> show system core-dumps
/var/crash/*core*: No such file or directory
rew-rw---- 1 root field 154514 Jun 4 2012 /var/tmp/pafxpcore.core.0.gz 
rew-rw---- 1 root field 154514 Jun 4 2012 /var/tmp/pafxpcore.core.1.gz 
rew-rw---- 1 root field 154514 Jun 4 2012 /var/tmp/pafxpcore.core.2.gz 
rew-rw---- 1 root field 154514 Jun 4 2012 /var/tmp/pafxpcore.core.3.gz 
rew-rw---- 1 root field 154514 Jun 5 2012 /var/tmp/pafxpcore.core.4.gz 
/var/tmp/pics/*core*: No such file or directory
/var/crash/kernel.*: No such file or directory
/tftpboot/corefiles/*core*: No such file or directory
```

show system core-dumps (QFabric Systems)

```
showsystemcore-dumps(QFabricSystems)
user@switch> show system core-dumps
Repository scope: shared
Repository head: /pbdata/export
List of nodes for core repository: /pbdata/export/rdumps/
Node Group  Node Identifier      Num  Model   Usage
DG-0        BCF72080-E44F-E011-802F-4171BAAC781D  0    qfx3100  0M
FM-0        73747cd8-0710-11e1-b6a4-00e081c5297e  0    fx-jvre  0M
DRE-0       77116f18-0710-11e1-a2a0-00e081c5297e  0    fx-jvre  0M
NW-NG-0     BBAKO394                       0    qfx3500  0M
NW-NG-0     cd78871a-0710-11e1-878e-00e081c5297e  0    fx-jvre  0M
NW-NG-0     d0afdale-0710-11e1-a1d0-00e081c5297e  0    fx-jvre  0M
FC-0        d31ab7a6-0710-11e1-ad1b-00e081c5297e  0    fx-jvre  0M
FC-1        d4d0f254-0710-11e1-90c3-00e081c5297e  0    fx-jvre  0M
IC-WS001    WS001                          0    -        -  
IC-WS001    WS001/YW3803                    0    qfxc08-3008  0M
IC-WS001    WS001/YN5999                    0    qfxc08-3008  0M
node-device1 BBAKO372                      0    qfx3500  0M
node-device1 EE3093                        0    qfx3500  0M
Total usage of core repository:0M of 70000M (0.0%)
List of nodes for log repository: /pbdata/export/rlogs/
Node Group    Node Identifier       Num  Model   Usage
DG-0          BCF72080-E44F-E011-802F-4171BAAC781D  0    qfx3100  0M
FM-0          73747cd8-0710-11e1-b6a4-00e081c5297e  1    fx-jvre  0M
DRE-0         77116f18-0710-11e1-a2a0-00e081c5297e  1    fx-jvre  0M
NW-NG-0       BBAKO394                 1    qfx3500  0M
NW-NG-0       cd78871a-0710-11e1-878e-00e081c5297e  1    fx-jvre  0M
NW-NG-0       d0afdale-0710-11e1-a1d0-00e081c5297e  3    fx-jvre  0M
FC-0          d31ab7a6-0710-11e1-ad1b-00e081c5297e  1    fx-jvre  0M
FC-1          d4d0f254-0710-11e1-90c3-00e081c5297e  1    fx-jvre  0M
IC-WS001      WS001                     0    -        -  
IC-WS001      WS001/YW3803              1    qfxc08-3008  0M
IC-WS001      WS001/YN5999              1    qfxc08-3008  0M
node-device1  BBAKO372                  1    qfx3500  0M
node-device1  EE3093                    1    qfx3500  0M
Total usage of log repository:0M of 70000M (0.0%)
show system core-dumps core-file-info component serial number core-file-name (QFabric Systems)

```
user@switch> show system core-dumps core-file-info component 
  e8ff4b3e-7d92-11e0-be5d-00e081c1fe0e cosd.core.0.1519.05162011131846.gz
Repository scope: shared
Repository head: /pbstorage
Repository name: core
Core filename: /pbstorage/rdumps/e8ff4b3e-7d92-11e0-be5d-00e081c1fe0e/5658.cosd.core.0.1519.05162011131846
Process name: cosd
Release: 11.3I0
Build server: /c/ssengupta/dfx_ha_v1/obj-i386-dcp/dcp/usr.sbin/cosd
Build date: 2011-05-14 01:11:44 UTC
Stack trace:
#0 0x8885d183 in select () from /usr/lib/libc.so.6
#0 0x8885d183 in select () from /usr/lib/libc.so.6
#1 0x887d4a45 in pselect () from /usr/lib/libc.so.6
#2 0x88774719 in pselect () from /usr/lib/libthr.so.2
#3 0x885de5db in __evGetNext () from /usr/lib/libisc.so.2
#4 0x885debf0 in __evMainLoop () from /usr/lib/libisc.so.2
#5 0x081125b2 in cosd_loop ()
#6 0x0812e19a in main ()
```

show system core-dumps component serial number display-order alphanumeric-sort repository core (QFabric Systems)

```
user@switch> show system core-dumps component BBAK8891 display-order alphanumeric-sort repository core
Repository scope: shared
Repository head: /pbdata/export
Repository name: core
List of core dumps for component BBAK8891
Repository location: /pbdata/export/rdumps/BBAK8891
Filename                                   Date                      Size
eswd.core.0.1361.11172011214257.gz         Nov 17 21:43:10 2011      4779553
eswd.core.1.80267.11172011214514.gz        Nov 17 21:45:19 2011      3541648
eswd.core.2.80682.11172011214535.gz        Nov 17 21:45:43 2011      2156683
vccpd.core.0.1195.11182011151131.gz        Nov 18 15:11:35 2011      375617
Number of core dumps in repository:4
```

show system core-dumps display-period (QFabric Systems)

```
user@switch> show system core-dumps display-period 24h
Repository scope: shared
Repository head: /pbdata/export
List of core dumps at repository: /pbdata/export/rdumps
Delta timespec: Last 24h
Component: BBAK8273
Filename                                   Size                      Date
vccpd.core.0.1195.11182011151131.gz        Nov 18 15:11:35 2011      375617
Component: cedb7b0e-0025-11e1-9a5f-00e081c52990
Filename                                   Size                      Date
vccpd.core.0.1195.11182011151131.gz        Nov 18 15:11:35 2011      375794
Component: ee19c4f8-0025-11e1-aef6-00e081c52990
Filename                                   Size                      Date
vccpd.core.0.1195.11182011151131.gz        Nov 18 15:11:31 2011      120951
vccpd.core.0.1461.11182011151131.gz        Nov 18 15:11:31 2011      109420
```
Component: BBAK8281
Filename vccpd.core.0.1196.11182011151131.gz Size 375373 Date Nov 18 15:11:36 2011
Component: BBAK8891
Filename vccpd.core.0.1195.11182011151131.gz Size 375617 Date Nov 18 15:11:35 2011
Component: BBAK8276
Filename vccpd.core.0.1196.11182011151131.gz Size 375350 Date Nov 18 15:11:35 2011
Component: BBAK8868
Filename vccpd.core.0.1196.11182011151131.gz Size 375350 Date Nov 18 15:11:35 2011
Component: BBAK8835
Filename vccpd.core.0.1195.11182011151131.gz Size 375700 Date Nov 18 15:11:35 2011
Component: BBAK8283
Filename vccpd.core.0.1195.11182011151131.gz Size 368298 Date Nov 18 15:11:36 2011
Component: YW3781/YW3781
Filename vccpd.core.0.1220.11182011151131.gz Size 380002 Date Nov 18 15:11:38 2011
Component: 09726be2-0026-11e1-82d9-00e081c52990
Filename vccpd.tarball.0.1461.11182011151131.tgz Size 119965 Date Nov 18 15:11:31 2011
Component: ee19c4f8-0025-11e1-aef6-00e081c52990
Filename vccpd.tarball.0.1461.11182011151131.tgz Size 118385 Date Nov 18 15:11:33 2011
Component: BBAK8273
Filename vccpd.tarball.0.1195.1118201115113138.tgz Size 20415 Date Nov 18 15:11:39 2011
Component: ced87b0e-0025-11e1-9a5f-00e081c52990
Filename vccpd.tarball.0.1461.11182011151131.tgz Size 19651 Date Nov 18 15:11:33 2011
Component: BBAK8281
Filename vccpd.tarball.0.1462.11182011151133.tgz Size 24650 Date Nov 18 15:11:36 2011

List of log dumps at repository: /pbdata/export/rlogs
Delta timespec: Last 24h
show system core-dumps kernel-crashinfo component serial number (QFabric Systems)

user@switch> show system core-dumps kernel-crashinfo component A0001/YA0197
Node: A0001/YA0197

Information about previous kernel crash:

-- Kernel panic data --

Panic string: kdb_sysctl_panic
System uptime: 3 day 20 hr 59 min 40 sec Kernel crash time: 2011-11-15 Wed 15:25:17
Kernel build linkstamp: JUNOS 11.3I #0: 2011-11-10 20:42:27 UTC

-- Stacktrace of panicing context --
Processor 1 (crash monarch):
  savectx+0x0 (c9552800,802a7fbc,c88ad05c) ra 801b93a8 sz 0
  kdm_kcore_save_crashinfo+0x254 (c9552800,0,802a7fbc,c88ad05c) ra 8022a9f8 sz 88
panic+0x1d0 (c9552800,0,4,77fed534) ra 802540c0 sz 56
kdb_sysctl_panic+0x70 (c9552800,0,4,77fed534) ra 80237e58 sz 40 sysctl_root+0x12c (c9552800,0,4,8e8c5cf8) ra 80238e50 sz 48
userland_sysctl+0x164 (c9552800,0,4,e8bc5cf8) ra 80238e50 sz 48
userland_sysctl+0xe (c9552800,0,4,8e8c5cf8) ra 80237e58 sz 40
sysctl_root+0x12c (c9552800,0,4,e8bc5cf8) ra 80237e58 sz 160
__sysctl+0xe (c9552800,0,4,e8bc5cf8) ra 80237e58 sz 160
trap+0xe4 (c9552800,0,4,e8bc5cf8) ra 80237e58 sz 160
MipsUserGenException+0x1a4 (c9552800,0,4,405cd12c) ra 0 sz 0
pid 82340, process: sysctl

Processor 0:
restoreintr+0x14 (1,81bca820,3,0) ra 806cdc3c sz 0
spinlock_exit+0x30 (1,81bca820,3,0) ra 8025d354 sz 24
spinlock_exit+0x30 (1,81bca820,3,0) ra 8025d354 sz 24
sleepq_release+0x64 (1,81bca820,3,0) ra 8025e670 sz 24
sleepq_release+0x64 (1,81bca820,3,0) ra 8025e670 sz 24
softclock+0x434 (1,81bca820,3,0) ra 802067f8 sz 80
softclock+0x434 (1,81bca820,3,0) ra 802067f8 sz 80
ithread_loop+0x244 (1,81bca820,3,0) ra 80200e28 sz 48
MipsNMIException+0x34 (1,81bca820,3,0) ra 0 sz 0
pid 82340, process: sysctl

Processor 1:
cpu_idle+0x20 (80960000,51bcb,2031df,81bca1b8) ra 80204948 sz 24 idle_proc+0x130 (80960000,51bcb,2031df,81bca1b8) ra 80200e28 sz 56 fork_exit+0xc0 (80960000,51bcb,2031df,81bca1b8) ra 80897c28 sz 48
MipsNMIException+0x34 (80960000,51bcb,2031df,81bca1b8) ra 0 sz 0
pid 82340, process: sysctl

Processor 2:
cpu_idle+0x20 (80960000,51bcb,2038df,81bca300) ra 80204948 sz 24 idle_proc+0x130 (80960000,51bcb,2038df,81bca300) ra 80200e28 sz 56 fork_exit+0xc0 (80960000,51bcb,2038df,81bca300) ra 80897c28 sz 48
MipsNMIException+0x34 (80960000,51bcb,2038df,81bca300) ra 0 sz 0
pid 82340, process: sysctl

Processor 3:
cpu_idle+0x20 (80960000,51bcb,2037df,81bca448) ra 80204948 sz 24 idle_proc+0x130 (80960000,51bcb,2037df,81bca448) ra 80200e28 sz 56 fork_exit+0xc0 (80960000,51bcb,2037df,81bca448) ra 80897c28 sz 48
MipsNMIException+0x34 (80960000,51bcb,2037df,81bca448) ra 0 sz 0
pid 82340, process: sysctl

Processor 4:
cpu_idle+0x20 (80960000,51bcb,2036df,81bca950) ra 80204948 sz 24 idle_proc+0x130 (80960000,51bcb,2036df,81bca950) ra 80200e28 sz 56 fork_exit+0xc0 (80960000,51bcb,2036df,81bca950) ra 80897c28 sz 48
MipsNMIException+0x34 (80960000,51bcb,2036df,81bca950) ra 0 sz 0
pid 82340, process: sysctl

Processor 5:
restoreintr+0x14 (1,51bcb,203edf,81bca590) ra 806cdc3c sz 0
spinlock_exit+0x30 (1,51bcb,203edf,81bca590) ra 80200e28 sz 56 fork_exit+0xc0 (1,51bcb,203edf,81bca590) ra 80200e28 sz 56 fork_exit+0xc0
MipsNMIException+0x34 (1,51bcb,203edf,81bca590) ra 0 sz 0
pid 82340, process: sysctl

Processor 6:
cpu_idle+0x20 (80960000,51bcb,205cdf,81bca6d8) ra 80204948 sz 24 idle_proc+0x130 (80960000,51bcb,205cdf,81bca6d8) ra 80200e28 sz 56 fork_exit+0xc0 (80960000,51bcb,205cdf,81bca6d8) ra 80897c28 sz 48
MipsNMIException+0x34 (80960000,51bcb,205cdf,81bca6d8) ra 0 sz 0
pid 82340, process: sysctl

Processor 7:
lockmgr+0x5ac (c97e8484,c8dd9800,0,c8dd9800) ra 8c11c81c sz 48
sal_sem_take+0x130 (c97e8484,c8dd9800,0,c8dd9800) ra 8c11c81c sz 48
_bcm_esw_linksan_thread+0x45c (c97e8484,c8dd9800,0,c8dd9800) ra 8c11c81c sz 48
sal_thread_start+0x74 (c97e8484,c8dd9800,0,c8dd9800) ra 80200e28 sz 32

Copyright © 2013, Juniper Networks, Inc.
fork_exit+0xc0 (c97e8484,c8dd9800,0,c8dd9800) ra 80897c28 sz 48
MipsNMIException+0x34 (c97e8484,c8dd9800,0,c8dd9800) ra 0 sz 0
pid 82340, process: sysctl
-- End of stacktrace --

show system core-dumps repository core (QFabric Systems)

user@switch> show system core-dumps repository core
Repository scope: shared
Repository head: /pbdata/export
Repository name: core
List of nodes for core repository: /pbdata/export/rdumps/

<table>
<thead>
<tr>
<th>Node Group</th>
<th>Node Identifier</th>
<th>Num</th>
<th>Model</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DG-0</td>
<td>BCF72080-E44F-E011-802F-4171BAAC781D</td>
<td>0</td>
<td>qfx3100</td>
<td>OM</td>
</tr>
<tr>
<td>FM-0</td>
<td>73747cd8-0710-11e1-b6a4-00e081c5297e</td>
<td>0</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>DRE-0</td>
<td>77116f18-0710-11e1-a2a0-00e081c5297e</td>
<td>0</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>NW-NG-0</td>
<td>BBAK0394</td>
<td>0</td>
<td>qfx3500</td>
<td>OM</td>
</tr>
<tr>
<td>NW-NG-0</td>
<td>cd78871a-0710-11e1-878e-00e081c5297e</td>
<td>0</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>NW-NG-0</td>
<td>d0afdaele-0710-11e1-a1d0-00e081c5297e</td>
<td>0</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>FC-0</td>
<td>d31ab7a6-0710-11e1-ad1b-00e081c5297e</td>
<td>0</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>FC-1</td>
<td>d4d0f254-0710-11e1-90c3-00e081c5297e</td>
<td>0</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>IC-WS001</td>
<td>WS001</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IC-WS001</td>
<td>WS001/YW3803</td>
<td>0</td>
<td>qfxc08-3008</td>
<td>OM</td>
</tr>
<tr>
<td>IC-WS001</td>
<td>WS001/YN5999</td>
<td>0</td>
<td>qfxc08-3008</td>
<td>OM</td>
</tr>
<tr>
<td>node-device1</td>
<td>BBAK0372</td>
<td>0</td>
<td>qfx3500</td>
<td>OM</td>
</tr>
<tr>
<td>node-device1</td>
<td>EE3093</td>
<td>0</td>
<td>qfx3500</td>
<td>OM</td>
</tr>
</tbody>
</table>

Total usage of core repository: 0M of 70000M (0.0%)

show system core-dumps repository log (QFabric Systems)

user@switch> show system core-dumps repository log
Repository scope: shared
Repository head: /pbdata/export
Repository name: log
List of nodes for log repository: /pbdata/export/rlogs/

<table>
<thead>
<tr>
<th>Node Group</th>
<th>Node Identifier</th>
<th>Num</th>
<th>Model</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DG-0</td>
<td>BCF72080-E44F-E011-802F-4171BAAC781D</td>
<td>0</td>
<td>qfx3100</td>
<td>OM</td>
</tr>
<tr>
<td>FM-0</td>
<td>73747cd8-0710-11e1-b6a4-00e081c5297e</td>
<td>1</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>DRE-0</td>
<td>77116f18-0710-11e1-a2a0-00e081c5297e</td>
<td>1</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>NW-NG-0</td>
<td>BBAK0394</td>
<td>1</td>
<td>qfx3500</td>
<td>OM</td>
</tr>
<tr>
<td>NW-NG-0</td>
<td>cd78871a-0710-11e1-878e-00e081c5297e</td>
<td>1</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>NW-NG-0</td>
<td>d0afdaele-0710-11e1-a1d0-00e081c5297e</td>
<td>3</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>FC-0</td>
<td>d31ab7a6-0710-11e1-ad1b-00e081c5297e</td>
<td>1</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>FC-1</td>
<td>d4d0f254-0710-11e1-90c3-00e081c5297e</td>
<td>1</td>
<td>fx-jvre</td>
<td>OM</td>
</tr>
<tr>
<td>IC-WS001</td>
<td>WS001</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IC-WS001</td>
<td>WS001/YN5999</td>
<td>1</td>
<td>qfxc08-3008</td>
<td>OM</td>
</tr>
<tr>
<td>IC-WS001</td>
<td>WS001/YN3803</td>
<td>1</td>
<td>qfxc08-3008</td>
<td>OM</td>
</tr>
<tr>
<td>node-device1</td>
<td>BBAK0372</td>
<td>1</td>
<td>qfx3500</td>
<td>OM</td>
</tr>
<tr>
<td>node-device1</td>
<td>EE3093</td>
<td>1</td>
<td>qfx3500</td>
<td>OM</td>
</tr>
</tbody>
</table>

Total usage of log repository: 0M of 70000M (0.0%)
**show system directory-usage**

**Syntax**

```plaintext
show system directory-usage
<depth number>
<path>
```

**Syntax (EX Series)**

```plaintext
show system directory-usage
<all-members>
<depth number>
<local>
<member member-id>
<path>
```

**Syntax (TX Matrix Router)**

```plaintext
show system directory-usage
<all-members> all-lcc | lcc number | scc>
<depth number>
<path>
```

**Syntax (TX Matrix Plus Router)**

```plaintext
show system directory-usage
<all-members> all-lcc | lcc number | sfc number>
<depth number>
<path>
```

**Syntax (MX Series Router)**

```plaintext
show system directory-usage
<all-members>
<depth number>
<local>
<member member-id>
<path>
```

**Syntax (QFX Series)**

```plaintext
show system directory-usage
<depth number>
<path>
<infrastructure name>
<interconnect-device name>
<node-group name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
sfc option introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display directory usage information.

**Options**

- **none**—Display all directory usage information.
- **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display directory usage information about all the T640 routers (in a routing matrix based on a TX Matrix router). Display directory usage information about all the T1600 or T4000 routers (in a routing matrix based on a TX Matrix Plus router) in the chassis.
all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display directory information for all T640 routers (or line-card chassis) connected to the TX Matrix router. On a TX Matrix Plus router, display directory information for all connected T1600 or T4000 LCCs.

all-members—(EX4200 switches and MX Series routers only) (Optional) Display directory information for all members of the Virtual Chassis configuration.

depth number—(Optional) Depth of the directory to traverse. This option is useful when you want to limit the output shown for a large file system.

infrastructure name— (QFabric systems only) (Optional) Display directory information for the fabric control Routing Engines and fabric manager Routing Engines.

interconnect-device name— (QFabric systems only) (Optional) Display directory information for the Interconnect device.

node-group name— (QFabric systems only) (Optional) Display directory information for the Node group.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display directory information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display directory information for a specific router that is connected to the TX Matrix Plus router. Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Display directory information for the local Virtual Chassis member.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Display directory information for the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

path—(Optional) Path or root directory to traverse.

scc—(TX Matrix router only) (Optional) Display directory information for the TX Matrix router (or switch-card chassis).

sfc number—(TX Matrix Plus routers only) (Optional) Display directory information for the TX Matrix Plus router. Replace number with 0.
Required Privilege Level

view

Related Documentation

- Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output

- `show system directory-usage scc (TX Matrix Router)` on page 1158
- `show system directory-usage sfc (TX Matrix Plus Router)` on page 1158
- `show system directory-usage (QFX3500 Switch)` on page 1158

Output Fields

Table 157 on page 1157 describes the output fields for the `show system directory-usage` command. Output fields are listed in the approximate order in which they appear.

**Table 157: show system directory-usage Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bytes</code></td>
<td>Number of bytes used by files in a directory.</td>
</tr>
<tr>
<td><code>directory-name</code></td>
<td>Name of the directory.</td>
</tr>
</tbody>
</table>
Sample Output

show system directory-usage scc (TX Matrix Router)

```shell
user@host> show system directory-usage /var/tmp scc
/var/tmp
1.0K /var/tmp/vi.recover
2.0K /var/tmp/instmp.tPMk8u
1.0K /var/tmp/install
/var/tmp/instmp.GUMpur
4.8M /var/tmp/instmp.GUMpur/packages
6.4M /var/tmp/troy1
297M /var/tmp/dsw
/var/tmp/pkg_tmp.2073
83K /var/tmp/pkg_tmp.2073/bin
/var/tmp/instmp.oMIDbl
89K /var/tmp/instmp.oMIDbl/bin
/var/tmp/instmp.byhMjR
4.6M /var/tmp/instmp.byhMjR/packages
1.7M /var/tmp/instmp.6fqHf3/packages
4.6M /var/tmp/instmp.mljEJe/packages
```

show system directory-usage sfc (TX Matrix Plus Router)

```shell
user@switch> show system directory-usage /var/tmp sfc 0
sfc0-re0:
/var/tmp
46K /var/tmp/gres-tp
/var/tmp/sec-download
2.0K /var/tmp/sec-download/sub-download
2.0K /var/tmp/vi.recover
2.0K /var/tmp/install
795M /var/tmp/cores
766K /var/tmp/pr440594
```

show system directory-usage (QFX3500 Switch)

```shell
user@switch> show system directory-usage
/var/tmp
30K /var/tmp/gres-tp
2.0K /var/tmp/rtadb
2.0K /var/tmp/vi.recover
2.0K /var/tmp/install
2.0K /var/tmp/pics
```
### show system processes

**Syntax**

```
show system processes
<brief | detail | extensive | summary>
<health (pid process-identifier | process-name process-name)>
<providers>
<resource-limits (brief | detail) process-name>
<wide>
```

**Syntax (EX Series Switches)**

```
show system processes
<all-members>
<brief | detail | extensive | summary>
<health (pid process-identifier | process-name process-name)>
<local>
<member member-id>
<providers>
<resource-limits (brief | detail) process-name>
<wide>
```

**Syntax (MX Series Routers)**

```
show system processes
<all-members>
<brief | detail | extensive | summary>
<health (pid process-identifier | process-name process-name)>
<local>
<member member-id>
<providers>
<resource-limits (brief | detail) process-name>
<wide>
```

**Syntax (QFX Series)**

```
show system processes
<brief | detail | extensive | summary>
<health (pid process-identifier | process-name process-name)>
<interconnect-device name>
<node-group name>
<providers>
<resource-limits>
<wide>
```

**Syntax (TX Matrix Routers)**

```
show system processes
<brief | detail | extensive | summary>
<all-chassis | all-lcc | lcc number | scc>
<wide>
```

**Syntax (TX Matrix Plus Router)**

```
show system processes
<brief | detail | extensive | summary>
<all-chassis | all-lcc | lcc number | sfc number>
<wide>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6.
- Command introduced in Junos OS Release 11.1 for the QFX Series.
**Description**
Display information about software processes that are running on the router or switch and that have controlling terminals.

**Options**
- **none**—Display standard information about system processes.
- **brief | detail | extensive | summary**—(Optional) Display the specified level of detail.
- **adaptive-services**—(Optional) Display the configuration management process that manages the configuration for stateful firewall, Network Address Translation (NAT), intrusion detection services (IDS), and IP Security (IPsec) services on the Adaptive Services PIC.
- **alarm-control**—(Optional) Display the process to configure the system alarm.
- **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Display standard system process information about all the T640 routers (in a routing matrix based on the TX Matrix router) or all the T1600 or T4000 routers (in a routing matrix based on the TX Matrix Plus router) in the chassis.
- **all-lcc**—(TX Matrix routers and TX Matrix Plus router only) (Optional) Display standard system process information for all T640 routers (or line-card chassis) connected to the TX Matrix router. Display standard system process information for all connected T1600 or T4000 LCCs.
- **all-members**—(EX4200 switches and MX Series routers only) (Optional) Display standard system process information for all members of the Virtual Chassis configuration.
- **ancpd-service**—Display the Access Node Control Protocol (ANCP) process, which works with a special Internet Group Management Protocol (IGMP) session to collect outgoing interface mapping events in a scalable manner.
- **application-identification**—Display the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.
- **audit-process**—(Optional) Display the RADIUS accounting process.
- **auto-configuration**—Display the Interface Auto-Configuration process.
- **bootp**—Display the process that enables a router, switch, or interface to act as a Dynamic Host Configuration Protocol (DHCP) or bootstrap protocol (BOOTP) relay agent. DHCP relaying is disabled.
- **captive-portal-content-delivery**—Display the HTTP redirect service by specifying the location to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber.
- **ce-l2tp-service**—(Optional) (M10, M10i, M7i, and MX Series routers only) Display the Universal Edge Layer 2 Tunneling Protocol (L2TP) process, which establishes L2TP tunnels and Point-to-Point Protocol (PPP) sessions through L2TP tunnels.
cfm—Display Ethernet Operations, Administration, and Maintenance (OAM) connectivity fault management (CFM) process, which can be used to monitor the physical link between two switches.

class-of-service—(Optional) Display the class-of-service (CoS) process, which controls the router’s or switch’s CoS configuration.

clicksyncd-service—Display the external clock synchronization process, which uses synchronous Ethernet (SyncE).

craft-control—Display the process for the I/O of the craft interface.

database-replication—(EX Series switches and MX Series routers only) (Optional) Display the database replication process.

datapath-trace-service—Display the packet path tracing process.

dhcp-service—(EX Series switches and MX Series routers only) (Optional) Display the Dynamic Host Configuration Protocol process, which enables a DHCP server to allocate network IP addresses and deliver configuration settings to client hosts without user intervention.

diameter-service—(Optional) Display the diameter process.

disk-monitoring—(Optional) Display the disk monitoring process, which checks the health of the hard disk drive on the Routing Engine.

dynamic-flow-capture—(Optional) Display the dynamic flow capture (DFC) process, which controls DFC configurations on Monitoring Services III PICs.

ecc-error-logging—(Optional) Display the error checking and correction (ECC) process, which logs ECC parity errors in memory on the Routing Engine.

ethernet-connectivity-fault-management—Display the process that provides IEEE 802.1ag OAM connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.

ethernet-link-fault-management—(EX Series switches and MX Series routers only) (Optional) Display the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.

event-processing—(Optional) Display the event process (eventd).

firewall—(Optional) Display the firewall management process, which manages the firewall configuration and enables accepting or rejecting packets that are transiting an interface on a router or switch.

general-authentication-service—(EX Series switches and MX Series routers only) (Optional) Display the general authentication process.
health (pid process-identifier | process-name process-name)—(Optional) Display process health information, either by process id (PID) or by process name.

iccp-service—Display the Inter-Chassis Communication Protocol (ICCP) process.

idp-policy—Display the intrusion detection and prevention (IDP) protocol process.

ilmi—Display the Integrated Local Management Interface (ILMI) protocol process, which provides bidirectional exchange of management information between two ATM interfaces across a physical connection.

inet-process—Display the IP multicast family process.

init—Display the process that initializes the USB modem.

interface-control—(Optional) Display the interface process, which controls the router's or switch's physical interface devices and logical interfaces.

kernel-replication—(Optional) Display the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.

l2-learning—(Optional) Display the Layer 2 address flooding and learning process.

l2cpd-service—Display the Layer 2 Control Protocol process, which enables features such as Layer 2 protocol tunneling and nonstop bridging.

lACP—(Optional) Display the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link to allow their link aggregation control instances to reach agreement on the identity of the LAG to which the link belongs, and then to move the link to that LAG, and to enable the transmission and reception processes for the link to function in an orderly manner.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router, display standard system process information for a specific T640 router that is connected to the TX Matrix router. On a TX Matrix Plus router, display standard system process information for a specific router that is connected to the TX Matrix Plus router.

Replace number with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when TI600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when TI600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
local—(EX4200 switches and MX Series routers only) (Optional) Display standard system process information for the local Virtual Chassis member.

local-policy-decision-function—Display the process for the Local Policy Decision Function, which regulates collection of statistics related to applications and application groups and tracking of information about dynamic subscribers and static interfaces.

logical-system-mux—Display the logical router multiplexer process (lrmuxd), which manages the multiple instances of the routing protocols process (rpd) on a machine running logical routers.

mac-validation—Display the MAC validation process, which configures MAC address validation for subscriber interfaces created on demux interfaces in dynamic profiles on MX Series routers.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Display standard system process information for the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

mib-process—(Optional) Display the MIB II process, which provides the router’s MIB II agent.

mobile-ip—(Optional) Display the Mobile IP process, which configures Junos OS Mobile IP features.

mountd-service—(EX Series switches and MX Series routers only) (Optional) Display the service for NFS mounts requests.

mpls-traceroute—(Optional) Display the MPLS Periodic Traceroute process.

mspd—(Optional) Display the Multiservice process.

multicast-snooping—(EX Series switches and MX Series routers only) (Optional) Display the multicast snooping process, which makes Layer 2 devices such as VLAN switches aware of Layer 3 information, such as the media access control (MAC) addresses of members of a multicast group.

named-service—(Optional) Display the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.

neighbor-liveness—Display the process, which specifies the maximum length of time that the router waits for its neighbor to re-establish an LDP session.

nfsd-service—(Optional) Display the Remote NFS Server process, which provides remote file access for applications that need NFS-based transport.

ntp—Display the Network Time Protocol (NTP) process, which provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse network.

packet-triggered-subscribers—Display the packet-triggered subscribers and policy control (PTSP) process, which allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device.
**peer-selection-service**—(Optional) Display the Peer Selection Service process.

**periodic-packet-services**—Display the Periodic packet management process, which is responsible for processing a variety of time-sensitive periodic tasks so that other processes can more optimally direct their resources.

**pfe**—Display the Packet Forwarding Engine management process.

**pgcp-service**—(Optional) Display the pgcpd service process running on the Routing Engine.

**pgm**—Display the Pragmatic General Multicast (PGM) protocol process, which enables a reliable transport layer for multicast applications.

**pic-services-logging**—(Optional) Display the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.

**ppp**—(Optional) Display the Point-to-Point Protocol (PPP) process, which is the encapsulation protocol process for transporting IP traffic across point-to-point links.

**ppp-service**—Display the Universal edge PPP process, which is the encapsulation protocol process for transporting IP traffic across universal edge routers.

**pppoe**—(Optional) Display the Point-to-Point Protocol over Ethernet (PPPoE) process, which combines PPP that typically runs over broadband connections with the Ethernet link-layer protocol that allows users to connect to a network of hosts over a bridge or access concentrator.

**process-monitor**—Display the process health monitor process (pmond).

**providers**—(Optional) Display provider processes.

**redundancy-interface-process**—(Optional) Display the ASP redundancy process.

**remote-operations**—(Optional) Display the remote operations process, which provides the ping and traceroute MIBs.

**resource-cleanup**—Display the resource cleanup process.

**resource-limits (brief | detail) process-name**—(Optional) Display process resource limits.

**routing**—(Optional) Display the routing protocol process.

**sampling**—(Optional) Display the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.

**sbc-configuration-process**—Display the session border controller (SBC) process of the border signaling gateway (BSG).

**scc**—(TX Matrix routers only) (Optional) Display standard system process information for the TX Matrix router (or switch-card chassis).
**sdk-service**—Display the SDK Service process, which runs on the Routing Engine and is responsible for communications between the SDK application and Junos OS. Although the SDK Service process is present on the router, it is turned off by default.

**secure-neighbor-discovery**—(EX Series switches and MX Series routers only) (Optional) Display the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.

**send**—(Optional) Display the Secure Neighbor Discovery Protocol (SEND) process, which provides support for protecting Neighbor Discovery Protocol (NDP) messages.

**service-deployment**—(Optional) Display the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.

**sfc number**—(TX Matrix Plus routers only) (Optional) Display system process information for the TX Matrix Plus router. Replace *number* with 0.

**snmp**—Display the SNMP process, which enables the monitoring of network devices from a central location and provides the router's or switch's SNMP master agent.

**sonet-aps**—Display the SONET Automatic Protection Switching (APS) process, which monitors any SONET interface that participates in APS.

**static-subscribers**—(Optional) Display the Static subscribers process, which associates subscribers with statically configured interfaces and provides dynamic service activation and activation for these subscribers.

**tunnel-oamd**—(Optional) Display the Tunnel OAM process, which enables the Operations, Administration, and Maintenance of Layer 2 tunneled networks. Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain.

**vrrp**—(EX Series switches and MX Series routers only) (Optional) Display the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.

**watchdog**—Display the watchdog timer process, which enables the watchdog timer when Junos OS encounters a problem.

**wide**—(Optional) Display process information that might be wider than 80 columns.

### Additional Information

By default, when you issue the `show system processes` command on the master Routing Engine of a TX Matrix router or a TX Matrix Plus router, the command is broadcast to all the master Routing Engines of the LCCs connected to it in the routing matrix. Likewise, if you issue the same command on the backup Routing Engine of a TX Matrix or a TX Matrix Plus router, the command is broadcast to all backup Routing Engines of the LCCs that are connected to it in the routing matrix.
Required Privilege
Level

Related Documentation
- List of Junos OS Processes
- Routing Matrix with a TX Matrix Plus Router Solutions Page

List of Sample Output
- show system processes on page 1168
- show system processes brief on page 1168
- show system processes detail on page 1169
- show system processes extensive on page 1169
- show system processes lcc wide (TX Matrix Routing Matrix) on page 1170
- show system processes summary on page 1170
- show system processes (TX Matrix Plus Router) on page 1171
- show system processes sfc (TX Matrix Plus Router) on page 1178
- show system processes lcc wide (TX Matrix Plus Routing Matrix) on page 1181
- show system processes (QFX Series) on page 1182

Output Fields
Table 158 on page 1166 describes the output fields for the show system processes command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>last pid</td>
<td>Last process identifier assigned to the process.</td>
<td>brief extensive summary</td>
</tr>
<tr>
<td>load averages</td>
<td>Three load averages followed by the current time.</td>
<td>brief extensive summary</td>
</tr>
<tr>
<td>processes</td>
<td>Number of existing processes and the number of processes in each state (sleeping, running, starting, zombies, and stopped).</td>
<td>brief extensive summary</td>
</tr>
<tr>
<td>Mem</td>
<td>Information about physical and virtual memory allocation.</td>
<td>brief extensive summary</td>
</tr>
<tr>
<td>Swap</td>
<td>Information about physical and virtual memory allocation.</td>
<td>brief extensive summary</td>
</tr>
<tr>
<td>PID</td>
<td>Process identifier.</td>
<td>detail extensive summary</td>
</tr>
<tr>
<td>TT</td>
<td>Control terminal name.</td>
<td>none detail</td>
</tr>
</tbody>
</table>
Table 158: show system processes Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAT</td>
<td>Symbolic process state. The state is given by a sequence of letters. The first letter indicates the run state of the process:</td>
<td>none detail</td>
</tr>
<tr>
<td></td>
<td>• D—in disk or other short-term, uninterruptible wait</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• I—Idle (sleeping longer than about 20 seconds)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• R—Runnable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• S—Sleeping for less than 20 seconds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• T—Stopped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Z—Dead (zombie)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• +—The process is in the foreground process group of its control terminal.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &lt;—The process has raised CPU scheduling priority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• &gt;—The process has specified a soft limit on memory requirements and is currently exceeding that limit; such a process is not swapped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A—The process requested random page replacement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• E—The process is trying to exit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L—The process has pages locked in core.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• N—The process has reduced CPU scheduling priority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• S—The process requested first-in, first-out (FIFO) page replacement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• s—The process is a session leader.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• V—The process is temporarily suspended.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• W—The process is swapped out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• X—The process is being traced or debugged.</td>
<td></td>
</tr>
<tr>
<td>UID</td>
<td>User identifier.</td>
<td>detail</td>
</tr>
<tr>
<td>USERNAME</td>
<td>Process owner.</td>
<td>extensive summary</td>
</tr>
<tr>
<td>PPID</td>
<td>Parent process identifier.</td>
<td>detail</td>
</tr>
<tr>
<td>CPU</td>
<td>(D)—Short-term CPU usage.</td>
<td>detail extensive summary</td>
</tr>
<tr>
<td></td>
<td>(E and S)—Raw (unweighted) CPU usage. The value of this field is used to sort the processes in the output.</td>
<td></td>
</tr>
<tr>
<td>RSS</td>
<td>Resident set size.</td>
<td>detail</td>
</tr>
<tr>
<td>WCHAN</td>
<td>Symbolic name of the wait channel.</td>
<td>detail</td>
</tr>
<tr>
<td>STARTED</td>
<td>Local time when the process started running.</td>
<td>detail</td>
</tr>
<tr>
<td>PRI</td>
<td>Current priority of the process. A lower number indicates a higher priority.</td>
<td>detail extensive summary</td>
</tr>
<tr>
<td>NI or NICE</td>
<td>UNIX &quot;niceness&quot; value. A lower number indicates a higher priority.</td>
<td>detail extensive summary</td>
</tr>
<tr>
<td>SIZE</td>
<td>Total size of the process (text, data, and stack), in kilobytes.</td>
<td>extensive summary</td>
</tr>
</tbody>
</table>
Table 158: show system processes Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>RES</td>
<td>Current amount of resident memory, in kilobytes.</td>
<td>extensive summary</td>
</tr>
<tr>
<td>STATE</td>
<td>Current state of the process (for example, sleep, wait, run, idle, zombie, or stop).</td>
<td>extensive summary</td>
</tr>
<tr>
<td>TIME</td>
<td>(S)—Number of system and user CPU seconds that the process has used. (None, D, and E)—Total amount of time that the command has been running.</td>
<td>detail extensive summary</td>
</tr>
<tr>
<td>WCPU</td>
<td>Weighted CPU usage.</td>
<td>extensive summary</td>
</tr>
<tr>
<td>COMMAND</td>
<td>Command that is currently running.</td>
<td>detail extensive summary</td>
</tr>
<tr>
<td>THR</td>
<td>Number of threads in the process</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

show system processes

```
user@host>  show system processes
PID  TT  STAT      TIME COMMAND
 0  ??  DLs    0:00.70  (swapper)
 1  ??  Is     0:00.35 /sbin/init --
 2  ??  DL     0:00.00  (pagedaemon)
 3  ??  DL     0:00.00  (vmdaemon)
 4  ??  DL     0:42.37  (update)
 5  ??  DL     0:00.00  (if_jnx)
 80 ??  Ss     0:14.66 syslogd -s
 96 ??  Is     0:00.01 portmap
128 ??  Is     0:02.70 cron
173 ??  Is     0:02.24 /usr/local/sbin/sshd (sshd1)
189 ??  S      0:03.80 /sbin/watchdog -t180
190 ??  I      0:00.03 /usr/sbin/tnetd -N
191 ??  S      2:24.76 /sbin/ifd -N
192 ??  Sc     0:55.44 /usr/sbin/xntpd -N
195 ??  S      0:53.11 /usr/sbin/snmpd -N
196 ??  S      1:15.73 /usr/sbin/mib2d -N
198 ??  I      0:00.75 /usr/sbin/inetd -N
2677 ??  I      0:00.01 /usr/sbin/mdm -N
2712 ??  Ss     0:00.24 rlogind
2735 ??  R      0:00.00 /bin/ps -ax
1985 p0-  S      0:07.41 ./rp -N
2713 p0  Is     0:00.24 -tcsh (tcsh)
2726 p0  S+     0:00.07 cli
```

show system processes brief

```
user@host>  show system processes brief
last pid: 543; load averages: 0.00, 0.00, 0.00  18:29:47
37 processes: 1 running, 36 sleeping
```
show system processes detail

user@host> show system processes detail

<table>
<thead>
<tr>
<th>PID</th>
<th>UID</th>
<th>PPID</th>
<th>CPU</th>
<th>PRI</th>
<th>NI</th>
<th>RSS</th>
<th>WCHAN</th>
<th>STARTED</th>
<th>TT</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>3151</td>
<td>1049</td>
<td>3129</td>
<td>2</td>
<td>28</td>
<td>0</td>
<td>672</td>
<td>-</td>
<td>1:13PM</td>
<td>p0</td>
<td>R+</td>
<td>0:00.00</td>
<td>ps -ax -r</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>12</td>
<td>psleep</td>
<td>1:51PM</td>
<td>DL</td>
<td></td>
<td>0:00.00</td>
<td>(pagedae)</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>28</td>
<td>0</td>
<td>12</td>
<td>psleep</td>
<td>1:51PM</td>
<td>DL</td>
<td></td>
<td>0:07.15</td>
<td>(vmdaemo)</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>12</td>
<td>pfi</td>
<td>1:51PM</td>
<td>IL</td>
<td></td>
<td>0:02.90</td>
<td>(if_pfe)</td>
</tr>
<tr>
<td>27</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>17936</td>
<td>mfsidl</td>
<td>1:51PM</td>
<td>Is</td>
<td></td>
<td>0:00.46</td>
<td>mfs /dev/</td>
</tr>
<tr>
<td>81</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>496</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:00.29</td>
<td>/sbin/ini</td>
</tr>
<tr>
<td>119</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>492</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:00.00</td>
<td>portmap</td>
</tr>
<tr>
<td>134</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>580</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:02.95</td>
<td>amd -p -a</td>
</tr>
<tr>
<td>151</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>532</td>
<td>pause</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:00.34</td>
<td>cron</td>
</tr>
<tr>
<td>183</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>420</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:00.07</td>
<td>/usr/loca</td>
</tr>
<tr>
<td>206</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>72</td>
<td>pause</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:00.51</td>
<td>/sbin/wat</td>
</tr>
<tr>
<td>207</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>520</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>I</td>
<td>0:00.16</td>
<td>/usr/sbin</td>
</tr>
<tr>
<td>208</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>536</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:08.21</td>
<td>/sbin/dcd</td>
</tr>
<tr>
<td>210</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>740</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:05.83</td>
<td>/usr/sbin</td>
</tr>
<tr>
<td>211</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>376</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>S</td>
<td>0:00.03</td>
<td>/usr/sbin</td>
</tr>
<tr>
<td>215</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>548</td>
<td>select</td>
<td>1:52PM</td>
<td>??</td>
<td>I</td>
<td>0:00.50</td>
<td>/usr/sbin</td>
</tr>
<tr>
<td>219</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>540</td>
<td>ttyin</td>
<td>1:52PM</td>
<td>v0</td>
<td>Is+</td>
<td>0:00.02</td>
<td>/usr/lib</td>
</tr>
<tr>
<td>220</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>540</td>
<td>ttyin</td>
<td>1:52PM</td>
<td>v1</td>
<td>Is+</td>
<td>0:00.01</td>
<td>/usr/lib</td>
</tr>
<tr>
<td>221</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>540</td>
<td>ttyin</td>
<td>1:52PM</td>
<td>v2</td>
<td>Is+</td>
<td>0:00.01</td>
<td>/usr/lib</td>
</tr>
<tr>
<td>222</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>540</td>
<td>ttyin</td>
<td>1:52PM</td>
<td>v3</td>
<td>Is+</td>
<td>0:00.01</td>
<td>/usr/lib</td>
</tr>
<tr>
<td>735</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>468</td>
<td>select</td>
<td>2:47PM</td>
<td>??</td>
<td>S</td>
<td>0:19.14</td>
<td>/sbin/lib</td>
</tr>
<tr>
<td>736</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>212</td>
<td>select</td>
<td>2:47PM</td>
<td>??</td>
<td>S</td>
<td>0:14.13</td>
<td>/sbin/lib</td>
</tr>
<tr>
<td>1380</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>888</td>
<td>ttyin</td>
<td>7:32PM</td>
<td>d0</td>
<td>Is+</td>
<td>0:06.46</td>
<td>bash</td>
</tr>
<tr>
<td>3019</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>636</td>
<td>select</td>
<td>10:49AM</td>
<td>??</td>
<td>S</td>
<td>0:02.93</td>
<td>tnp.chass</td>
</tr>
<tr>
<td>3122</td>
<td>0</td>
<td>2</td>
<td>1380</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>1764</td>
<td>select</td>
<td>12:33PM</td>
<td>d0</td>
<td>S</td>
<td>0:00.77</td>
</tr>
<tr>
<td>3128</td>
<td>0</td>
<td>2</td>
<td>215</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>580</td>
<td>select</td>
<td>12:45PM</td>
<td>??</td>
<td>S</td>
<td>0:00.12</td>
</tr>
<tr>
<td>3129</td>
<td>1049</td>
<td>3128</td>
<td>1</td>
<td>18</td>
<td>0</td>
<td>944</td>
<td>pause</td>
<td>12:45PM</td>
<td>p0</td>
<td>S</td>
<td>0:00.14</td>
<td>-tcsh (tc</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-18</td>
<td>0</td>
<td>0</td>
<td>sched</td>
<td>1:51PM</td>
<td>??</td>
<td>DLs</td>
<td>0:00.10</td>
<td>(swapper</td>
</tr>
</tbody>
</table>

show system processes extensive

user@host> show system processes extensive

Mem: 241M Active, 99M Inact, 78M Wired, 325M Cache, 69M Buf, 1251M Free
Swap: 2048M Total, 2048M Free

<table>
<thead>
<tr>
<th>PID</th>
<th>USERNAME</th>
<th>THR</th>
<th>PRI</th>
<th>NICE</th>
<th>SIZE</th>
<th>RES</th>
<th>STATE</th>
<th>TIME</th>
<th>WCPU</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>root</td>
<td>1</td>
<td>171</td>
<td>52</td>
<td>0K</td>
<td>12K</td>
<td>RUN</td>
<td>807.5h</td>
<td>98.73%</td>
<td>idle</td>
</tr>
<tr>
<td>13</td>
<td>root</td>
<td>1</td>
<td>-20</td>
<td>-139</td>
<td>0K</td>
<td>12K</td>
<td>WAIT</td>
<td>36:17</td>
<td>0.00%</td>
<td>clock sio</td>
</tr>
<tr>
<td>1499</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>7212K</td>
<td>3040K</td>
<td>select</td>
<td>34:01</td>
<td>0.00%</td>
<td>license-check</td>
</tr>
<tr>
<td>1621</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>20968K</td>
<td>11216K</td>
<td>select</td>
<td>20:25</td>
<td>0.00%</td>
<td>mib2d</td>
</tr>
<tr>
<td>1465</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>115M</td>
<td>7464K</td>
<td>select</td>
<td>14:32</td>
<td>0.00%</td>
<td>chassisd</td>
</tr>
<tr>
<td>1478</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>6336K</td>
<td>3816K</td>
<td>select</td>
<td>11:28</td>
<td>0.00%</td>
<td>ppmd</td>
</tr>
<tr>
<td>1618</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>39584K</td>
<td>7464K</td>
<td>select</td>
<td>8:47</td>
<td>0.00%</td>
<td>pfed</td>
</tr>
<tr>
<td>1622</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>15268K</td>
<td>10988K</td>
<td>select</td>
<td>6:16</td>
<td>0.00%</td>
<td>smmpd</td>
</tr>
<tr>
<td>1466</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>7408K</td>
<td>2896K</td>
<td>select</td>
<td>5:44</td>
<td>0.00%</td>
<td>alarmd</td>
</tr>
<tr>
<td>7</td>
<td>root</td>
<td>1</td>
<td>-16</td>
<td>0</td>
<td>12K</td>
<td>12K</td>
<td>client</td>
<td>5:09</td>
<td>0.00%</td>
<td>ifstate notify</td>
</tr>
<tr>
<td>1480</td>
<td>root</td>
<td>1</td>
<td>96</td>
<td>0</td>
<td>5388K</td>
<td>2660K</td>
<td>select</td>
<td>4:29</td>
<td>0.00%</td>
<td>ksysvc</td>
</tr>
<tr>
<td>12</td>
<td>root</td>
<td>1</td>
<td>-40</td>
<td>-159</td>
<td>0</td>
<td>12K</td>
<td>WAIT</td>
<td>4:15</td>
<td>0.00%</td>
<td>swi2: netisr 0</td>
</tr>
</tbody>
</table>
show system processes lcc wide (TX Matrix Routing Matrix)

user@host> show system processes lcc 2 wide
lcc2-re0:

<table>
<thead>
<tr>
<th>PID</th>
<th>TT</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>??</td>
<td>DLs</td>
<td>0:00.00</td>
<td>(swapper)</td>
</tr>
<tr>
<td>1</td>
<td>??</td>
<td>ILS</td>
<td>0:00.10</td>
<td>/sbin/preinit -- (init)</td>
</tr>
<tr>
<td>2</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>(pagedaemon)</td>
</tr>
<tr>
<td>3</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>(vmdaemon)</td>
</tr>
<tr>
<td>4</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>(bufdaemon)</td>
</tr>
<tr>
<td>5</td>
<td>??</td>
<td>DL</td>
<td>0:00.04</td>
<td>(syncer)</td>
</tr>
<tr>
<td>6</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>(netdaemon)</td>
</tr>
<tr>
<td>7</td>
<td>??</td>
<td>IL</td>
<td>0:00.00</td>
<td>(if_pic_listen)</td>
</tr>
<tr>
<td>8</td>
<td>??</td>
<td>IL</td>
<td>0:00.00</td>
<td>(scs_housekeeping)</td>
</tr>
<tr>
<td>9</td>
<td>??</td>
<td>IL</td>
<td>0:00.00</td>
<td>(if_pfe_listen)</td>
</tr>
<tr>
<td>10</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>(vmuncachedaemon)</td>
</tr>
<tr>
<td>11</td>
<td>??</td>
<td>SL</td>
<td>0:00.02</td>
<td>(cb_poll)</td>
</tr>
<tr>
<td>172</td>
<td>??</td>
<td>ILS</td>
<td>0:00.21</td>
<td>mfs -o noauto /dev/ad1s1b /tmp (newfs)</td>
</tr>
<tr>
<td>2909</td>
<td>??</td>
<td>Is</td>
<td>0:00.00</td>
<td>pccardd</td>
</tr>
<tr>
<td>2932</td>
<td>??</td>
<td>Ss</td>
<td>0:00.07</td>
<td>syslogd -r -s</td>
</tr>
<tr>
<td>3039</td>
<td>??</td>
<td>Is</td>
<td>0:00.00</td>
<td>cron</td>
</tr>
<tr>
<td>3217</td>
<td>??</td>
<td>I</td>
<td>0:00.00</td>
<td>/sbin/watchdog -d</td>
</tr>
<tr>
<td>3218</td>
<td>??</td>
<td>I</td>
<td>0:00.02</td>
<td>/usr/sbin/tnetd -N</td>
</tr>
<tr>
<td>3221</td>
<td>??</td>
<td>S</td>
<td>0:00.11</td>
<td>/usr/sbin/alarmd -N</td>
</tr>
<tr>
<td>3222</td>
<td>??</td>
<td>S</td>
<td>0:00.85</td>
<td>/usr/sbin/craftd -N</td>
</tr>
<tr>
<td>3223</td>
<td>??</td>
<td>S</td>
<td>0:00.05</td>
<td>/usr/sbin/mgd -N</td>
</tr>
<tr>
<td>3224</td>
<td>??</td>
<td>I</td>
<td>0:00.02</td>
<td>/usr/sbin/inetd -N</td>
</tr>
<tr>
<td>3225</td>
<td>??</td>
<td>I</td>
<td>0:00.00</td>
<td>/usr/sbin/tnp.sntpd -N</td>
</tr>
<tr>
<td>3226</td>
<td>??</td>
<td>I</td>
<td>0:00.01</td>
<td>/usr/sbin/tnp.sntpc -N</td>
</tr>
<tr>
<td>3228</td>
<td>??</td>
<td>I</td>
<td>0:00.01</td>
<td>/usr/sbin/smartd -N</td>
</tr>
<tr>
<td>3231</td>
<td>??</td>
<td>I</td>
<td>0:00.01</td>
<td>/usr/sbin/ecd -N</td>
</tr>
<tr>
<td>3425</td>
<td>??</td>
<td>S</td>
<td>0:00.09</td>
<td>/usr/sbin/dfwd -N</td>
</tr>
<tr>
<td>3426</td>
<td>??</td>
<td>S</td>
<td>0:00.19</td>
<td>/sbin/dcd -N</td>
</tr>
<tr>
<td>3427</td>
<td>??</td>
<td>I</td>
<td>0:00.04</td>
<td>/usr/sbin/pfed -N</td>
</tr>
<tr>
<td>3430</td>
<td>??</td>
<td>S</td>
<td>0:00.10</td>
<td>/usr/sbin/ksyncd -N</td>
</tr>
<tr>
<td>3482</td>
<td>??</td>
<td>S</td>
<td>1:53.63</td>
<td>/usr/sbin/chassisd -N</td>
</tr>
<tr>
<td>4285</td>
<td>??</td>
<td>SL</td>
<td>0:00.01</td>
<td>(peer proxy)</td>
</tr>
<tr>
<td>4286</td>
<td>??</td>
<td>SL</td>
<td>0:00.00</td>
<td>(peer proxy)</td>
</tr>
<tr>
<td>4303</td>
<td>??</td>
<td>Ss</td>
<td>0:00.00</td>
<td>mgd: (mgd) (root) (mgd)</td>
</tr>
<tr>
<td>4304</td>
<td>??</td>
<td>R</td>
<td>0:00.00</td>
<td>/bin/ps -ax -ww</td>
</tr>
<tr>
<td>3270</td>
<td>d0</td>
<td>Is+</td>
<td>0:00.00</td>
<td>/usr/libexec/getty_std.9600 ttyd0</td>
</tr>
</tbody>
</table>

show system processes summary

user@host> show system processes summary

last pid: 543; load averages: 0.00, 0.00, 0.00 18:29:47
37 processes: 1 running, 36 sleeping
show system processes (TX Matrix Plus Router)

user@host> show system processes

sfc0-re0:

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>PID</th>
<th>TT</th>
<th>STAT</th>
<th>TIME COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>??</td>
<td>WLs</td>
<td>0:00.00 [swapper]</td>
</tr>
<tr>
<td>1</td>
<td>??</td>
<td>IIs</td>
<td>0:01.16 /packages/mnt/jbase/sbin/init --</td>
</tr>
<tr>
<td>2</td>
<td>??</td>
<td>DL</td>
<td>0:00.01 [g_event]</td>
</tr>
<tr>
<td>3</td>
<td>??</td>
<td>DL</td>
<td>0:00.11 [g_up]</td>
</tr>
<tr>
<td>4</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [thread taskfq]</td>
</tr>
<tr>
<td>5</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [kqueue taskfq]</td>
</tr>
<tr>
<td>6</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [pagedaemon]</td>
</tr>
<tr>
<td>7</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [vmdaemon]</td>
</tr>
<tr>
<td>8</td>
<td>??</td>
<td>DL</td>
<td>0:01.77 [pagezero]</td>
</tr>
<tr>
<td>9</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [ktrace]</td>
</tr>
<tr>
<td>10</td>
<td>??</td>
<td>DL</td>
<td>17:22:31 [idle]</td>
</tr>
<tr>
<td>11</td>
<td>??</td>
<td>WL</td>
<td>0:00.32 [swi2: net]</td>
</tr>
<tr>
<td>12</td>
<td>??</td>
<td>WL</td>
<td>0:01.21 [swi7: clock sio]</td>
</tr>
<tr>
<td>13</td>
<td>??</td>
<td>WL</td>
<td>0:00.00 [swi6: vm]</td>
</tr>
<tr>
<td>14</td>
<td>??</td>
<td>DL</td>
<td>0:00.10 [yarrow]</td>
</tr>
<tr>
<td>15</td>
<td>??</td>
<td>WL</td>
<td>0:00.00 [swi9: +]</td>
</tr>
<tr>
<td>16</td>
<td>??</td>
<td>WL</td>
<td>0:00.00 [swi8: +]</td>
</tr>
<tr>
<td>17</td>
<td>??</td>
<td>WL</td>
<td>0:00.00 [swi5: cambio]</td>
</tr>
<tr>
<td>18</td>
<td>??</td>
<td>WL</td>
<td>0:00.00 [swi9: task queue]</td>
</tr>
<tr>
<td>19</td>
<td>??</td>
<td>WL</td>
<td>0:02.73 [irq10: bcm0 uhci1+*]</td>
</tr>
<tr>
<td>20</td>
<td>??</td>
<td>WL</td>
<td>0:00.02 [irq11: cb0 uhci0+*]</td>
</tr>
<tr>
<td>21</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [usb0]</td>
</tr>
<tr>
<td>22</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [usbtask]</td>
</tr>
<tr>
<td>23</td>
<td>??</td>
<td>DL</td>
<td>0:00.00 [usb1]</td>
</tr>
<tr>
<td>24</td>
<td>??</td>
<td>DL</td>
<td>0:00.05 [usb2]</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>PID</th>
<th>TT</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>??</td>
<td>WLs</td>
<td>0:00.00</td>
<td>[swapper]</td>
</tr>
<tr>
<td>1</td>
<td>??</td>
<td>IIs</td>
<td>0:00.17</td>
<td>/packages/mnt/jbase/sbin/init --</td>
</tr>
<tr>
<td>2</td>
<td>??</td>
<td>DL</td>
<td>0:00.01</td>
<td>[g_event]</td>
</tr>
<tr>
<td>3</td>
<td>??</td>
<td>DL</td>
<td>0:00.16</td>
<td>[g_up]</td>
</tr>
<tr>
<td>4</td>
<td>??</td>
<td>DL</td>
<td>0:00.11</td>
<td>[g_down]</td>
</tr>
<tr>
<td>5</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[thread taskq]</td>
</tr>
<tr>
<td>6</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[kqueue taskq]</td>
</tr>
<tr>
<td>7</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[pagedaemon]</td>
</tr>
<tr>
<td>8</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[vmdaemon]</td>
</tr>
<tr>
<td>9</td>
<td>??</td>
<td>DL</td>
<td>0:01.77</td>
<td>[pagezero]</td>
</tr>
<tr>
<td>10</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[ktrace]</td>
</tr>
<tr>
<td>11</td>
<td>??</td>
<td>RL</td>
<td>17:22.83</td>
<td>[idle]</td>
</tr>
<tr>
<td>12</td>
<td>??</td>
<td>WL</td>
<td>0:00.35</td>
<td>[swi2: net]</td>
</tr>
<tr>
<td>13</td>
<td>??</td>
<td>WL</td>
<td>0:01.20</td>
<td>[swi7: clock sio]</td>
</tr>
<tr>
<td>14</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi6: vm]</td>
</tr>
<tr>
<td>15</td>
<td>??</td>
<td>DL</td>
<td>0:00.10</td>
<td>[yarrow]</td>
</tr>
<tr>
<td>16</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi9: +]</td>
</tr>
<tr>
<td>17</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi8: +]</td>
</tr>
<tr>
<td>18</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi5: cambio]</td>
</tr>
<tr>
<td>19</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi9: task queue]</td>
</tr>
<tr>
<td>20</td>
<td>??</td>
<td>WL</td>
<td>0:02.87</td>
<td>[irq10: bcm0 uhci1*]</td>
</tr>
<tr>
<td>21</td>
<td>??</td>
<td>WL</td>
<td>0:00.02</td>
<td>[irq11: cb0 uhci0+*]</td>
</tr>
<tr>
<td>22</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[usb0]</td>
</tr>
<tr>
<td>23</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[usbtask]</td>
</tr>
<tr>
<td>24</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[usb1]</td>
</tr>
<tr>
<td>25</td>
<td>??</td>
<td>DL</td>
<td>0:00.05</td>
<td>[usb2]</td>
</tr>
<tr>
<td>26</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[usb3]</td>
</tr>
<tr>
<td>27</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[usb4]</td>
</tr>
<tr>
<td>28</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[usb5]</td>
</tr>
<tr>
<td>29</td>
<td>??</td>
<td>DL</td>
<td>0:00.04</td>
<td>[usb6]</td>
</tr>
<tr>
<td>30</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[usb7]</td>
</tr>
<tr>
<td>31</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[irq14: ata0]</td>
</tr>
<tr>
<td>32</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[irq15: atal]</td>
</tr>
<tr>
<td>33</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[irq1: atkbd0]</td>
</tr>
<tr>
<td>34</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi0: sio]</td>
</tr>
<tr>
<td>35</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi3: ip6opt ipopt]</td>
</tr>
<tr>
<td>36</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi4: ip6mismatch+]</td>
</tr>
<tr>
<td>37</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi1: ipfw]</td>
</tr>
<tr>
<td>38</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[bufdaemon]</td>
</tr>
<tr>
<td>39</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[vn1ru]</td>
</tr>
<tr>
<td>40</td>
<td>??</td>
<td>DL</td>
<td>0:00.01</td>
<td>[syncer]</td>
</tr>
<tr>
<td>41</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[softdepflush]</td>
</tr>
<tr>
<td>42</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[netdaemon]</td>
</tr>
<tr>
<td>43</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[vmuncachedaemon]</td>
</tr>
<tr>
<td>44</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[if_pic_listen]</td>
</tr>
<tr>
<td>45</td>
<td>??</td>
<td>DL</td>
<td>0:00.02</td>
<td>[vmkmemdaemon]</td>
</tr>
<tr>
<td>PID</td>
<td>TT</td>
<td>STAT</td>
<td>TIME</td>
<td>COMMAND</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>0</td>
<td>??</td>
<td>WLs</td>
<td>0:00.00</td>
<td>[swapper]</td>
</tr>
<tr>
<td>1</td>
<td>??</td>
<td>ILS</td>
<td>0:00.18</td>
<td>/packages/mnt/jbase/sbin/init --</td>
</tr>
<tr>
<td>2</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[g_event]</td>
</tr>
<tr>
<td>3</td>
<td>??</td>
<td>DL</td>
<td>0:00.17</td>
<td>[g_up]</td>
</tr>
<tr>
<td>4</td>
<td>??</td>
<td>DL</td>
<td>0:00.12</td>
<td>[g_down]</td>
</tr>
</tbody>
</table>
Chapter 24: Administration

5 ?? DL 0:00.00 [thread taskq]
6 ?? DL 0:00.00 [kqueue taskq]
7 ?? DL 0:00.00 [pagedaemon]
8 ?? DL 0:00.00 [vmdaemon]
9 ?? DL 0:01.77 [pagezero]
10 ?? DL 0:00.00 [ktrace]
11 ?? RL 17:19.13 [idle]
12 ?? WL 0:00.36 [swi2: net]
13 ?? WL 0:01.20 [swi7: clock sio]
14 ?? WL 0:00.00 [swi6: vm]
15 ?? DL 0:00.13 [yarrow]
16 ?? WL 0:00.00 [swi9: +]
17 ?? WL 0:00.00 [swi8: +]
18 ?? WL 0:00.00 [swi5: cambio]
19 ?? WL 0:00.00 [swi9: task queue]
20 ?? WL 0:03.03 [irq10: bcm0 uhci1*]
21 ?? WL 0:00.02 [irq11: cb0 uhci0+*]
22 ?? DL 0:00.00 [usb0]
23 ?? DL 0:00.00 [usbtask]
24 ?? DL 0:00.00 [usb1]
25 ?? DL 0:00.05 [usb2]
26 ?? DL 0:00.00 [usb3]
27 ?? DL 0:00.00 [usb4]
28 ?? DL 0:00.00 [usb5]
29 ?? DL 0:00.04 [usb6]
30 ?? DL 0:00.00 [usb7]
31 ?? WL 0:00.00 [irq14: ata0]
32 ?? WL 0:00.00 [irq15: ata1]
33 ?? WL 0:00.00 [irq1: atkbd0]
34 ?? WL 0:00.00 [swi0: sio]
35 ?? WL 0:00.00 [swi3: ip6opt ipopt]
36 ?? WL 0:00.00 [swi4: ip6mismatch+]
37 ?? WL 0:00.00 [swi1: ipfwd]
38 ?? DL 0:00.00 [bufdaemon]
39 ?? DL 0:00.00 [vn1ru]
40 ?? DL 0:00.01 [syncer]
41 ?? DL 0:00.00 [softdepflush]
42 ?? DL 0:00.00 [netdaemon]
43 ?? DL 0:00.00 [vmuncachedaemon]
44 ?? DL 0:00.00 [if_pie_listen]
45 ?? DL 0:00.02 [vmkmemdaemon]
46 ?? DL 0:00.01 [cb_poll]
47 ?? DL 0:00.00 [if_pfe_listen]
48 ?? DL 0:00.00 [scs_housekeeping]
49 ?? IL 0:00.00 [kern_dump_proc]
50 ?? IL 0:00.00 [nfsiod 0]
51 ?? IL 0:00.00 [nfsiod 1]
52 ?? IL 0:00.00 [nfsiod 2]
53 ?? IL 0:00.00 [nfsiod 3]
54 ?? DL 0:00.02 [schedcpu]
55 ?? DL 0:00.75 [md0]
77 ?? DL 0:03.48 [md1]
98 ?? DL 0:00.59 [md2]
116 ?? DL 0:00.02 [md3]
137 ?? DL 0:00.56 [md4]
158 ?? DL 0:00.15 [md5]
179 ?? DL 0:00.00 [md6]
215 ?? DL 0:00.03 [md7]
225 ?? DL 0:00.03 [md8]
1052 ?? DL 0:00.00 [jsr_kkcm]
1337 ?? SL 0:00.09 [bcmTX]
show system processes sfc (TX Matrix Plus Router)

user@host> show system processes sfc0
sfc0-re0:

<table>
<thead>
<tr>
<th>PID</th>
<th>TT</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>??</td>
<td>WLs</td>
<td>0:00.00</td>
<td>[swapper]</td>
</tr>
<tr>
<td>1</td>
<td>??</td>
<td>SLs</td>
<td>0:01.18</td>
<td>[packages/mnt/jbase/sbin/init --]</td>
</tr>
<tr>
<td>2</td>
<td>??</td>
<td>DL</td>
<td>0:00.20</td>
<td>[g_event]</td>
</tr>
<tr>
<td>3</td>
<td>??</td>
<td>DL</td>
<td>0:00.39</td>
<td>[g_up]</td>
</tr>
<tr>
<td>4</td>
<td>??</td>
<td>DL</td>
<td>0:00.32</td>
<td>[g_down]</td>
</tr>
<tr>
<td>5</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[thread taskq]</td>
</tr>
<tr>
<td>6</td>
<td>??</td>
<td>DL</td>
<td>0:00.09</td>
<td>[kqueue taskq]</td>
</tr>
<tr>
<td>7</td>
<td>??</td>
<td>DL</td>
<td>0:00.01</td>
<td>[pagedaemon]</td>
</tr>
<tr>
<td>8</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[vmdaemon]</td>
</tr>
<tr>
<td>9</td>
<td>??</td>
<td>DL</td>
<td>0:00.63</td>
<td>[pagezero]</td>
</tr>
<tr>
<td>10</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[ktrace]</td>
</tr>
<tr>
<td>11</td>
<td>??</td>
<td>RL</td>
<td>0:12.09</td>
<td>[idle]</td>
</tr>
<tr>
<td>12</td>
<td>??</td>
<td>WL</td>
<td>0:11.07</td>
<td>[swi2: net]</td>
</tr>
<tr>
<td>13</td>
<td>??</td>
<td>WL</td>
<td>0:27.70</td>
<td>[swi7: clock sio]</td>
</tr>
<tr>
<td>14</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi6: vm]</td>
</tr>
<tr>
<td>15</td>
<td>??</td>
<td>DL</td>
<td>0:03.03</td>
<td>[yarrow]</td>
</tr>
<tr>
<td>16</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi9: +]</td>
</tr>
<tr>
<td>17</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi8: +]</td>
</tr>
<tr>
<td>18</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td>[swi5: cambio]</td>
</tr>
</tbody>
</table>
| 19  | ??  | WL   | 0:00.00| [swi9: task queue]
Chapter 24: Administration

20 ?? WL 0:11.46 [irq16: uhci0 uhci*]
21 ?? DL 0:00.00 [usb0]
22 ?? DL 0:00.00 [usbtask]
23 ?? WL 0:39.63 [irq17: uhci1 uhci*]
24 ?? DL 0:00.00 [usb1]
25 ?? WL 0:00.00 [irq18: uhci2 uhci*]
26 ?? DL 0:00.84 [usb2]
27 ?? DL 0:00.00 [usb3]
28 ?? DL 0:00.00 [usb4]
29 ?? DL 0:00.00 [usb5]
30 ?? DL 0:00.73 [usb6]
31 ?? DL 0:00.00 [usb7]
32 ?? WL 0:00.00 [irq14: ata0]
33 ?? WL 0:00.00 [irq15: atal]
34 ?? WL 0:00.00 [irq1: atkbd0]
35 ?? WL 0:00.00 [swi0: sio]
36 ?? WL 0:00.00 [irq11: isab0]
37 ?? WL 0:00.00 [swi3: ip6opt ipopt]
38 ?? WL 0:00.00 [swi4: ip6mismatch+]
39 ?? WL 0:00.00 [swi1: ipfwd]
40 ?? DL 0:00.02 [bufdaemon]
41 ?? DL 0:00.02 [vnlru]
42 ?? DL 0:00.39 [syncer]
43 ?? DL 0:00.05 [softdepflush]
44 ?? DL 0:00.00 [netdaemon]
45 ?? DL 0:00.02 [vmuncachedaemon]
46 ?? DL 0:00.00 [if_pic_listen]
47 ?? DL 0:00.35 [vmkmendaemon]
48 ?? DL 0:00.00 [cb_poll]
49 ?? DL 0:00.06 [if_pfe_listen]
50 ?? DL 0:00.00 [scs_housekeeping]
51 ?? IL 0:00.00 [kern_dump_proc]
52 ?? IL 0:00.00 [nfsiod 0]
53 ?? IL 0:00.00 [nfsiod 1]
54 ?? IL 0:00.00 [nfsiod 2]
55 ?? IL 0:00.00 [nfsiod 3]
56 ?? DL 0:00.37 [schedcpu]
57 ?? DL 0:00.56 [md0]
58 ?? DL 0:02.58 [md1]
59 ?? DL 0:00.03 [md2]
60 ?? DL 0:00.01 [md3]
61 ?? DL 0:00.95 [md4]
62 ?? DL 0:00.12 [md5]
63 ?? DL 0:00.00 [md6]
64 ?? DL 0:00.02 [md7]
65 ?? DL 0:00.05 [md8]
66 ?? SL 0:01.35 [bcmTCP]
67 ?? SL 0:01.69 [bcmXG3AsyncTX]
68 ?? SL 0:41.57 [bcmLINK.0]
69 ?? SL 0:33.97 [bcmLINK.1]
70 ?? Is 0:00.01 /usr/sbin/cron
71 ?? S 0:00.01 /sbin/watchdog -t -I
72 ?? S 0:00.86 /usr/libexec/bslockd -mp -N
73 ?? I 0:00.01 /usr/sbin/tnetd -N
74 ?? S 0:01.32 /usr/sbin/alarmd -N
75 ?? S 0:14.54 /usr/sbin/craftd -N
76 ?? S 0:01.20 /usr/sbin/mdg -N
77 ?? S 0:00.05 /usr/sbin/inetd -N
78 ?? S 0:00.10 /usr/sbin/tmp.sntpd -N
79 ?? S 0:00.11 /usr/sbin/smactd -N
80 ?? S 0:01.11 /usr/sbin/idpd -N
<table>
<thead>
<tr>
<th>PID</th>
<th>UID</th>
<th>State</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1526</td>
<td>??</td>
<td>S</td>
<td>0:01.43</td>
<td>/usr/sbin/license-check -U -M -p 10 -i 10</td>
</tr>
<tr>
<td>1527</td>
<td>??</td>
<td>I</td>
<td>0:00.01</td>
<td>/usr/libexec/getty Pc ttyv0</td>
</tr>
<tr>
<td>1616</td>
<td>??</td>
<td>DL</td>
<td>0:00.30</td>
<td>[peer proxy]</td>
</tr>
<tr>
<td>1617</td>
<td>??</td>
<td>DL</td>
<td>0:00.32</td>
<td>[peer proxy]</td>
</tr>
<tr>
<td>1618</td>
<td>??</td>
<td>DL</td>
<td>0:00.34</td>
<td>[peer proxy]</td>
</tr>
<tr>
<td>1619</td>
<td>??</td>
<td>DL</td>
<td>0:00.30</td>
<td>[peer proxy]</td>
</tr>
<tr>
<td>2391</td>
<td>??</td>
<td>Is</td>
<td>0:00.01</td>
<td>telnetd</td>
</tr>
<tr>
<td>7331</td>
<td>??</td>
<td>Ss</td>
<td>0:00.03</td>
<td>telnetd</td>
</tr>
<tr>
<td>9538</td>
<td>??</td>
<td>DL</td>
<td>0:01.16</td>
<td>[jsr_kkcm]</td>
</tr>
<tr>
<td>9613</td>
<td>??</td>
<td>DL</td>
<td>0:00.18</td>
<td>[peer proxy]</td>
</tr>
<tr>
<td>23781</td>
<td>??</td>
<td>Ss</td>
<td>0:00.01</td>
<td>telnetd</td>
</tr>
<tr>
<td>23926</td>
<td>??</td>
<td>Ss</td>
<td>0:00.03</td>
<td>mgd: (mgd) (regress)/dev/ttyp2 (mgd)</td>
</tr>
<tr>
<td>36867</td>
<td>??</td>
<td>S</td>
<td>0:03.14</td>
<td>/usr/sbin/rpd -N</td>
</tr>
<tr>
<td>36874</td>
<td>??</td>
<td>S</td>
<td>0:00.08</td>
<td>/usr/sbin/lmpd</td>
</tr>
<tr>
<td>36876</td>
<td>??</td>
<td>S</td>
<td>0:00.17</td>
<td>/usr/sbin/lacpd -N</td>
</tr>
<tr>
<td>36877</td>
<td>??</td>
<td>S</td>
<td>0:00.15</td>
<td>/usr/sbin/bfdd -N</td>
</tr>
<tr>
<td>36878</td>
<td>??</td>
<td>S</td>
<td>0:05.05</td>
<td>/usr/sbin/ppmd -N</td>
</tr>
<tr>
<td>36907</td>
<td>??</td>
<td>S</td>
<td>0:26.63</td>
<td>/usr/sbin/chassisd -N</td>
</tr>
<tr>
<td>37775</td>
<td>??</td>
<td>S</td>
<td>0:00.01</td>
<td>/usr/sbin/bdbrepd -N</td>
</tr>
<tr>
<td>45727</td>
<td>??</td>
<td>S</td>
<td>0:00.02</td>
<td>/usr/sbin/xntpd -j -N -g (ntpd)</td>
</tr>
<tr>
<td>45729</td>
<td>??</td>
<td>S</td>
<td>0:00.40</td>
<td>/usr/sbin/l2ald -N</td>
</tr>
<tr>
<td>45730</td>
<td>??</td>
<td>S&lt;</td>
<td>0:00.13</td>
<td>/usr/sbin/apsd -N</td>
</tr>
<tr>
<td>45731</td>
<td>??</td>
<td>SN</td>
<td>0:00.10</td>
<td>/usr/sbin/sampled -N</td>
</tr>
<tr>
<td>45732</td>
<td>??</td>
<td>S</td>
<td>0:00.09</td>
<td>/usr/sbin/rmopd -N</td>
</tr>
<tr>
<td>45734</td>
<td>??</td>
<td>S</td>
<td>0:00.31</td>
<td>/usr/sbin/cosd</td>
</tr>
<tr>
<td>45735</td>
<td>??</td>
<td>I</td>
<td>0:00.00</td>
<td>/usr/sbin/rtspd -N</td>
</tr>
<tr>
<td>45736</td>
<td>??</td>
<td>S</td>
<td>0:00.06</td>
<td>/usr/sbin/fsad -N</td>
</tr>
<tr>
<td>45737</td>
<td>??</td>
<td>S</td>
<td>0:00.05</td>
<td>/usr/sbin/rrdd -N</td>
</tr>
<tr>
<td>45738</td>
<td>??</td>
<td>S</td>
<td>0:00.10</td>
<td>/usr/sbin/pppd -N</td>
</tr>
<tr>
<td>45739</td>
<td>??</td>
<td>S</td>
<td>0:00.05</td>
<td>/usr/sbin/dfccd -N</td>
</tr>
<tr>
<td>45740</td>
<td>??</td>
<td>S</td>
<td>0:00.08</td>
<td>/usr/sbin/lfmd -N</td>
</tr>
<tr>
<td>45741</td>
<td>??</td>
<td>S</td>
<td>0:00.01</td>
<td>/usr/sbin/mplsoamd -N</td>
</tr>
<tr>
<td>45742</td>
<td>??</td>
<td>S</td>
<td>0:00.01</td>
<td>/usr/sbin/sendd -N</td>
</tr>
<tr>
<td>45743</td>
<td>??</td>
<td>S</td>
<td>0:00.08</td>
<td>/usr/sbin/appidd -N</td>
</tr>
<tr>
<td>45744</td>
<td>??</td>
<td>S</td>
<td>0:00.05</td>
<td>/usr/sbin/mspd -N</td>
</tr>
<tr>
<td>45745</td>
<td>??</td>
<td>S</td>
<td>0:00.27</td>
<td>/usr/sbin/jdiameterd -N</td>
</tr>
<tr>
<td>45746</td>
<td>??</td>
<td>S</td>
<td>0:00.10</td>
<td>/usr/sbin/pfed -N</td>
</tr>
<tr>
<td>45747</td>
<td>??</td>
<td>S</td>
<td>0:00.19</td>
<td>/usr/sbin/lpdfd -N</td>
</tr>
<tr>
<td>45748</td>
<td>??</td>
<td>S</td>
<td>0:00.64</td>
<td>/sbin/ddc -N</td>
</tr>
<tr>
<td>45750</td>
<td>??</td>
<td>S</td>
<td>0:00.46</td>
<td>/sbin/mib2d -N</td>
</tr>
<tr>
<td>45751</td>
<td>??</td>
<td>S</td>
<td>0:00.16</td>
<td>/sbin/dfwd -N</td>
</tr>
<tr>
<td>45752</td>
<td>??</td>
<td>S</td>
<td>0:00.15</td>
<td>/sbin/irsd -N</td>
</tr>
<tr>
<td>45764</td>
<td>??</td>
<td>S</td>
<td>0:20.60</td>
<td>/sbin/snmpe -N</td>
</tr>
<tr>
<td>56481</td>
<td>??</td>
<td>Ss</td>
<td>0:00.02</td>
<td>telnetd</td>
</tr>
<tr>
<td>56548</td>
<td>??</td>
<td>Rs</td>
<td>0:00.19</td>
<td>mgd: (mgd) (regress)/dev/ttyp0 (mgd)</td>
</tr>
<tr>
<td>56577</td>
<td>??</td>
<td>Ss</td>
<td>0:00.00</td>
<td>mgd: (mgd) (root) (mgd)</td>
</tr>
<tr>
<td>56787</td>
<td>??</td>
<td>R</td>
<td>0:00.00</td>
<td>/bin/ps -ax</td>
</tr>
<tr>
<td>1142</td>
<td>d0-</td>
<td>S</td>
<td>0:00.01</td>
<td>/usr/sbin/usbd -N</td>
</tr>
<tr>
<td>1160</td>
<td>d0-</td>
<td>S</td>
<td>0:29.71</td>
<td>/usr/sbin/eventd -N -r -s -A</td>
</tr>
<tr>
<td>6527</td>
<td>d0+</td>
<td>Is+</td>
<td>0:00.00</td>
<td>/usr/libexec/getty std.9600 ttyd0</td>
</tr>
<tr>
<td>56482</td>
<td>p0</td>
<td>Is</td>
<td>0:00.00</td>
<td>login [pam] (login)</td>
</tr>
<tr>
<td>56483</td>
<td>p0</td>
<td>S</td>
<td>0:00.01</td>
<td>-csh (csh)</td>
</tr>
<tr>
<td>56547</td>
<td>p0</td>
<td>S+</td>
<td>0:00.02</td>
<td>cli</td>
</tr>
<tr>
<td>2392</td>
<td>p1</td>
<td>Is</td>
<td>0:00.00</td>
<td>login [pam] (login)</td>
</tr>
<tr>
<td>2393</td>
<td>p1</td>
<td>I</td>
<td>0:00.00</td>
<td>-csh (csh)</td>
</tr>
<tr>
<td>2394</td>
<td>p1</td>
<td>I</td>
<td>0:00.00</td>
<td>su -</td>
</tr>
<tr>
<td>2395</td>
<td>p1</td>
<td>I+</td>
<td>0:00.01</td>
<td>-su (csh)</td>
</tr>
<tr>
<td>23782</td>
<td>p2</td>
<td>Is</td>
<td>0:00.00</td>
<td>login [pam] (login)</td>
</tr>
<tr>
<td>23881</td>
<td>p2</td>
<td>I</td>
<td>0:00.00</td>
<td>-csh (csh)</td>
</tr>
<tr>
<td>23925</td>
<td>p2</td>
<td>S+</td>
<td>0:00.03</td>
<td>cli</td>
</tr>
</tbody>
</table>
show system processes lcc wide (TX Matrix Plus Routing Matrix)

```
user@host>  show system processes lcc 2 wide
lcc2-re0:
```

```
<table>
<thead>
<tr>
<th>PID</th>
<th>TT</th>
<th>STAT</th>
<th>TIME</th>
<th>PROVIDER</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>??</td>
<td>WLs</td>
<td>0:00.00</td>
<td>(null)</td>
<td>[swapper]</td>
</tr>
<tr>
<td>1</td>
<td>??</td>
<td>IIs</td>
<td>0:00.19</td>
<td>/packages/mnt/jbase/sbin/init --</td>
<td>g_event</td>
</tr>
<tr>
<td>2</td>
<td>??</td>
<td>DL</td>
<td>0:00.02</td>
<td></td>
<td>[g_up]</td>
</tr>
<tr>
<td>3</td>
<td>??</td>
<td>DL</td>
<td>0:00.19</td>
<td></td>
<td>[g_down]</td>
</tr>
<tr>
<td>4</td>
<td>??</td>
<td>DL</td>
<td>0:00.13</td>
<td></td>
<td>[thread taskq]</td>
</tr>
<tr>
<td>5</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[kqueue taskq]</td>
</tr>
<tr>
<td>6</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[pagedaemon]</td>
</tr>
<tr>
<td>7</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[vmdaemon]</td>
</tr>
<tr>
<td>8</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[pagezero]</td>
</tr>
<tr>
<td>9</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[ktrace]</td>
</tr>
<tr>
<td>10</td>
<td>??</td>
<td>RL</td>
<td>0:00.38</td>
<td></td>
<td>[idle]</td>
</tr>
<tr>
<td>11</td>
<td>??</td>
<td>WL</td>
<td>0:00.14</td>
<td></td>
<td>[swi2: net]</td>
</tr>
<tr>
<td>12</td>
<td>??</td>
<td>WL</td>
<td>0:00.14</td>
<td></td>
<td>[swi7: clock sio]</td>
</tr>
<tr>
<td>13</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td></td>
<td>[swi6: vm]</td>
</tr>
<tr>
<td>14</td>
<td>??</td>
<td>DL</td>
<td>0:00.08</td>
<td></td>
<td>[yarrow]</td>
</tr>
<tr>
<td>15</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[swi9: +]</td>
</tr>
<tr>
<td>16</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td></td>
<td>[swi8: +]</td>
</tr>
<tr>
<td>17</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td></td>
<td>[swi5: cambio]</td>
</tr>
<tr>
<td>18</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td></td>
<td>[swi9: task queue]</td>
</tr>
<tr>
<td>19</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td></td>
<td>[irql0: bcm0 uhci1*]</td>
</tr>
<tr>
<td>20</td>
<td>??</td>
<td>WL</td>
<td>0:00.00</td>
<td></td>
<td>[irql1: cb0 uhci0*]</td>
</tr>
<tr>
<td>21</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usbo]</td>
</tr>
<tr>
<td>22</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usbtask]</td>
</tr>
<tr>
<td>23</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usb1]</td>
</tr>
<tr>
<td>24</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usb2]</td>
</tr>
<tr>
<td>25</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usb3]</td>
</tr>
<tr>
<td>26</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usb4]</td>
</tr>
<tr>
<td>27</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usb5]</td>
</tr>
<tr>
<td>28</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usb6]</td>
</tr>
<tr>
<td>29</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[usb7]</td>
</tr>
<tr>
<td>30</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[irq14: ata0]</td>
</tr>
<tr>
<td>31</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[irq15: ata1]</td>
</tr>
<tr>
<td>32</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[irq1: atkbd0]</td>
</tr>
<tr>
<td>33</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[swi0: sio]</td>
</tr>
<tr>
<td>34</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[swi3: ip6opt ipopt]</td>
</tr>
<tr>
<td>35</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[swi4: ip6mismatch+]</td>
</tr>
<tr>
<td>36</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[swi1: ipfw]</td>
</tr>
<tr>
<td>37</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[bufdaemon]</td>
</tr>
<tr>
<td>38</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[vnlnru]</td>
</tr>
<tr>
<td>39</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[syncer]</td>
</tr>
<tr>
<td>40</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[softdepflush]</td>
</tr>
<tr>
<td>41</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[netdaemon]</td>
</tr>
<tr>
<td>42</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[vmuncachedaemon]</td>
</tr>
<tr>
<td>43</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[if_pic_listen]</td>
</tr>
<tr>
<td>44</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[vmmkmmdaemon]</td>
</tr>
<tr>
<td>45</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[if_fpe_listen]</td>
</tr>
<tr>
<td>46</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[vms_csc_housekeeping]</td>
</tr>
<tr>
<td>47</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td></td>
<td>[kern_dump_proc]</td>
</tr>
<tr>
<td>48</td>
<td>??</td>
<td>IL</td>
<td>0:00.00</td>
<td></td>
<td>[nfsiod]</td>
</tr>
</tbody>
</table>
```
show system processes (QFX Series)

user@switch> show system processes

<table>
<thead>
<tr>
<th>PID</th>
<th>TT</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>??</td>
<td>WLs</td>
<td>-2341043-31.01</td>
<td>[swapper]</td>
</tr>
<tr>
<td>1</td>
<td>??</td>
<td>Sls</td>
<td>0:01.34</td>
<td>/packages/mnt/jbase/sbin/init --</td>
</tr>
<tr>
<td>2</td>
<td>??</td>
<td>DL</td>
<td>2:48.31</td>
<td>[g_event]</td>
</tr>
<tr>
<td>3</td>
<td>??</td>
<td>DL</td>
<td>1:47.44</td>
<td>[g_up]</td>
</tr>
<tr>
<td>4</td>
<td>??</td>
<td>DL</td>
<td>1:37.82</td>
<td>[g_down]</td>
</tr>
<tr>
<td>5</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[kdm_tcp_poller]</td>
</tr>
<tr>
<td>6</td>
<td>??</td>
<td>DL</td>
<td>0:00.00</td>
<td>[thread taskq]</td>
</tr>
<tr>
<td>7</td>
<td>??</td>
<td>DL</td>
<td>0:04.86</td>
<td>[kqueue taskq]</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Chapter 24: Administration

9 ?? DL 0:03.94 [pagedaemon]
10 ?? DL 0:00.00 [ktrace]
11 ?? RL 0:00.00 [idle: cpu31]
12 ?? RL 0:00.00 [idle: cpu30]
13 ?? RL 0:00.00 [idle: cpu29]
14 ?? RL 0:00.00 [idle: cpu28]
15 ?? RL 0:00.00 [idle: cpu27]
16 ?? RL 0:00.00 [idle: cpu26]
17 ?? RL 0:00.00 [idle: cpu25]
18 ?? RL 0:00.00 [idle: cpu24]
19 ?? RL 0:00.00 [idle: cpu23]
20 ?? RL 0:00.00 [idle: cpu22]
21 ?? RL 0:00.00 [idle: cpu21]
22 ?? RL 0:00.00 [idle: cpu20]
23 ?? RL 0:00.00 [idle: cpu19]
24 ?? RL 0:00.00 [idle: cpu18]
25 ?? RL 0:00.00 [idle: cpu17]
26 ?? RL 0:00.00 [idle: cpu16]
27 ?? RL 0:00.00 [idle: cpu15]
28 ?? RL 0:00.00 [idle: cpu14]
29 ?? RL 0:00.00 [idle: cpu13]
30 ?? RL 0:00.00 [idle: cpu12]
31 ?? RL 0:00.00 [idle: cpu11]
32 ?? RL 0:00.00 [idle: cpu10]
33 ?? RL 0:00.00 [idle: cpu9]
34 ?? RL 18184:07.25 [idle: cpu8]
35 ?? RL 0:00.00 [idle: cpu7]
36 ?? RL 17862:11.31 [idle: cpu6]
37 ?? RL 19343:45.16 [idle: cpu5]
38 ?? RL 5192:38.30 [idle: cpu4]
39 ?? RL 0:00.00 [idle: cpu3]
40 ?? RL 19278:02.24 [idle: cpu2]
41 ?? RL 19291:00.72 [idle: cpu1]
42 ?? RL 18910:31.21 [idle: cpu0]
43 ?? WL 19:03.74 [swi2: net]
44 ?? WL 261:43.82 [swi7: clock sio]
45 ?? WL 0:00.00 [swi6: vm]
46 ?? DL 2:18.57 [yarrow]
47 ?? WL 0:00.00 [swi9: +]
48 ?? WL 0:00.00 [swi8: +]
49 ?? WL 0:12.36 [swi5: cambio]
50 ?? WL 0:00.00 [swi9: task queue]
51 ?? WL 0:00.00 [swi10: sio]
52 ?? WL 0:32.40 [irq39: ehci0]
53 ?? DL 0:00.21 [usb0]
54 ?? DL 0:00.00 [usbtask]
55 ?? WL 0:00.00 [irq22: xlr_lbus0]
56 ?? WL 0:00.00 [irq38: xlr_lbus0]
57 ?? WL 0:00.00 [swi3: ip6opt ipopt]
58 ?? WL 0:00.00 [swi4: ip6mismatch+]
59 ?? WL 0:00.00 [swi1: ipfw]
60 ?? DL 0:18.65 [pagezero]
61 ?? DL 0:18.59 [bufdaemon]
62 ?? DL 1:10.44 [vn1ru_mem]
63 ?? DL 1:51.66 [syncer]
64 ?? DL 0:20.22 [vn1ru]
65 ?? DL 0:40.48 [softdepflush]
66 ?? DL 0:00.00 [netdaemon]
67 ?? DL 20:47.67 [vkmndemdaemon]
68 ?? DL 0:00.00 [if_pfe_list]
69 ?? SL 0:02.80 [kdm_checkkcore]
Complete Software Guide for Junos® OS for EX4300 Switches, Release 13.2X50

70  ??  SL  0:03.34 [kdm_savekcore]
71  ??  SL  0:04.31 [kdm_livekcore]
72  ??  SL  0:06.14 [kdm_logger]
73  ??  SL  0:00.00 [kdm_logger]
74  ??  SL  0:00.00 [devrt_kernel_thread]
75  ??  DL  0:21.54 [vmuncachedaemon]
76  ??  DL  0:00.00 [if_pic_pause]
77  ??  SL  0:00.00 [nfsiod 0]
78  ??  SL  0:00.00 [nfsiod 1]
79  ??  SL  0:00.00 [nfsiod 2]
80  ??  SL  0:00.00 [nfsiod 3]
81  ??  WL  5:59.98 [irq13: +]
82  ??  RL  105:06.81 [pkt_sender: cpu0]
83  ??  DL  0:00.00 [md0]
84  ??  DL  0:06.01 [md1]
85  ??  DL  0:00.00 [md2]
86  ??  DL  0:00.00 [md3]
87  ??  DL  0:21.17 [md4]
88  ??  DL  0:01.90 [md5]
89  ??  DL  0:06.26 [md6]
90  ??  DL  0:00.00 [md7]
91  ??  SS  0:04.17 /usr/sbin/cron
92  ??  S  0:00.10 /usr/sbin/tnetd -N
93  ??  S  0:06.82 /usr/sbin/mdadm -N
94  ??  S  0:00.32 /usr/sbin/innetd -N
95  ??  S  1:05.34 /usr/sbin/dhcpd -N
96  ??  S  0:00.18 /usr/sbin/inetd -p /var/run/inetd_4.pid -N JU __juniper_private4__
97  ??  L  0:31:21 /usr/sbin/dcm -N (pafxc)
98  ??  S  0:31:21 /usr/sbin/vccpd -N
99  ??  S  9:43.45 /usr/sbin/chassism -N
100 ??  S  0:02.89 /sbin/watchdog -t -l
101 ??  S  3:34.00 /sbin/dcm -N
102 ??  S  10:30.13 /sbin/chassisd -N
103 ??  DL  0:00.21 [peer proxy]
104 ??  S  0:47.03 /sbin/alarmd -N
105 ??  S  0:31.69 /sbin/craftd -N
106 ??  S  0:55.16 /sbin/mib2d -N
107 ??  S  3:40.64 /sbin/rpd -N
108 ??  S  0:00.03 /sbin/tnp.sntpd -N
109 ??  S  0:51.94 /sbin/pfед -N
110 ??  S  0:47.31 /sbin/rmopd -N
111 ??  S  0:33.65 /sbin/cosd
112 ??  S  1:48.41 /sbin/ppmd -N
113 ??  S  0:07.18 /sbin/dfwd -N
114 ??  S  1:02.56 /sbin/bfd -N
115 ??  S  0:00.63 /sbin/rdd -N
116 ??  S  0:40.61 /sbin/dfcd -N
117 ??  S  0:07.81 /sbin/bdbrepd -N
118 ??  S  0:00.28 /sbin/send -N
119 ??  S  1:37.69 /sbin/xntpd -j -N -g -JU __juniper_private4__ (nt
120 ??  S  5:56.28 /sbin/smpd -N JU __juniper_private4__
121 ??  S  16:46.82 /sbin/jdiameterd -N
122 ??  S  2:34.13 /sbin/eswd -N
123 ??  S  1:03.05 /sbin/sflowd -N
124 ??  S  0:22.30 /sbin/fcd -N
125 ??  S  1:07.01 /sbin/vccpdf -N
126 ??  S  0:25.25 /sbin/mcsnoopd -N
127 ??  S  3:45.68 /sbin/rpdf -N
128 ??  S  0:37.87 /sbin/lacpd -N
129 ??  DL  0:01.29 [peer proxy]
130 ??  S  0:00.00 [swi2: FMNITHRD+]

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>State</th>
<th>Elapsed Time</th>
<th>Command and Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1112</td>
<td>??</td>
<td>DL</td>
<td>0:00.03</td>
<td>[peer proxy]</td>
</tr>
<tr>
<td>12816</td>
<td>??</td>
<td>S</td>
<td>15:35.32</td>
<td>/usr/sbin/sfid -N</td>
</tr>
<tr>
<td>30893</td>
<td>??</td>
<td>Ss</td>
<td>0:00.65</td>
<td>sshd: tlewis@tttyp0 (sshd)</td>
</tr>
<tr>
<td>30897</td>
<td>??</td>
<td>Ss</td>
<td>0:00.15</td>
<td>mgd: (mgd) (tlewis)/dev/ttyp0 (mgd)</td>
</tr>
<tr>
<td>30905</td>
<td>??</td>
<td>Ss</td>
<td>0:00.64</td>
<td>sshd: tlewis@tttyp1 (sshd)</td>
</tr>
<tr>
<td>30909</td>
<td>??</td>
<td>Ss</td>
<td>0:00.15</td>
<td>mgd: (mgd) (tlewis)/dev/ttyp1 (mgd)</td>
</tr>
<tr>
<td>30910</td>
<td>??</td>
<td>Ss</td>
<td>0:01.26</td>
<td>sshd: tcheng@tttyp2 (sshd)</td>
</tr>
<tr>
<td>30914</td>
<td>??</td>
<td>Ss</td>
<td>0:00.80</td>
<td>mgd: (mgd) (tcheng)/dev/ttyp2 (mgd)</td>
</tr>
<tr>
<td>30937</td>
<td>??</td>
<td>R</td>
<td>0:00.03</td>
<td>/bin/ps -ax</td>
</tr>
<tr>
<td>661</td>
<td>d0</td>
<td>S</td>
<td>0:21.24</td>
<td>/usr/sbin/eventd -N -r -s -A</td>
</tr>
<tr>
<td>860</td>
<td>d0</td>
<td>Ss+</td>
<td>0:00.07</td>
<td>/usr/libexec/getty std.9600 ttyd0</td>
</tr>
<tr>
<td>30896</td>
<td>p0</td>
<td>Ss+</td>
<td>0:00.55</td>
<td>-cli (cli)</td>
</tr>
<tr>
<td>30908</td>
<td>p1</td>
<td>Ss+</td>
<td>0:00.50</td>
<td>-cli (cli)</td>
</tr>
<tr>
<td>30913</td>
<td>p2</td>
<td>Ss+</td>
<td>0:00.85</td>
<td>-cli (cli)</td>
</tr>
</tbody>
</table>
PART 9

System Services

- Overview on page 1189
- Configuration on page 1229
- Administration on page 1527
Overview

- Software Overview on page 1189
- DHCP Local Server on page 1191
- DHCP Relay Agent on page 1214
- Public Key Cryptography Overview on page 1225
- Self-Signed Certificates Overview on page 1227

Software Overview

- Understanding Software Infrastructure and Processes on page 1189

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- Routing Engine and Packet Forwarding Engine on page 1189
- Junos OS Processes on page 1190

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- Packet Forwarding Engine— Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.
Routing Engine—Provides three main functions:
- Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network.
- Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.
- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

Junos OS Processes

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions. The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

Table 61 on page 112 describes the primary Junos OS processes.

Table 159: Junos OS Processes

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis process</td>
<td>chassid</td>
<td>Detects hardware on the system that is used to configure network interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>eswd</td>
<td>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>switching</td>
<td></td>
<td>Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarding</td>
<td>pfern</td>
<td>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface process</td>
<td>dcd</td>
<td>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</td>
</tr>
</tbody>
</table>
### Table 159: Junos OS Processes (continued)

<table>
<thead>
<tr>
<th>Process</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management process</td>
<td>mgd</td>
<td>Provides communication between the other processes and an interface to the configuration database. Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured. Interacts with the other processes when commands are issued through one of the user interfaces on the switch. If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</td>
</tr>
</tbody>
</table>

| Routing protocol process | rpd  | Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables. |

#### Related Documentation
- For more information about processes, see *Junos OS Network Operations Guide*
- For more information about basic system parameters, supported protocols, and software processes, see *Junos OS System Basics Configuration Guide*

#### DHCP Local Server

- Extended DHCP Local Server Overview on page 1192
- DHCPv6 Local Server Overview on page 1196
- DHCP Local Server Handling of Client Information Request Messages on page 1197
- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 1198
- Group-Specific DHCP Local Server Options on page 1199
- Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients on page 1200
- DHCP Snooping Support on page 1203
- DHCP Auto Logout Overview on page 1204
- Address-Assignment Pools Overview on page 1206
- Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address on page 1207
- Multiple Address Assignment for DHCPv6 Clients on page 1208
- Centrally Configured Opaque DHCP Options on page 1209
- Port Number Requirements for DHCP Firewall Filters on page 1213
Extended DHCP Local Server Overview

You can enable the router or switch to function as an extended DHCP local server and configure the extended DHCP local server options on the router (or switch). The extended DHCP local server provides an IP address and other configuration information in response to a client request. The DHCP local server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or DHCP client authentication. You can configure dynamic profile and authentication support on a global basis or for a specific group of interfaces.

The extended DHCP local server enhances traditional DHCP server operation by utilizing centralized address-assignment pools. The address-assignment pools are managed by the authd process, independently of the DHCP local server, and can be shared by different client applications.

You can also configure the extended DHCP local server to support IPv6 clients. Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client. See “DHCPv6 Local Server Overview” on page 1196 for information about the DHCPv6 local server feature.

NOTE: You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router (or switch), you include the dhcp-local-server statement at the [edit system services] hierarchy level. See the [edit system services dhcp-local-server] Hierarchy Level for the complete DHCP local server syntax.

This overview covers:

- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 1192
- Providing DHCP Client Configuration Information on page 1193
- Minimal Configuration for Clients on page 1194
- DHCP Local Server and Address-Assignment Pools on page 1194
- DHCP Liveness Detection on page 1195

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

The pattern of interaction between the DHCP local server, the DHCP client, and address-assignment pools is the same regardless of whether the software installation is on a router or a switch. Technically, the codes operates in the same manner, regardless of the hardware platform. However, there are some difference in the details of usage.

- On routers—in a typical carrier edge network configuration, the DHCP client is on the subscriber’s computer, and the DHCP local server is configured on the router.
• On switches—In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.

The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber (or DHCP client).

2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.

3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.

4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Providing DHCP Client Configuration Information

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool, the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional — a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address-assignment pool to provide the configuration for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. Table 160 on page 1194 lists the information that RADIUS might include in the authentication grant. See RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management or DHCP management.
### Table 160: Information in Authentication Grant

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS attribute 8</td>
<td>Framed-IP-Address</td>
<td>Client IP address</td>
</tr>
<tr>
<td>RADIUS attribute 9</td>
<td>Framed-IP-Netmask</td>
<td>Subnet mask for client IP address (DHCP option 1)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-4</td>
<td>Primary-DNS</td>
<td>Primary domain server (DHCP option 6)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-5</td>
<td>Secondary-DNS</td>
<td>Secondary domain server (DHCP option 6)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-6</td>
<td>Primary-WINS</td>
<td>Primary WINS server (DHCP option 44)</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-7</td>
<td>Secondary-WINS</td>
<td>Secondary WINS server (DHCP option 44)</td>
</tr>
<tr>
<td>RADIUS attribute 27</td>
<td>Session-Timeout</td>
<td>Lease time</td>
</tr>
<tr>
<td>RADIUS attribute 88</td>
<td>Framed-Pool</td>
<td>Address assignment pool name</td>
</tr>
<tr>
<td>Juniper Networks VSA 26-109</td>
<td>DHCP-Guided-Relay-Server</td>
<td>DHCP relay server</td>
</tr>
</tbody>
</table>

### Minimal Configuration for Clients

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client’s subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

### DHCP Local Server and Address-Assignment Pools

In the traditional DHCP server operation, the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools.
The centralized address-assignment pools are managed by the authd process, independently of the DHCP local server, and can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

**DHCP Liveness Detection**

Liveness detection for DHCP subscriber IP (or DHCP client IP) sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients are expected to respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented. You can configure

NOTE: DHCP liveness detection either globally or per DHCP group.

**Related Documentation**

- Address-Assignment Pools Overview on page 1206
- Configuring Address-Assignment Pools
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 1279
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview
- Using External AAA Authentication Services with DHCP on page 1256
- Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address on page 1207
- Graceful Routing Engine Switchover
- Subscriber Management Unified ISSU Support
DHCPv6 Local Server Overview

The DHCPv6 local server enhances the extended DHCP local server by providing support for IPv6. When a DHCPv6 client logs in, the DHCPv6 local server can optionally use the AAA service framework to interact with the RADIUS server. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters.

You can configure DHCPv6 local server to communicate the following attributes to the AAA service framework and RADIUS at login time:

- Client username
- Client password

**NOTE:** The client username, which uniquely identifies a subscriber or a DHCP client, must be present in the configuration in order for DHCPv6 local server to use RADIUS authentication.

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in Table 161 on page 1196 to configure the client:

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Session-Timeout</td>
<td>Lease time, in seconds. If not supplied, the lease does not expire</td>
</tr>
<tr>
<td>123</td>
<td>Delegated-IPv6-Prefix</td>
<td>Prefix that is delegated to the client</td>
</tr>
<tr>
<td>26-143</td>
<td>Max-Clients-Per-Interface</td>
<td>Maximum number of clients allowed per interface</td>
</tr>
</tbody>
</table>

The DHCPv6 local server is compatible with the extended DHCP local server and the extended DHCP relay agent, and can be enabled on the same interface as either the extended DHCP local server or DHCP relay agent.
The DHCPv6 local server provides many of the same features as the extended DHCP local server, including:

- Configuration for a specific interface or for a group of interfaces
- Site-specific usernames and passwords
- Numbered Ethernet interfaces
- Statically configured CoS and filters
- AAA directed login
- Use of the IA_NA option to assign a specific address to a client

To configure the extended DHCPv6 local server on the router (or switch), you include the `dhcpv6` statement at the `[editsystemservicesdhcp-local-server]` hierarchy level. See the `[edit system services dhcp-local-server] Hierarchy Level` for the complete DHCP local server syntax, including the DHCPv6 syntax.

You can also include the `dhcpv6` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name system services dhcp-local-server]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server]`

**Related Documentation**

- Extended DHCP Local Server Overview on page 1192
- Using External AAA Authentication Services with DHCP on page 1256
- Grouping Interfaces with Common DHCP Configurations on page 1258
- Group-Specific DHCP Local Server Options on page 1199
- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Configuring Passwords for Usernames on page 1276
- Creating Unique Usernames for DHCP Clients on page 1276
- Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address on page 1207
- Verifying and Managing DHCPv6 Local Server Configuration on page 1532
- Example: Extended DHCPv6 Local Server Configuration

**DHCP Local Server Handling of Client Information Request Messages**

DHCP clients that already have externally provided addresses may solicit further configuration information from a DHCP server by sending a DHCP information request that indicates what information is desired. By default, DHCP local server and DHCPv6 local server ignore any DHCP information requests that they receive. You can override this default behavior to enable processing of these messages. Include the `process-inform`
statement at the [edit system services dhcp-local-server overrides] or [edit system services
dhcp-local-server dhcpv6 overrides] hierarchy level.

By default, DHCP relay and DHCP relay proxy automatically forward DHCP information
request messages without modification if the messages are received on an interface
configured for a DHCP server group. DHCP relay and relay proxy drop information request
messages received on any other interfaces. You cannot disable this default DHCP relay
and relay proxy behavior.

The information requested by these clients has typically been configured with the
dhcp-attributes statement for an address pool defined by the address-assignment pool
pool-name statement at the [edit access] hierarchy level.

When you enable processing of DHCP information requests, you can optionally specify
the name of the pool from which the local server retrieves the requested configuration
information for the client. If you do not do specify a local pool, then the local server
requests that AAA selects and returns only the name of the relevant pool.

DHCP local server responds to the client with a DHCP acknowledgment message that
includes the requested information—if it is available. DHCPv6 local server responds in
the same manner but uses a DHCP reply message. No subscriber management or
DHCP-management is applied as a result of the DHCP information request message.

NOTE: PPP interfaces are not supported on EX Series switches.

When DHCPv6 is configured over PPP interfaces, the PPP RADIUS authentication data
can be used to select the pool from which the response information is taken. Additionally
other RADIUS attributes can also be inserted into the DHCPv6 reply message. If an overlap
exists between RADIUS attributes and local pool attributes, the RADIUS values are used
instead of the local configuration data. If no RADIUS information is received from the
underlying PPP interface, then the behavior is the same as described previously for
non-PPP interfaces.

Related Documentation
- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Enabling Processing of Client Information Requests on page 1265

DHCP Duplicate Client Differentiation Using Client Subinterface Overview

In some network environments, client IDs and MAC addresses might not be unique,
resulting in duplicate clients. For example, two network adapters might be manufactured
with the same hardware address, resulting in a duplicate MAC address among the DHCP
clients attached to the router (or switch). A duplicate DHCP client occurs when a client
attempts to get a lease, and that client has the same client ID or the same MAC address
as an existing DHCP client.

When DHCP server receives a request from a new client that has a duplicate ID or MAC
address, DHCP server terminates the address lease for the existing client and returns the
address to its original address pool. DHCP server then assigns a new address and lease
to the new client.

By default, both DHCP local server and DHCP relay use the subnet information to
differentiate between duplicate clients. However, in some cases, this level of differentiation
is not adequate. For example, when multiple subinterfaces share the same underlying
loopback interface with the same preferred source address, the interfaces appear to be
on the same subnet. In this situation, the default configuration prevents duplicate clients.

You can provide greater differentiation between duplicate clients by configuring DHCP
to consider the client subinterface when duplicate clients occur. In this optional
configuration, DHCP uniquely identifies:

- The subnet on which the client resides
- The subinterface on which the client resides
- The client within the subnet

Related Documentation
- Configuring DHCP Duplicate Client Support on page 1258
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 1257

Group-Specific DHCP Local Server Options

You can include the following statements at the [edit system services dhcp-local-server
group group-name] hierarchy level to set group-specific DHCP local server configuration
options, and at the [edit system services dhcp-local-server] hierarchy level to set global
DHCP local server configuration options. Statements configured at the [edit system
services dhcp-local-server group group-name] hierarchy level apply only to the named
group of interfaces, and override any global DHCP local server settings configured with
the same statements at the [edit system services dhcp-local-server] hierarchy level.

DHCPv6 local server supports the same set of statements with the exception of the
dynamic-profile statement.

- authentication—Configure the parameters the router sends to the external AAA server.
- dynamic-profile—Specify the dynamic profile that is attached to a group of interfaces.
- interface—Specify one or more interfaces, or a range of interfaces, that are within the
  specified group.
- overrides—Override the default configuration settings for the extended DHCP local
  server. For information, see "Overriding Default DHCP Local Server Configuration
  Settings" on page 1261.

Related Documentation
- Grouping Interfaces with Common DHCP Configurations on page 1258
Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients

Dynamic reconfiguration of clients enables the extended DHCP local server to initiate a client update without waiting for the client to initiate a request.

Default Client/Server Interaction

Typically the DHCP client initiates all of the basic DHCP client/server interactions. The DHCP server sends information to a client only in response to a request from that client. This behavior does not enable a client to be quickly updated with its network address and configuration in the event of server changes:

NOTE: Technically, the DHCP client/server interactions are the same on routers and switches. However, the primary usage of this technology on the routers is for subscriber management. The switches are not used for subscriber management. Therefore, this topic provides two sample scenarios. The actions are the same, but the implementation details are different.

- On routers—Suppose a service provider restructures its addressing scheme or changes the server IP addresses that it provided to clients. Without dynamic reconfiguration, the service provider typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, the provider can wait for customers to make a service call about the network failures and then instruct them to power cycle their customer premises equipment to reinitiate the connection. Neither of these actions is timely or convenient for customers.

- On switches—Suppose you restructure the addressing scheme or change the server IP addresses that the DHCP server provides to clients. Without dynamic reconfiguration, the network typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, you can wait for users to notify you of the network failures and then instruct them to power cycle their equipment to reinitiate the connection. Neither of these actions is timely or convenient for users.

Dynamic Client/Server Interaction for DHCPv4

Dynamic reconfiguration for DHCPv4 is available through a partial implementation of RFC 3203, DHCP Reconfigure Extension for DHCPv4. It enables the DHCPv4 local server to send a message to the client to force reconfiguration.
The server sends a forcerenew message to a DHCPv4 client, initiating a message exchange. In response, DHCPv4 clients that support the forcerenew message then send a lease renewal message to the server. The server rejects the lease renewal request and sends a NAK to the client, causing the client to reinitiate the DHCP connection. A successful reconnection results in the reconfiguration of the DHCP client. Only the exchange of forcerenew, renew, and NAK messages is supported from RFC 3202. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to forcerenew messages other than to forward them to the client.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber services or DHCP-managed services, such as forwarding and statistics, continue to work. Client statistics are not maintained in the interval between a successful reconfiguration and the subsequent client binding. When the server responds to the client renewal request with a NAK, the client entry is removed from the binding table and final statistics are reported. New statistics are collected when the client sends a discover message to establish a new session.

**Dynamic Client/Server Interaction for DHCPv6**

Dynamic reconfiguration for DHCPv6 is available through a partial implementation of RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. It enables the DHCPv6 local server to send a message to the client to force reconfiguration.

DHCPv6 servers send reconfigure messages to DHCPv6 clients, initiating a message exchange. In response, DHCPv6 clients that support the reconfigure message transition to the renewing state and send a renew message to the server. The server returns a reply message with a lifetime of zero (0). The client transitions to the init state and sends a solicit message. The server sends an advertise message to indicate that it is available for service. The client sends a request for configuration parameters, which the server then includes in its reply. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to reconfigure messages other than to forward them to the client.

When a DHCPv6 server is triggered to initiate reconfiguration on a bound DHCPv6 client, the client transitions to the reconfigure state. All subscriber services, such as forwarding and statistics, continue to work. The server then sends the reconfigure message to the client. If the DHCPv6 client is already in the reconfigure state, the DHCPv6 server ignores the reconfiguration trigger. For clients in any state other than bound or reconfigure, the server clears the binding state of the client, as if the `clear dhcpv6 server binding` command had been issued.

**Dynamic Configuration Options**

You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

- To enable dynamic reconfiguration with default reconfiguration values for all DHCP clients, include the `reconfigure` statement at the `[edit system services dhcp-local-server]` hierarchy level for DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6]` hierarchy level for DHCPv6 clients.
Alternatively, to enable dynamic reconfiguration for only the DHCP clients serviced by a specified group of interfaces, include the `reconfigure` statement at the `[edit system services dhcp-local-server group group-name]` hierarchy level for DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level for DHCPv6 clients.

You can optionally modify the behavior of the reconfiguration process by including the appropriate statements at the `[edit system services dhcp-local-server reconfigure]` hierarchy level for all DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6 reconfigure]` hierarchy level for all DHCPv6 clients. To override this global configuration for only the DHCP clients serviced by a specified group of interfaces, you can include the statements with different values at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level for DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]` hierarchy level for DHCPv6 clients.

Include the `attempts` statement to specify how many times the local server sends the `forcerenew` or `reconfigure` message to initiate client reconfiguration. Include the `timeout` statement to set the interval between the first and second attempts. The interval between each subsequent attempt doubles the previous value. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on.

By default, the DHCP client’s original configuration is restored if all of the reconfiguration attempts fail. Include the `clear-on-abort` statement to delete the client instead.

You can configure an authentication token by including the `token` statement. The DHCP local server then includes this token inside the authentication option when it sends `forcerenew` or `reconfigure` messages. If the service provider has previously configured the DHCP client with this token, then the client can compare that token against the newly received token, and reject the message if the tokens do not match. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

In the event of a RADIUS-initiated disconnect (RID), the client is deleted by default. You can configure the client to be reconfigured instead of deleted by including the `radius-disconnect` statement. The client is deleted if all attempts to reconfigure the client fail.

For the DHCPv6 server only, you can include the `strict` statement. By default, the server accepts `solicit` messages from clients that do not support server-initiated reconfiguration. Including this statement causes the server to discard `solicit` messages from nonsupporting clients; consequently the server does not bind these clients.

You can force the local server to initiate the reconfiguration process for clients by issuing the `request dhcp server reconfigure` command for DHCPv4 clients, and the `request dhcpv6 server reconfigure` command for DHCPv6 clients. Command options determine whether reconfiguration is then attempted for all clients or specified clients.
Events that take place while a reconfiguration is in process take precedence over the reconfiguration. Table 162 on page 1203 lists the actions taken in response to several different events.

### Table 162: Action Taken for Events That Occur During a Reconfiguration

<table>
<thead>
<tr>
<th>Event</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server receives a discover (DHCPv4) or solicit (DHCPv6) message from the client.</td>
<td>Server drops packet and deletes client.</td>
</tr>
<tr>
<td>Server receives a request, renew, rebind, or init-reboot message from the client.</td>
<td>DHCPv4—Server sends NAK message and deletes client. DHCPv6—Server drops packet and deletes client. Server replies to renew message with lease time of zero (0).</td>
</tr>
<tr>
<td>Server receives a release or decline message from the client.</td>
<td>Server deletes client.</td>
</tr>
<tr>
<td>The client lease times out.</td>
<td>Server deletes client.</td>
</tr>
<tr>
<td>The <code>clear dhcp server binding</code> command is issued.</td>
<td>Server deletes client.</td>
</tr>
<tr>
<td>The <code>request dhcpv4 server reconfigure</code> or <code>request dhcpv6 server reconfigure</code> command is issued.</td>
<td>Command is ignored.</td>
</tr>
<tr>
<td>GRES or DHCP restart occurs.</td>
<td>Reconfiguration process is halted.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268

### DHCP Snooping Support

DHCP snooping provides DHCP security on the router or switch by filtering incoming messages. When DHCP snooping is enabled, the router differentiates between trusted and untrusted interfaces, and forwards messages from trusted sources while rejecting the untrusted messages.

In Junos OS, DHCP snooping is enabled in a routing instance when you configure either the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level, or the `dhcp-local-server` statement at the `[edit system services]` hierarchy level in that routing instance. However, depending on the Junos OS release, the router processes the snooped packets differently, as described in the following list:

- In Junos OS Release 10.0 and earlier, the router processes snooped packets normally.
- In Junos OS Release 10.1 and later, the router discards snooped packets by default. To enable normal processing of snooped packets in Junos OS Release 10.1 and later, you must explicitly configure the `allow-snooped-clients` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.
You can configure DHCP snooping support for the following:

- **DHCPv4 relay agent**—Override the router’s (or switch’s) default snooping configuration and specify that DHCP snooping is enabled or disabled globally, for a named group of interfaces, or for a specific interface within a named group.

  In a separate procedure, you can set a global configuration to specify whether the DHCPv4 relay agent forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces. The router also uses the global DHCP relay agent snooping configuration to determine whether to forward or drop snooped BOOTREPLY packets.

- **DHCPv6 relay agent**—As you can with snooping support for the DHCPv4 relay agent, you can override the default DHCPv6 relay agent snooping configuration on the router to explicitly enable or disable snooping support globally, for a named group of interfaces, or for a specific interface with a named group of interfaces.

  In multi-relay topologies where more than one DHCPv6 relay agent is between the DHCPv6 client and the DHCPv6 server, snooping enables intervening DHCPv6 relay agents between the client and the server to correctly receive and process the unicast traffic from the client and forward it to the server. The DHCPv6 relay agent snoops incoming unicast DHCPv6 packets by setting up a filter with UDP port 547 (the DHCPv6 UDP server port) on a per-forwarding table basis. The DHCPv6 relay agent then processes the packets intercepted by the filter and forwards the packets to the DHCPv6 server.

  Unlike the DHCPv4 relay agent, the DHCPv6 relay agent does not support global configuration of forwarding support for DHCPv6 snooped packets.

- **DHCP local server**—Configure whether DHCP local server forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces.

**Related Documentation**
- Configuring DHCP Snooping for DHCP Relay Agent on page 1293
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 1274
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 1239

**DHCP Auto Logout Overview**

This topic provides an introduction to the optional DHCP auto logout feature and includes the following sections:

- Auto Logout Overview on page 1204
- How DHCP Identifies and Releases Clients on page 1205
- Option 60 and Option 82 Requirements on page 1206

**Auto Logout Overview**

Auto logout is an optional configuration for DHCP local server and DHCP relay agent that improves the efficiency of DHCP IP address assignment. Auto logout enables IP addresses to be immediately released and returned to the address pool when the addresses are no
longer used by DHCP clients. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example (on the routers), you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address—the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. The secondary identification method is based on the DHCP option 60 and option 82 information in DHCP discover messages.

Both the primary and secondary identification methods use subnet information to differentiate between clients. The primary identification method differentiates between two clients with the same MAC address (or same Client Identifier) if the clients are on different subnets. Similarly, the secondary identification method considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the discover packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

If the DHCP relay receives a DISCOVER message from an existing client, the DHCP relay forwards the DISCOVER message to the DHCP server. The DHCP relay preserves the binding if the client’s existing IP address is returned by the DHCP server. This
behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.

NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in "DHCP Relay Agent Option 82 Value for Auto Logout" on page 1292.

Related Documentation

- Automatically Logging Out DHCP Clients on page 1264
- DHCP Relay Agent Option 82 Value for Auto Logout on page 1292
- Clearing DHCP Bindings for Subscriber Access

Address-Assignment Pools Overview

The address-assignment pool feature supports subscriber management and DHCP management functionality by enabling you to create centralized IPv4 and IPv6 address pools independently of the client applications that use the pools. The authd process manages the pools and the address allocation, whether the addresses come from local pools or from a RADIUS server. For example, multiple client applications, such as DHCP, can use the same address-assignment pool to provide addresses for their particular clients. Client applications can acquire addresses for either authenticated or unauthenticated clients.

Address-assignment pools support both dynamic and static address assignment. In dynamic address assignment, a client is automatically assigned an address from the address-assignment pool. In static address assignment, which is supported for IPv4 pools only, you reserve an address that is then always used by a particular client. Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

You can configure named address ranges within an address-assignment pool. A named range is a subset of the overall address range. A client application can use named ranges to manage address assignment based on client-specific criteria. For example, for IPv4 address-assignment pools, you might create a named range that is based on a specific DHCP option 82 value. Then, when a DHCP client request matches the specified option 82 value, an address from the specified range is assigned to the client.
You can link address-assignment pools together to provide backup pools for address assignment. When the primary pool is fully allocated, the router or switch automatically switches to the linked, or secondary, pool and begins allocating addresses from that pool.

You can also explicitly identify that an address-assignment pool is used for ND/RA.

**Related Documentation**
- Configuring Address-Assignment Pools
- DNS Address Assignment Precedence
- Address-Assignment Pools Licensing Requirements
- Example: Configuring an Address-Assignment Pool
- Configuring an Extended DHCP Server with DHCPv6 on EX Series Switches (CLI Procedure)

---

**Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address**

Subscriber management or DHCP management enables you to specify that DHCP local server assign a particular address to a client. For example, if a client is disconnected, you might use this capability to assign the same address that the client was using prior to being disconnected. If the requested address is available, DHCP assigns it to the client. If the address is unavailable, the DHCP local server offers another address, based on the address allocation process.

Both DHCP local server and DHCPv6 local server support the specific address request feature. DHCP local server uses DHCP option 50 in DHCP DISCOVER messages to request a particular address, while DHCPv6 local server uses the IA_NA option (Identity Association for Non-Temporary Addresses) in DHCPv6 SOLICIT messages.

---

**NOTE:** Subscriber management (DHCP management) supports only one address for each of the DHCPv6 IA_NA or IA_PD address types. If the DHCPv6 client requests more than one address for a given type, the DHCPv6 local server uses only the first address and ignores the other addresses.

---

**Related Documentation**
- Extended DHCP Local Server Overview on page 1192
- DHCPv6 Local Server Overview on page 1196
Multiple Address Assignment for DHCPv6 Clients

Subscriber management (on the routers) or DHCP management (on the switches) enables you to assign multiple addresses to a single DHCPv6 client. Multiple address support is enabled by default, and is activated when the DHCPv6 local server receives a DHCPv6 Solicit message from a subscriber (or DHCP client) that contains multiple addresses.

For example, if you are implementing this feature on the routers, you might use the multiple address assignment feature in a networking environment in which a customer premises equipment (CPE) device requires a host address and a delegated prefix. In such an environment, you can configure subscriber management to assign both a DHCPv6 IA_NA (Identity Association for Non-Temporary Addresses) and an IA_PD (Identity Association for Prefix Delegation) address to the client (the CPE device).

- Multiple Address Assignment Using Local Address Pools or RADIUS on page 1208
- Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment on page 1208

Multiple Address Assignment Using Local Address Pools or RADIUS

You can use either local address pools or RADIUS when assigning multiple addresses to a DHCP client. When at least one address is successfully allocated, the router or switch creates a subscriber (or DHCP client) entry and binds the entry to the assigned address. If both addresses are successfully allocated, the router (or switch) creates a single subscriber (or DHCP client) entry and binds both addresses to that entry.

You can also configure a delegated address pool, which explicitly specifies the address pool that subscriber management (or DHCP management) uses to assign IPv6 prefixes for subscribers (or DHCP clients).

Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment

NOTE: EX Series switches do not support demux.

(On the routers only) Subscriber management provides a predefined variable that you can use to dynamically configure DHCPv6 multiple address assignment. You apply the Junos OS predefined variable, $junos-subscriber-ipv6-multi-address, as a demux source address in a dynamic profile. When the dynamic profile is attached to a subscriber, the variable is expanded to include both the host and prefix addresses. You use this variable instead of the $junos-subscriber-ipv6-address variable, which supports a single IPv6 address.

You include the $junos-subscriber-ipv6-multi-address variable at the [edit dynamic-profile profile-name interfaces interface-name unit logical-unit-number family inet6 demux-source] hierarchy level.

Related Documentation
- Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 1266
- Junos OS Predefined Variables
Centrally Configured Opaque DHCP Options
Subscriber management (on the routers) or DHCP management (on the switches) enables you to centrally configure DHCP options on a RADIUS server and then distribute the options on a per-subscriber or per DHCP-client basis. This method results in RADIUS-sourced DHCP options—the DHCP options originate at the RADIUS server and are sent to the subscriber (or DHCP client). This differs from the traditional client-sourced method (also called DHCP-sourced) of configuring DHCP options, in which the options originate at the client and are sent to the RADIUS server. The subscriber management (DHCP management) RADIUS-sourced DHCP options are also considered to be *opaque*, because DHCP local server performs minimal processing and error checking for the DHCP options string before passing the options to the subscriber (DHCP client).

Subscriber management (or DHCP management) uses Juniper Networks VSA 26-55 (DHCP-Options) to distribute the RADIUS-sourced DHCP options. The RADIUS server includes VSA 26-55 in the Access-Accept message that the server returns during subscriber authentication or DHCP client authentication. The RADIUS server sends the Access-Accept message to the RADIUS client, and then on to DHCP local server for return to the DHCP subscriber. The RADIUS server can include multiple instances of VSA 26-55 in a single Access-Accept message. The RADIUS client concatenates the multiple instances and uses the result as a single instance.

There is no CLI configuration required to enable subscriber management (DHCP management) to use the centrally configured DHCP options—the procedure is triggered by the presence of VSA 26-55 in the RADIUS Access-Accept message.

When building the offer packet for the DHCP client, DHCP local server uses the following sequence:

1. Processes any RADIUS-configured parameters that are passed as separate RADIUS attributes; for example, RADIUS attribute 27 (Session Timeout).
2. Processes any client-sourced parameters; for example, RADIUS attributes 53 (DHCP Message Type) and 54 (Server Identifier).
3. Appends (without performing any processing) the opaque DHCP options string contained in the VSA 26-55 received from the RADIUS server.

In addition to supporting central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options), subscriber management (DHCP management) also supports the traditional client-sourced options configuration, in which the router’s (switch’s) DHCP component sends the options to the RADIUS server. The client-sourced DHCP options method is supported for both DHCP local server and DHCP relay agent; however, the RADIUS-sourced central configuration method is supported on DHCP local server only. Both the RADIUS-sourced and client-sourced methods support DHCPv4 and DHCPv6 subscribers (clients).

**NOTE:** You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.
Data Flow for RADIUS-Sourced DHCP Options

Figure 5 on page 1211 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

Figure 5: DHCP Options Data Flow

The following general sequence describes the data flow when subscriber management (DHCP management) uses RADIUS-sourced DHCP options and VSA 26-55 to configure a DHCP subscriber (client):

1. The subscriber (DHCP client) sends a DHCP discover message (or DHCPv6 solicit message) to the DHCP local server. The message includes client-sourced DHCP options.
2. The DHCP local server initiates authentication with the Junos OS RADIUS client.
3. The RADIUS client sends an Access-Request message on behalf of the subscriber (DHCP client) to the external RADIUS server. The message includes the subscriber’s (DHCP client’s) client-sourced DHCP options.
4. The external RADIUS server responds by sending an Access-Accept message to the RADIUS client. The Access-Accept message includes the RADIUS-sourced opaque DHCP options in VSA 26-55.
5. The RADIUS client sends the DHCP options string to DHCP local server. If there are multiple VSA 26-55 instances, the RADIUS client first assembles them into a single options string.
6. DHCP local server processes all options into the DHCP offer (or DHCPv6 reply) message, except for the RADIUS-sourced VSA 26-55 DHCP options. After processing all other options, DHCP local server then appends the unmodified VSA 26-55 DHCP options to the message and sends the message to the subscriber (DHCP client).
7. The subscriber (DHCP client) is configured with the DHCP options.

8. The following operations occur after the subscriber (DHCP client) receives the DHCP options:
   • Accounting—The RADIUS client sends Acct-Start and Interim-Accounting requests to the RADIUS server, including the RADIUS-sourced DHCP options in VSA 26-55. By default, the DHCP options are included in accounting requests.
   • Renewal—When the subscriber (DHCP client) renews, the cached DHCP options value is returned in the DHCP renew (or DHCPv6 ACK) message. The originally assigned DHCP options cannot be modified during a renew cycle.
   • Logout—When the subscriber (DHCP client) logs out, the RADIUS client sends an Acct-Stop message to the RADIUS server, including the RADIUS-sourced VSA 26-55.

### Multiple VSA 26-55 Instances Configuration

VSA 26-55 supports a maximum size of 247 bytes. If your RADIUS-sourced DHCP options field is greater than 247 bytes, you must break the field up and manually configure multiple instances of VSA 26-55 for the RADIUS server to return. When using multiple instances for an options field, you must place the instances in the packet in the order in which the fragments are to be reassembled by the RADIUS client. The fragments can be of any size of 247 bytes or less.

**BEST PRACTICE:** For ease of configuration and management of your DHCP options, you might want to have one DHCP option per VSA 26-55 instance, regardless of the size of the option field.

When the RADIUS client returns a reassembled opaque options field in an accounting request to the RADIUS server, the client uses 247-byte fragments. If you had originally created instances of fewer than 247 bytes, the returned fragments might not be the same as you originally configured on the RADIUS server.

**NOTE:** If you are configuring Steel-Belted Radius (SBR) to support multiple VSA 26-55 instances, ensure that you specify VSA 26-55 with the RO flags in the Subscriber Management RADIUS dictionary file. The R value indicates a multivalued reply attribute and the O value indicates an ordered attribute.

### DHCP Options That Cannot Be Centrally Configured

Table 163 on page 1213 shows the DHCP options that you must not centrally configure on the RADIUS server.
Table 163: Unsupported Opaque DHCP Options

<table>
<thead>
<tr>
<th>DHCP Option</th>
<th>Option Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 0</td>
<td>Pad Option</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Option 51</td>
<td>IP Address Lease Time</td>
<td>Value is provided by RADIUS attribute 27 (Session-Timeout).</td>
</tr>
<tr>
<td>Option 52</td>
<td>Option Overload</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Option 53</td>
<td>DHCP Message Type</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td>Option 54</td>
<td>Server Identifier</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td>Option 55</td>
<td>Parameter Request List</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td>Option 255</td>
<td>End</td>
<td>Value is provided by DHCP local server.</td>
</tr>
<tr>
<td></td>
<td>–</td>
<td>DHCP magic cookie – Not supported.</td>
</tr>
</tbody>
</table>

Related Documentation

- Monitoring DHCP Options Configured on RADIUS Servers

Port Number Requirements for DHCP Firewall Filters

When you configure a firewall filter to perform some action on DHCP packets at the Routing Engine, such as protecting the Routing Engine by allowing only proper DHCP packets, you must specify both port 67 (bootps) and port 68 (bootpc) for both the source and destination. The firewall filter acts at both the line cards and the Routing Engine.

This requirement applies to both DHCP local server and DHCP relay, but it applies only when DHCP is provided by the jdhcpd process. MX Series routers, MI20 routers, and M320 routers use jdhcpd. For DHCP relay, that means the configuration is required only at the \[edit forwarding-options dhcp-relay\] hierarchy level and not at the \[edit forwarding-options helpers bootp\] hierarchy level.

DHCP packets received on the line cards are encapsulated by jdhcpd with a new UDP header where their source and destination addresses are set to port 68 before being forwarded to the Routing Engine.

For DHCP relay and DHCP proxy, packets sent to the DHCP server from the router have both the source and destination UDP ports set to 67. The DHCP server responds using the same ports. However, when the line card receives these DHCP response packets, it changes both port numbers from 67 to 68 before passing the packets to the Routing Engine. Consequently the filter needs to accept port 67 for packets relayed from the client to the server, and port 68 for packets relayed from the server to the client.
Failure to include both port 67 and port 68 as described here results in most DHCP packets not being accepted.

For complete information about configuring firewall filters in general, see Junos OS Firewall Filters and Traffic Policers Library for Routing Devices.

### Related Documentation
- Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine
- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215
- Dynamic Firewall Filters Overview

### DHCP Relay Agent
- Extended DHCP Relay Agent Overview on page 1215
- DHCP Relay Proxy Overview on page 1218
- DHCPv6 Relay Agent Overview on page 1220
- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 1221
- Group-Specific DHCP Relay Options on page 1221
- DHCP Snooping Support on page 1222
- DHCP Auto Logout Overview on page 1223
Extended DHCP Relay Agent Overview

You can configure extended DHCP relay options on the router or on the switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or DHCP client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCP relay agents.

On the routers, you can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers. For more information about how to use the DHCP relay agent in a video/IPTV application, see the Junos OS Feature Guides.

On the switches, you can use DHCP relay to obtain configuration parameters including an IP address for DHCP clients.

NOTE: The extended DHCP relay agent options configured with the dhcp-relay statement are incompatible with the DHCP/BOOTP relay agent options configured with the bootp statement. As a result, you cannot enable both the extended DHCP relay agent and the DHCP/BOOTP relay agent on the router at the same time.

For information about the DHCP/BOOTP relay agent, see the Routing Policy Feature Guide for Routing Devices.

You can also configure the extended DHCP relay agent to support IPv6 clients. See “DHCPv6 Relay Agent Overview” on page 1220 for information about the DHCPv6 relay agent feature.

To configure the extended DHCP relay agent on the router (or switch), include the dhcp-relay statement at the [edit forwarding-options] hierarchy level. See the [edit forwarding-options dhcp-relay] Hierarchy Level for the complete DHCP relay agent syntax.

You can also include the dhcp-relay statement at the following hierarchy levels:

- [edit logical-systems logical-system-name forwarding-options]
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options]
- [edit routing-instances routing-instance-name forwarding-options]
This overview covers:

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers on page 1216
- DHCP Liveness Detection on page 1217

### Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers

The pattern of interaction among the DHCP Relay agent, DHCP client, and DHCP servers is the same regardless of whether the software installation is on a router or a switch. However, there are some differences in the details of usage.

On routers—in a typical carrier edge network configuration, the DHCP client is on the subscriber’s computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.

On switches—in a typical network configuration, the DHCP client is on an access device such as a personal computer and the DHCP relay agent is configured on the switch between the DHCP client and one or more DHCP servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.

1. The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client’s state.
3. In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
4. On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.
6. The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client’s configuration parameters.
8. The DHCP relay agent receives the ACK packet and forwards it to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay
agent “snoops” on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as lease shadowing or passive snooping.

**DHCP Liveness Detection**

Liveness detection for DHCP subscriber or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients are expected to respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

---

**NOTE:** DHCP liveness detection either globally or per DHCP group.

---

**Related Documentation**

- DHCPv6 Relay Agent Overview on page 1220
- Access and Access-Internal Routes for Subscriber Management
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview
- Using External AAA Authentication Services with DHCP on page 1256
- DHCP Relay Proxy Overview on page 1218
- Graceful Routing Engine Switchover
- Subscriber Management Unified ISSU Support
- Verifying and Managing DHCP Relay Configuration on page 1532
- Tracing Extended DHCP Operations
- Example: Minimum DHCP Relay Agent Configuration on page 1234
- Example: DHCP Relay Agent Configuration with Multiple Clients and Servers
- Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 1235
- Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing
- Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine
DHCP Relay Proxy Overview

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

DHCP relay proxy provides the following benefits:

- **DHCP server isolation and DoS protection**—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.

- **Multiple lease offer selection**—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.

- **Support for both numbered and unnumbered Ethernet interfaces**—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is automatically removed when the lease time expires or when the client releases the address.

- **Logical system support**—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.

---

**NOTE:** Extended DHCP relay proxy is not supported for the J Series Services Routers DHCP server. Also, you cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.

---

Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers

The DHCP relay agent is configured on the router (or switch), which operates between the DHCP client and one or more DHCP servers.
The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.
2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.
3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:
   - a. Selects the first offer received as the offer to sent to the client
   - b. Replaces the DHCP server address with the address of the DHCP relay proxy
   - c. Forwards the offer to the DHCP client.
4. The DHCP client receives the offer from the DHCP relay proxy.
5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.
6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.
8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.
11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

Related Documentation
- Extended DHCP Relay Agent Overview on page 1215
- Enabling DHCP Relay Proxy Mode on page 1307
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 1310
DHCPv6 Relay Agent Overview

The DHCPv6 relay agent enhances the extended DHCP relay agent by providing support in an IPv6 network. The DHCPv6 relay agent passes messages between the DHCPv6 client and the DHCPv6 server, similar to the way DHCP relay agent supports an IPv4 network.

When a DHCPv6 client logs in, the DHCPv6 relay agent uses the AAA service framework to interact with the RADIUS server to provide authentication and accounting. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters, such as session timeout and the maximum number of clients allowed per interface.

NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCPv6 relay agents.

The DHCPv6 relay agent is compatible with the extended DHCP local server and the extended DHCP relay agent, and can be enabled on the same interface as either the extended DHCP local server or DHCP relay agent.

To configure the DHCPv6 relay agent on the router (or switch), you include the `dhcpv6` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.

You can also include the `dhcpv6` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name forwarding-options dhcp-relay]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay]`

Related Documentation

- Using External AAA Authentication Services with DHCP on page 1256
- Grouping Interfaces with Common DHCP Configurations on page 1258
- Group-Specific DHCP Relay Options on page 1221
- Overriding the Default DHCP Relay Configuration Settings on page 1285
- Configuring Passwords for Usernames on page 1276
- Creating Unique Usernames for DHCP Clients on page 1276
- Verifying and Managing DHCPv6 Local Server Configuration on page 1532
- Example: Extended DHCPv6 Local Server Configuration
DHCP Duplicate Client Differentiation Using Client Subinterface Overview

In some network environments, client IDs and MAC addresses might not be unique, resulting in duplicate clients. For example, two network adapters might be manufactured with the same hardware address, resulting in a duplicate MAC address among the DHCP clients attached to the router (or switch). A duplicate DHCP client occurs when a client attempts to get a lease, and that client has the same client ID or the same MAC address as an existing DHCP client.

When DHCP server receives a request from a new client that has a duplicate ID or MAC address, DHCP server terminates the address lease for the existing client and returns the address to its original address pool. DHCP server then assigns a new address and lease to the new client.

By default, both DHCP local server and DHCP relay use the subnet information to differentiate between duplicate clients. However, in some cases, this level of differentiation is not adequate. For example, when multiple subinterfaces share the same underlying loopback interface with the same preferred source address, the interfaces appear to be on the same subnet. In this situation, the default configuration prevents duplicate clients.

You can provide greater differentiation between duplicate clients by configuring DHCP to consider the client subinterface when duplicate clients occur. In this optional configuration, DHCP uniquely identifies:

- The subnet on which the client resides
- The subinterface on which the client resides
- The client within the subnet

Related Documentation

- Configuring DHCP Duplicate Client Support on page 1258
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 1257

Group-Specific DHCP Relay Options

You can include the following statements at the [edit forwarding-options dhcp-relay group group-name] hierarchy level to set group-specific DHCP relay agent configuration options. Group-specific statements apply only to the named group of interfaces, and override any global DHCP relay agent settings for the same statement.

Include the statements at the [edit forwarding-options dhcp-relay dhcpv6 group group-name] hierarchy level to configure group-specific options for DHCPv6 relay agent.

- active-server-group—Configure an active server group to apply a common DHCP relay agent configuration to a named group of DHCP server addresses. For information, see “Configuring Active Server Groups” on page 1307.
- authentication—Configure the parameters the router (or switch) sends to the external AAA server.
- dynamic-profile—Specify the dynamic profile that is attached to a group of interfaces.
interface—Specify one or more interfaces, or a range of interfaces, that are within the specified group.

liveness-detection—Configure bidirectional failure detection timers and authentication criteria for static routes. For more information, see “DHCP Liveness Detection Overview” on page 1309.

overrides—Override the default configuration settings for the extended DHCP relay agent. For information, see “Overriding the Default DHCP Relay Configuration Settings” on page 1285.

relay-agent-interface-id—(DHCPv6 only) Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.

relay-option—Configure selective processing, which uses DHCP options in client packets to identify and filter client traffic, and to specify the action DHCP relay agent takes with the traffic. For more information, see Using DHCP Option Information to Selectively Process DHCP Client Traffic.

relay-option-82—(DHCPv4 only) Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see “Enabling and Disabling Insertion of Option 82 Information” on page 1303.

service-profile—Specify the default subscriber service, (or default profile) which is activated when the subscriber (or DHCP client) logs in and no other service is activated by a RADIUS server or a provisioning server. For more information, see Default Subscriber Service Overview.

Related Documentation

Grouping Interfaces with Common DHCP Configurations on page 1258

DHCP Snooping Support

DHCP snooping provides DHCP security on the router or switch by filtering incoming messages. When DHCP snooping is enabled, the router differentiates between trusted and untrusted interfaces, and forwards messages from trusted sources while rejecting the untrusted messages.

In Junos OS, DHCP snooping is enabled in a routing instance when you configure either the dhcp-relay statement at the [edit forwarding-options] hierarchy level, or the dhcp-local-server statement at the [edit system services] hierarchy level in that routing instance. However, depending on the Junos OS release, the router processes the snooped packets differently, as described in the following list:

- In Junos OS Release 10.0 and earlier, the router processes snooped packets normally.
- In Junos OS Release 10.1 and later, the router discards snooped packets by default. To enable normal processing of snooped packets in Junos OS Release 10.1 and later, you must explicitly configure the allow-snooped-clients statement at the [edit forwarding-options dhcp-relay] hierarchy level.
You can configure DHCP snooping support for the following:

- **DHCPv4 relay agent**—Override the router’s (or switch’s) default snooping configuration and specify that DHCP snooping is enabled or disabled globally, for a named group of interfaces, or for a specific interface within a named group.

  In a separate procedure, you can set a global configuration to specify whether the DHCPv4 relay agent forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces. The router also uses the global DHCP relay agent snooping configuration to determine whether to forward or drop snooped BOOTREPLY packets.

- **DHCPv6 relay agent**—As you can with snooping support for the DHCPv4 relay agent, you can override the default DHCPv6 relay agent snooping configuration on the router to explicitly enable or disable snooping support globally, for a named group of interfaces, or for a specific interface with a named group of interfaces.

  In multi-relay topologies where more than one DHCPv6 relay agent is between the DHCPv6 client and the DHCPv6 server, snooping enables intervening DHCPv6 relay agents between the client and the server to correctly receive and process the unicast traffic from the client and forward it to the server. The DHCPv6 relay agent snoops incoming unicast DHCPv6 packets by setting up a filter with UDP port 547 (the DHCPv6 UDP server port) on a per-forwarding table basis. The DHCPv6 relay agent then processes the packets intercepted by the filter and forwards the packets to the DHCPv6 server.

  Unlike the DHCPv4 relay agent, the DHCPv6 relay agent does not support global configuration of forwarding support for DHCPv6 snooped packets.

- **DHCP local server**—Configure whether DHCP local server forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces.

### Related Documentation

- Configuring DHCP Snooping for DHCP Relay Agent on page 1293
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 1274
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 1239

### DHCP Auto Logout Overview

This topic provides an introduction to the optional DHCP auto logout feature and includes the following sections:

- Auto Logout Overview on page 1223
- How DHCP Identifies and Releases Clients on page 1224
- Option 60 and Option 82 Requirements on page 1225

### Auto Logout Overview

Auto logout is an optional configuration for DHCP local server and DHCP relay agent that improves the efficiency of DHCP IP address assignment. Auto logout enables IP addresses to be immediately released and returned to the address pool when the addresses are no
longer used by DHCP clients. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example (on the routers), you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address—the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. The secondary identification method is based on the DHCP option 60 and option 82 information in DHCP discover messages.

Both the primary and secondary identification methods use subnet information to differentiate between clients. The primary identification method differentiates between two clients with the same MAC address (or same Client Identifier) if the clients are on different subnets. Similarly, the secondary identification method considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the discover packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

If the DHCP relay receives a DISCOVER message from an existing client, the DHCP relay forwards the DISCOVER message to the DHCP server. The DHCP relay preserves the binding if the client’s existing IP address is returned by the DHCP server. This
behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.

NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in “DHCP Relay Agent Option 82 Value for Auto Logout” on page 1292.

Related Documentation
- Automatically Logging Out DHCP Clients on page 1264
- DHCP Relay Agent Option 82 Value for Auto Logout on page 1292
- Clearing DHCP Bindings for Subscriber Access

Public Key Cryptography Overview

- Understanding Public Key Cryptography on Switches on page 1226
Understanding Public Key Cryptography on Switches

Cryptography describes the techniques related to the following aspects of information security:

- Privacy or confidentiality
- Integrity of data
- Authentication
- Nonrepudiation or nonrepudiation of origin—Nonrepudiation of origin means that signers cannot claim that they did not sign a message while claiming that their private key remains secret. In some nonrepudiation schemes used in digital signatures, a timestamp is attached to the digital signature, so that even if the private key is exposed, the signature remains valid. Public and private keys are described in the following text.

In practice, cryptographic methods protect the data transferred from one system to another over public networks by encrypting the data using an encryption key. Public key cryptography (PKC), which is used on Juniper Networks EX Series Ethernet Switches, uses a pair of encryption keys: a public key and a private key. The public and private keys are created simultaneously using the same encryption algorithm. The private key is held by a user secretly and the public key is published. Data encrypted with a public key can be decrypted only with the corresponding private key and vice versa. When you generate a public/private key pair, the switch automatically saves the key pair in a file in the certificate store, from which it is subsequently used in certificate request commands. The generated key pair is saved as `certificate-id.priv`.

**NOTE:** The default RSA and DSA key size is 1024 bits. If you are using the Simple Certificate Enrollment Protocol (SCEP), Juniper Networks Junos operating system (Junos OS) supports RSA only.

This topic describes:

- Public Key Infrastructure (PKI) and Digital Certificates on page 1226

**Public Key Infrastructure (PKI) and Digital Certificates**

Public key infrastructure (PKI) allows the distribution and use of the public keys in public key cryptography with security and integrity. PKI manages the public keys by using digital certificates. A digital certificate provides an electronic means of verifying the identity of an individual, an organization, or a directory service that can store digital certificates.

A PKI typically consists of a Registration Authority (RA) that verifies the identities of entities, authorizes their certificate requests, and generates unique asymmetric key pairs (unless the users’ certificate requests already contain public keys); and a Certificate Authority (CA) that issues corresponding digital certificates for the requesting entities. Optionally, you can use a Certificate Repository that stores and distributes certificates and a certificate revocation list (CRL) identifying the certificates that are no longer valid.
Each entity possessing the authentic public key of a CA can verify the certificates issued by that CA.

Digital signatures exploit the public key cryptographic system as follows:

1. A sender digitally signs data by applying a cryptographic operation, involving its private key, on a digest of the data.
2. The resulting signature is attached to the data and sent to the receiver.
3. The receiver obtains the digital certificate of the sender, which provides the sender’s public key and confirmation of the link between its identity and the public key. The sender’s certificate is often attached to the signed data.
4. The receiver either trusts this certificate or attempts to verify it. The receiver verifies the signature on the data by using the public key contained in the certificate. This verification ensures the authenticity and integrity of the received data.

As an alternative to using a PKI, an entity can distribute its public key directly to all potential signature verifiers, so long as the key’s integrity is protected. The switch does it by using a self-signed certificate as a container for the public key and the corresponding entity’s identity.

**Related Documentation**
- Understanding Self-Signed Certificates on EX Series Switches on page 1227

**Self-Signed Certificates Overview**

- Understanding Self-Signed Certificates on EX Series Switches on page 1227

**Understanding Self-Signed Certificates on EX Series Switches**

When you initialize a Juniper Networks EX Series Ethernet Switch with the factory default configuration, the switch generates a self-signed certificate, allowing secure access to the switch through the Secure Sockets Layer (SSL) protocol. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) and XML Network Management over Secure Sockets Layer (XNM-SSL) are the two services that can make use of the self-signed certificates.

**NOTE:** Self-signed certificates do not provide additional security as do those generated by Certificate Authorities (CAs). This is because a client cannot verify that the server he or she has connected to is the one advertised in the certificate.

The switches provide two methods for generating a self-signed certificate:

- **Automatic generation**

  In this case, the creator of the certificate is the switch. An automatically generated (also called “system-generated”) self-signed certificate is configured on the switch by default.
After the switch is initialized, it checks for the presence of an automatically generated self-signed certificate. If it does not find one, the switch generates one and saves it in the file system.

A self-signed certificate that is automatically generated by the switch is similar to an SSH host key. It is stored in the file system, not as part of the configuration. It persists when the switch is rebooted, and it is preserved when a request system snapshot command is issued.

The switch uses the following distinguished name for the automatically generated certificate:

“CN=<device serial number>, CN=system generated, CN=self-signed”

If you delete the system-generated self-signed certificate on the switch, the switch generates a self-signed certificate automatically.

- Manual generation

In this case, you create the self-signed certificate for the switch. At any time, you can use the CLI to generate a self-signed certificate. Manually generated self-signed certificates are stored in the file system, not as part of the configuration.

Self-signed certificates are valid for five years from the time they are generated. When the validity of an automatically generated self-signed certificate expires, you can delete it from the switch so that the switch generates a new self-signed certificate.

System-generated self-signed certificates and manually generated self-signed certificates can coexist on the switch.

### Related Documentation

- Understanding Public Key Cryptography on Switches on page 1226
- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 1254
CHAPTER 26

Configuration

- DHCP Local Server Examples on page 1229
- DHCP Relay Agent Examples on page 1234
- Configuration Tasks on page 1240
- Configuration Tasks for DHCP Local Server on page 1255
- Configuration Tasks for DHCP Relay Agent on page 1280
- DHCP Local Server Configuration Statements on page 1313
- DHCP Relay Agent Configuration Statements on page 1386
- Other Configuration Statements on page 1474

DHCP Local Server Examples

- Example: Minimum Extended DHCP Local Server Configuration on page 1229
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 1230
- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231

Example: Minimum Extended DHCP Local Server Configuration

This example shows the minimum configuration you need to use for the extended DHCP local server on the router or switch:

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
    }
}
```

NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.
This example creates the server group named `group_one`, and specifies that the DHCP local server is enabled on interface `fe-0/0/2.0` within the group. The DHCP local server uses the default pool match configuration of `ip-address-first`.

**Related Documentation**

- Extended DHCP Local Server Overview on page 1192

**Example: Extended DHCP Local Server Configuration with Optional Pool Matching**

This example shows an extended DHCP local server configuration that includes optional IPv4 address-assignment pool matching and interface groups. For pool matching, this configuration specifies that the DHCP local server first check the response from an external authentication authority (for example, RADIUS) and use the Framed-IPv6-Pool attribute to determine the address-assignment pool to use for the client address. If no external authority match is found, the DHCP local server then uses ip-address-first matching together with the option 82 information to match the named address range for client IPv4 address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
        interface fe-0/0/2.1;
    }
    group group_two {
        interface fe-0/0/3.0;
        interface fe-0/0/3.1;
    }
    pool-match-order {
        external-authority
        ip-address-first;
        option-82;
    }
}
```

**NOTE:** The interface type in this topic is just an example. The fe-interface type is not supported by EX Series switches.

**Related Documentation**

- Extended DHCP Local Server Overview on page 1192
- Address-Assignment Pools Overview on page 1206
Example: Configuring Group Liveness Detection for DHCP Local Server Clients

This example shows how to configure group liveness detection for DHCP local server subscribers or DHCP clients using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

- Requirements on page 1231
- Overview on page 1231
- Configuration on page 1231

Requirements

- Juniper Networks MX Series routers
- Juniper Networks EX Series switches
- Junos OS Release 12.1R1 or later
- Junos OS Release 12.3R2 or later for EX Series switches
- Configure DHCP local server. See “Extended DHCP Local Server Overview” on page 1192.

Overview

In this example, you configure group liveness detection for DHCP local server subscribers (clients) by completing the following operations:

1. Enable liveness detection for DHCP local server subscriber (or DHCP client) groups.
2. Specify BFD as the liveness detection method for all dynamically created DHCP local server subscribers (clients).
3. Configure BFD-specific statements to define how the protocol behaves.
4. Configure the action the router (switch) takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the liveness-detection statement, and any subsequent configuration statements, at the [edit system services dhcp-local-server dhcpv6] or [edit system services dhcp-local-server dhcpv6 group group-name] hierarchy level.

Configuration

Step-by-Step Procedure

To configure group liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.

```plaintext
[edit system services dhcp-local-server ]
user@host# edit liveness-detection
```
2. Specify that you want to configure liveness detection for a specific DHCP local server group.

   ```
   [edit system services dhcp-local-server liveness-detection]
   user@host# edit group local_group_1
   ```

3. Specify that you want to configure the liveness detection method.

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection]
   user@host# edit method
   ```

4. Specify BFD as the liveness detection method that you want DHCP to use.

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method]
   user@host# edit bfd
   ```

5. Configure the detection time threshold (in milliseconds) at which a trap is produced.

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set detection-time threshold 30000
   ```

6. Configure the time (in milliseconds) for which BFD holds a session up notification.

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set holddown-interval 50
   ```

7. Configure the BFD minimum transmit and receive interval (in milliseconds).

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set minimum-interval 45000
   ```

8. Configure the minimum receive interval (in milliseconds).

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set minimum-receive-interval 60000
   ```

9. Configure a multiplier value for the detection time.

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set multiplier 100
   ```

10. Disable the ability for BFD interval timers to change or adapt to network situations.

   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set enable false
   ```
11. Configure the BFD session mode.
   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set no-adaptation
   ```

12. Configure the threshold and minimum interval for the BFD transmit interval.
   ```
   [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
   user@host# set session-mode automatic
   ```
   
   **NOTE:** You do not need to configure the transmit interval values if you have already configured the minimum transmit and receive interval for BFD.

13. Configure the BFD protocol version you want to detect.
    ```
    [edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
    user@host# set version automatic
    ```

14. Configure the action the router (switch) takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.
    ```
    [edit system services dhcp-local-server group local_group_1 liveness-detection]
    user@host# edit failure-action action
    ```

**Results**

From configuration mode, confirm your configuration by entering the `show system` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it.

```
[edit]
regress@montag# show system
services {
    dhcp-local-server {
        group local_group_1 {
            liveness-detection {
                failure-action clear-binding-if-interface-up;
                method {
                    bfd {
                        version automatic;
                        minimum-interval 45000;
                        minimum-receive-interval 60000;
                        multiplier 100;
                        no-adaptation;
                        transmit-interval {
                            minimum-interval 45000;
                            threshold 60000;
                        }
                    }
                }
            }
        }
    }
}
```
If you are done configuring the device, enter `commit` from configuration mode.

**Related Documentation**
- Extended DHCP Local Server Overview on page 1192
- DHCP Liveness Detection Overview on page 1309
- Configuring Detection of DHCP Local Server Client Connectivity on page 1273

**DHCP Relay Agent Examples**

- Example: Minimum DHCP Relay Agent Configuration on page 1234
- Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 1235
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 1239

**Example: Minimum DHCP Relay Agent Configuration**

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```plaintext
[edit forwarding-options]
dhcp-relay {
  server-group {
    test 10.0.2.1;
  }
  active-server-group test;
  group all {
    interface fe-0/0/2.0;
  }
}
```

**NOTE:** The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

This example creates a server group and an active server group named `test` with IP address 10.0.2.1. The DHCP relay agent configuration is applied to a group named `all`. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.
Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings

This example shows how to configure DHCP relay agent to use DHCP option strings to selectively identify, filter, and process client traffic.

- Requirements on page 1235
- Overview on page 1235
- Configuration on page 1236
- Verification on page 1237

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers or EX Series Switches
- Junos OS Release 12.3 or later or Junos OS Release 12.3R2 for EX Series switches

Before you configure DHCP relay agent selective processing support, be sure you:

- Configure DHCP relay agent.
  See “Extended DHCP Relay Agent Overview” on page 1215.
- (Optional) Configure a named DHCP local server group if you want to forward client traffic to a server group.
  See “Grouping Interfaces with Common DHCP Configurations” on page 1258.

Overview

In this example, you configure DHCP relay agent to use DHCP option strings in client packets to selectively identify, filter, and process client traffic. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCP option that DHCP relay agent uses to identify the client traffic you want to process. The option you specify matches the option in the client traffic.
2. Configure a default action—Specify the default processing action, which DHCP relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filter the client traffic. The criteria can be an exact match or a partial match with the option string in the client traffic. Associate a processing action with each match criterion.
Configuration

To configure DHCP relay agent selective processing based on DHCP option information, perform these tasks:

- Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings on page 1236
- Results on page 1237

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the [edit] hierarchy level.

```
set forwarding-options dhcp-relay relay-option option-number 60
set forwarding-options dhcp-relay relay-option equals ascii video-gold forward-only
set forwarding-options dhcp-relay relay-option equals ascii video-bronze local-server-group servergroup-15
set forwarding-options dhcp-relay relay-option starts-with-hexadecimal ffffff
local-server-group servergroup-east
set forwarding-options dhcp-relay relay-option default-action drop
```

Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings

Step-by-Step Procedure

To configure DHCP relay selective processing:

1. Specify that you want to configure DHCP relay agent support.

   ```
   [edit forwarding-options]
   user@host# edit dhcp-relay
   ```

2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# set relay-option option-number 60
   ```

3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# set relay-option default-action drop
   ```

4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# set relay-option equals ascii video-gold forward-only
   ```

5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# set relay-option equals ascii video-bronze local-server-group servergroup-15
   ```
6. Configure a partial match criteria and associated action that DHCP relay uses to process client traffic.

   [edit forwarding-options dhcp-relay]
   user@host# set relay-option starts-with hexadecimal ffffff local-server-group servergroup-east

**Results**

From configuration mode, confirm the results of your configuration by issuing the `show` statement at the `[edit forwarding-options]` hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

   [edit forwarding-options]
   user@host# show
   dhcp-relay {
     relay-option {
       option-number 60;
       equals {
         asciivideo-gold {
           forward-only;
         }
       }
       equals {
         asciivideo-bronze {
           local-server-group servergroup-15;
         }
       }
       default-action {
         drop;
       }
       starts-with {
         hexadecimal ffffff {
           local-server-group servergroup-east;
         }
       }
     }
   }

If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

To verify the status of DHCP relay agent selective traffic processing, perform this task:

- Verifying the Status of DHCP Relay Agent Selective Traffic Processing on page 1237

**Verifying the Status of DHCP Relay Agent Selective Traffic Processing**

**Purpose** Verify the DHCP relay agent selective traffic processing status.
**Action**  Display statistics for DHCP relay agent.

```bash
user@host> show dhcp relay statistics
Packets dropped:
  Total                      30
  Bad hardware address       1
  Bad opcode                 1
  Bad options                3
  Invalid server address     5
  No available addresses     1
  No interface match         2
  No routing instance match  9
  No valid local address     4
  Packet too short           2
  Read error                 1
  Send error                 1
  Option 60                  1
  Option 82                  2

Messages received:
  BOOTREQUEST         116
  DHCPDECLINE         0
  DHCPDISCOVER        11
  DHCPINFORM          0
  DHCPRELEASE         0
  DHCPREQUEST         105

Messages sent:
  BOOTREPLY            0
  DHCPOFFER            2
  DHCPACK              1
  DHCPNAK              0
  DHCPFORCERENEW      0

Packets forwarded:
  Total                      4
  BOOTREQUEST                2
  BOOTREPLY                  2
```

**Meaning**  The `Packets forwarded` field in the `show dhcp relay statistics` command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCP relay agent has forwarded, as well as a breakdown for the number of `BOOTREQUEST` and `BOOTREPLY` packets forwarded.

**Related Documentation**
- Extended DHCP Relay Agent Overview on page 1215
- DHCP Options and Selective Traffic Processing Overview
- Using DHCP Option Information to Selectively Process DHCP Client Traffic
- Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings
- Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing
Example: Configuring DHCP Snooping Support for DHCP Relay Agent

This example shows how to configure DHCP snooping support for DHCP relay agent.

• Requirements on page 1239
• Overview on page 1239
• Configuration on page 1239

Requirements

• Configure DHCP relay agent. See “Extended DHCP Relay Agent Overview” on page 1215.

Overview

In this example, you configure DHCP snooping support for DHCP relay agent by completing the following operations:

• Override the default DHCP snooping configuration and enable DHCP snooping support for the interfaces in group frankfurt.
• Configure DHCP relay agent to forward snooped packets to only configured interfaces.

NOTE: By default, DHCP snooping is enabled globally in Junos OS Release 10.0 and earlier and disabled globally in Junos OS Release 10.1 and later.

Configuration

Step-by-Step Procedure

To configure DHCP relay support for DHCP snooping:

1. Specify that you want to configure DHCP relay agent.
   
   [edit]
   user@host# edit forwarding-options dhcp-relay

2. Specify the named group of interfaces on which DHCP snooping is supported.
   
   [edit forwarding-options dhcp-relay]
   user@host# edit group frankfurt

3. Specify the interfaces that you want to include in the group. DHCP relay agent considers these as the configured interfaces when determining whether to forward or drop traffic.
   
   [edit forwarding-options dhcp-relay group frankfurt]
   user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9

4. Specify that you want to override the default configuration for the group.
   
   [edit forwarding-options dhcp-relay group frankfurt]
   user@host# edit overrides

5. Enable DHCP snooping support for the group.
   
   [edit forwarding-options dhcp-relay group frankfurt overrides]
   user@host# set allow-snooped-clients
6. Return to the [edit forwarding-options dhcp-relay] hierarchy level to configure the forwarding action and specify that DHCP relay agent forward snooped packets on only configured interfaces:

   [edit forwarding-options dhcp-relay group frankfurt overrides]
   user@host# up 2

7. Enable DHCP snooped packet forwarding for DHCP relay agent.

   [edit forwarding-options dhcp-relay]
   user@host# edit forward-snooped-clients

8. Specify that snooped packets are forwarded on only configured interfaces (the interfaces in group frankfurt).

   [edit forwarding-options dhcp-relay forward-snooped-clients]
   user@host# set configured-interfaces

Results

From configuration mode, confirm your configuration by entering the show forwarding-options command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

   [edit]
   regress@montag# show forwarding-options
dhcp-relay {
   forward-snooped-clients configured-interfaces;
group frankfurt {
   overrides {
   allow-snooped-clients;
   }
   interface fe-1/0/1.3 {
   upto fe-1/0/1.9;
   }
   }
}

If you are done configuring the device, enter commit from configuration mode.

Related Documentation

- DHCP Snooping Support on page 1203
- Configuring DHCP Snooping for DHCP Relay Agent on page 1293

Configuration Tasks

- Configuring DHCP Services (J-Web Procedure) on page 1241
- Configuring a DHCP SIP Server (CLI Procedure) on page 1248
- Configuring a DHCP Client (CLI Procedure) on page 1249
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 1252
Configuring DHCP Services (J-Web Procedure)

Use the J-Web DHCP Configuration pages to configure DHCP pools for subnets and static bindings for DHCP clients on an ACX Series Universal Access Gateway router or an EX Series Ethernet Switch. If DHCP pools or static bindings are already configured, use the Configure Global DHCP Parameters Configuration page to add settings for these pools and static bindings. Settings that have been previously configured for DHCP pools or static bindings are not overridden when you use the Configure Global DHCP Parameters Configuration page.

To configure the DHCP server:

1. Select Configure > Services > DHCP
2. Access a DHCP Configuration page:
   - To configure a DHCP pool for a subnet, click Add in the DHCP Pools box.
   - To configure a static binding for a DHCP client, click Add in the DHCP Static Binding box.
   - To globally configure settings for existing DHCP pools and static bindings, click Configure Global DHCP Parameters.
3. Enter information into the DHCP Service Configuration pages as described in Table 164 on page 1241
4. To apply the configuration, click Apply.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 164: DHCP Service Configuration Pages Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Pool Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP Subnet (required)</td>
<td>Specifies the subnet on which DHCP is configured.</td>
<td>Type an IP address prefix.</td>
</tr>
</tbody>
</table>
Table 164: DHCP Service Configuration Pages Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Range (Low)</td>
<td>Specifies the lowest address in the IP address pool range.</td>
<td>Type an IP address that is part of the subnet specified in DHCP Subnet field.</td>
</tr>
<tr>
<td>Address Range (High)</td>
<td>Specifies the highest address in the IP address pool range.</td>
<td>Type an IP address that is part of the subnet specified in DHCP Subnet. This address must be greater than the address specified in the Address Range (Low) field.</td>
</tr>
</tbody>
</table>
| Exclude Addresses            | Specifies addresses to exclude from the IP address pool.                 | • To add an excluded address, type the address next to the Add button, and click Add.  
                                                                           | • To delete an excluded address, select the address in the Exclude Addresses box, and click Delete. |
| Lease Time                   |                                                                          |                                                                            |
| Maximum Lease Time (Seconds) | Specifies the maximum length of time a client can hold a lease.          | Type a number from 60 through 4,294,967,295 (seconds). You can also type infinite to specify a lease that never expires. |
| Default Lease Time (Seconds) | Specifies the length of time a client can hold a lease for clients that do not request a specific lease length. | Type a number from 60 through 2,147,483,647 (seconds). You can also type infinite to specify a lease that never expires. |
| Server Information           |                                                                          |                                                                            |
| Server Identifier            | Specifies the IP address of the DHCP server reported to a client.        | Type the IP address of the server. If you do not specify a server identifier, the primary address of the interface on which the DHCP exchange occurs is used. |
| Domain Name                  | Specifies the domain name that clients must use to resolve hostnames.    | Type the name of the domain.                                                |
| Domain Search                | Specifies the order—from top to bottom—in which clients must append domain names when resolving hostnames using DNS. | • To add a domain name, type the name next to the Add button, and click Add.  
                                                                           | • To delete a domain name, select the name in the Domain Search box, and click Delete. |
| DNS Name Servers             | Defines a list of DNS servers that the client can use, in the specified order—from top to bottom. | • To add a DNS server, type an IP address next to the Add button, and click Add.  
                                                                           | • To remove a DNS server, select the IP address in the DNS Name Servers box, and click Delete. |
| Gateway Routers              | Defines a list of relay agents on the subnet, in the specified order—from top to bottom. | • To add a relay agent, type an IP address next to the Add button, and click Add.  
                                                                           | • To remove a relay agent, select the IP address in the Gateway Routers box, and click Delete. |
### Table 164: DHCP Service Configuration Pages Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| WINS Servers                        | Defines a list of NetBIOS name servers, in the specified order—from top to bottom. | • To add a NetBIOS name server, type an IP address next to the **Add** button, and click **Add**.  
  • To remove a NetBIOS name server, select the IP address in the WINS Servers box, and click **Delete**. |
| Boot Options                        |                                                                          | |
| Boot File                           | Specifies the path and filename of the initial boot file to be used by the client. | Type a path and filename.                                                                                                                    |
| Boot Server                         | Specifies the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file. | Type the IP address or hostname of the TFTP server.                                                                                          |
| DHCP Static Binding Information     |                                                                          | |
| DHCP MAC Address (required)         | Specifies the MAC address of the client to be permanently assigned a static IP address. | Type the hexadecimal MAC address of the client.                                                                                               |
| Fixed IP Addresses (required)       | Defines a list of IP addresses permanently assigned to the client. A static binding must have at least one fixed address assigned to it, but multiple addresses are also allowed. | • To add an IP address, type it next to the **Add** button, and click **Add**.  
  • To remove an IP address, select it in the Fixed IP Addresses box, and click **Delete**. |
| Host Name                           | Specifies the name of the client used in DHCP messages exchanged between the server and the client. The name must be unique to the client within the subnet on which the client resides. | Type a client hostname.                                                                                                                      |
| Client Identifier                   | Specifies the name of the client used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides. | Type a client identifier in string form.                                                                                                      |
| Hexadecimal Client Identifier       | Specifies the name of the client, in hexadecimal form, used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides. | Type a client identifier in hexadecimal form.                                                                                               |

**Configuring DHCP Services on EX4300 Switches (J-Web Procedure)**

On EX4300 switches, use the DHCP Configuration page to create DHCP pools and set the DHCP parameters for them and to configure DHCP settings for existing DHCP pools and static bindings.
To configure the DHCP services on EX4300 switches:

1. Select **Configure > Services > DHCP**

2. Access a DHCP Configuration page:
   - To configure a DHCP pool for a subnet, click **Add** in the DHCP Pools box.
   - To configure DHCP groups, click **Add** in the DHCP Groups box.
   - To globally configure settings for existing DHCP pools and static bindings, click **Configure Global DHCP Parameters**.

3. Enter information into the DHCP Service Configuration pages as described in **Table 165 on page 1244**

4. To apply the configuration, click **OK**.

**NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

### Table 165: DHCP Service Configuration Pages Summary for EX4300 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP Gropus</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Name</td>
<td>Specifies the name of the group.</td>
<td>Enter the name of the group.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Family inet interface is listed, only if it is already configured with family inet.</td>
<td>Select the interface for the specific group.</td>
</tr>
<tr>
<td><strong>DHCP Pool Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool Name</td>
<td>Specifies the name of an address-assignment pool.</td>
<td>Type the pool name.</td>
</tr>
<tr>
<td>Link Pool</td>
<td>Specifies the pool name to which it is linked.</td>
<td>Select the option from the list.</td>
</tr>
<tr>
<td><strong>Network Address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies the IP address pool range.</td>
<td>Type an IP address that is part of the subnet specified in the DHCP Subnet field.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Specifies the subnet specified in DHCP Subnet.</td>
<td>Type a subnet mask that is specified in the DHCP Subnet field.</td>
</tr>
<tr>
<td><strong>DHCP Pool Attributes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool Name</td>
<td>Displays the name of an address-assignment pool.</td>
<td>The pool name is displayed.</td>
</tr>
</tbody>
</table>
### Table 165: DHCP Service Configuration Pages Summary for EX4300 Switches *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Identifier</td>
<td>Specifies the IP address of the DHCP server reported to a client.</td>
<td>Type the IP address of the server. If you do not specify a server identifier, the primary address of the interface on which the DHCP exchange occurs is used.</td>
</tr>
<tr>
<td>TFTP Server</td>
<td>Specifies the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file.</td>
<td>Enter the IP address of the TFTP server.</td>
</tr>
<tr>
<td>Maximum Lease Time</td>
<td>Specifies the maximum length of time a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)</td>
<td>Type a number.</td>
</tr>
<tr>
<td>Boot File</td>
<td>Specifies the path and filename of the initial boot file to be used by the client.</td>
<td>Type a path and filename.</td>
</tr>
<tr>
<td>Boot Server</td>
<td>Specifies the TFTP server that provides the initial boot file to the client.</td>
<td>Type the IP address or hostname of the TFTP server.</td>
</tr>
<tr>
<td>Grace Period</td>
<td>Specifies the grace period for which a client can hold a lease.</td>
<td>Type the grace period in seconds.</td>
</tr>
<tr>
<td>DNS Name Servers</td>
<td>Defines a list of DNS servers the client can use.</td>
<td>• To add a DNS server, click <strong>Add</strong>. Type an IP address in the <strong>Add IP Address</strong> pop-up window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click <strong>OK</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To remove a DNS server, select the IP address in the DNS Name Servers box, and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>WINS Servers</td>
<td>Defines a list of NetBIOS name servers.</td>
<td>• To add a NetBIOS name server, click <strong>Add</strong>. Type an IP address in the <strong>Add IP Address</strong> pop-up window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click <strong>OK</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To remove a NetBIOS name server, select the IP address in the WINS Servers box, and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the domain name that clients must use to resolve hostnames.</td>
<td>Type the name of the domain.</td>
</tr>
<tr>
<td>Netbios Node Type</td>
<td>Specifies the NetBIOS node that provides the initial node file to the client.</td>
<td>Select the type from the list.</td>
</tr>
<tr>
<td>Gateway Routers</td>
<td>Defines a list of relay agents on the subnet, in the specified order—from top to bottom.</td>
<td>• To add a relay agent, click <strong>Add</strong>. Type an IP address in the <strong>Add IP Address</strong> pop-up window.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click <strong>OK</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To remove a relay agent, select the IP address in the Gateway Routers box, and click <strong>Remove</strong>.</td>
</tr>
</tbody>
</table>


Table 165: DHCP Service Configuration Pages Summary for EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Specifies the DHCP options.</td>
<td>• To add a DHCP option, click Add. The Add DHCP Option pop-up window is displayed. Enter the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter the DHCP Code in the Code box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select the DHCP type from the Type list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select the DHCP subtype from the Sub Type list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enter the DHCP value in the Value box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To remove a DHCP option, select the option in the Option box, and click Remove.</td>
</tr>
<tr>
<td>Option-82</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Circuit Identifier</td>
<td>Identifies the circuit (interface or VLAN or both) on the switch on which the request was received.</td>
<td>Type the circuit identifier.</td>
</tr>
<tr>
<td>Ranges</td>
<td>Specifies the circuit identifier range.</td>
<td>Type the range for the circuit identifier.</td>
</tr>
<tr>
<td>Remote identifier</td>
<td>By default, the remote ID is the MAC address of the switch</td>
<td>Type the remote identifier.</td>
</tr>
<tr>
<td>Ranges</td>
<td>Specifies the remote identifier range.</td>
<td>Type the range for the remote identifier.</td>
</tr>
<tr>
<td>Address Range</td>
<td>Specifies the network address.</td>
<td></td>
</tr>
<tr>
<td>Range Name</td>
<td>Specifies the name of the range.</td>
<td>Click Add. The Add Address Range pop-up window is displayed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Type the range name in the Range Name box.</td>
</tr>
<tr>
<td>Address Range</td>
<td>Specifies the network address.</td>
<td></td>
</tr>
<tr>
<td>Address Range (Low)</td>
<td>Specifies the lowest address in the IP address pool range.</td>
<td>Type an IP address that is part of the subnet specified in DHCP Subnet</td>
</tr>
<tr>
<td>Address Range (High)</td>
<td>Specifies the highest address in the IP address pool range.</td>
<td>Type an IP address that is part of the subnet specified in DHCP Subnet. This address must be greater than the address specified in Address Range (Low).</td>
</tr>
<tr>
<td>Static Bindings</td>
<td>Specifies the name of the client used in DHCP messages exchanged between the server and the client. The name must be unique to the client within the subnet on which the client resides.</td>
<td>Type a client hostname.</td>
</tr>
</tbody>
</table>
Table 165: DHCP Service Configuration Pages Summary for EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Specifies the MAC address of the client to be permanently assigned a static IP address.</td>
<td>Type the hexadecimal MAC address of the client.</td>
</tr>
<tr>
<td>Fixed IP Address</td>
<td>Specifies the IP address of the client.</td>
<td>Type the IP address.</td>
</tr>
<tr>
<td><strong>Global Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duplicate clients on interface</td>
<td>Specifies the DHCP local server to include the client subinterface when distinguishing between duplicate DHCP clients (clients with the same MAC address or client ID) in the same subnet.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Pool Match Order</td>
<td>Specifies the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client.</td>
<td>Select the pool match order.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password that is sent to the external AAA authentication server for subscriber authentication.</td>
<td>Type the password.</td>
</tr>
<tr>
<td><strong>Username-include</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Circuit Type</td>
<td>Specifies the circuit type that is linked with the username.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Name of the interface.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>Specifies the MAC address of the client PDU that is linked with the username during the subscriber authentication process.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Logical System Name</td>
<td>Specifies that the logical system name that is linked with the username during the subscriber authentication process.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Option-60</td>
<td>Specifies the payload of Option 60 (Vendor Class Identifier) from the client PDU be linked with the username during the subscriber authentication process.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Routing Instance Name</td>
<td>Specifies the routing instance name that is linked with the username during the subscriber authentication process.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Option-82</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 165: DHCP Service Configuration Pages Summary for EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit Identifier</td>
<td>Specifies the name of the client used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Remote Identifier</td>
<td>Specifies the remote ID option in the client.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the domain name that clients must use to resolve hostnames.</td>
<td>Type the domain name.</td>
</tr>
<tr>
<td>User Prefix</td>
<td>Specifies the prefix to the username as defined by the user.</td>
<td>Type the prefix.</td>
</tr>
<tr>
<td>Delimiter</td>
<td>Specifies a character that separates components that make up the username.</td>
<td>Type the delimiter.</td>
</tr>
</tbody>
</table>

Configuring a DHCP SIP Server (CLI Procedure)

You can use the `sip-server` statement on the EX Series switch to configure option 120 on a DHCP server. The DHCP server sends configured option values—Session Initiation Protocol (SIP) server addresses or names—to DHCP clients when they request them. Previously, you were only allowed to specify a SIP server by address using `[edit system services dhcp option 120]`. You specify either an IPv4 address or a fully qualified domain name to be used by SIP clients to locate a SIP server. You cannot specify both an address and name in the same statement.

To configure a SIP server using the `address` option:

```
[edit system services dhcp]
user@switch# set sip-server address
```

For example, to configure one address:

```
[edit system services dhcp]
user@switch set sip-server 172.168.0.11
```

To configure a SIP server using the `name` option:

```
[edit system services dhcp]
user@switch# set sip-server name
```

For example, to configure a name:

```
[edit system services dhcp]
user@switch set sip-server abc.example.com
```
Configuring a DHCP Client (CLI Procedure)

A Dynamic Host Configuration Protocol (DHCP) server can provide many valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients, and it can also deliver software upgrades to clients.

DHCP configuration consists of two components, configuration of DHCP clients and configuration of a DHCP server. Client configuration determines how clients send a message requesting an IP address, whereas a DHCP server configuration enables the server to send an IP address configuration back to the client. This topic describes configuring a DHCP client. For directions for configuring a DHCP server, see “Configuring a DHCP Server on Switches (CLI Procedure)” on page 1250.

You can change DHCP client configurations from the switch, using client identifiers to indicate which clients you want to configure.

To configure a DHCP client, you configure an interface to belong to the DHCP family and specify additional attributes, as desired:

```
[edit]
user@switch# set interfaces interface-name unit number family inet dhcp configuration-statement
```

The options that you can configure are listed in Table 166 on page 1249. Replace the variable `configuration-statement` with one or more of the statements listed in this table. If you do not explicitly configure these options, the switch uses default values for them.

<table>
<thead>
<tr>
<th>Configuration Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-identifier</td>
<td>Unique client ID—By default this consists of the hardware type (01 for Ethernet) and the MAC address (a.b.c.d). For this example, the value would be 01abcd.</td>
</tr>
<tr>
<td>lease-time</td>
<td>Time in seconds that a client holds the lease for an IP address assigned by a DHCP server. If a client does not request a specific lease time, then the server sends the default lease time. The default lease time on a Junos OS DHCP server is 1 day.</td>
</tr>
<tr>
<td>retransmission-attempt</td>
<td>Number of times the client attempts to retransmit a DHCP packet.</td>
</tr>
<tr>
<td>retransmission-interval</td>
<td>Time between transmission attempts.</td>
</tr>
<tr>
<td>server-address</td>
<td>IP address of the server that the client queries for an IP address.</td>
</tr>
<tr>
<td>update-server</td>
<td>TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch are propagated.</td>
</tr>
<tr>
<td>vendor-option</td>
<td>Vendor class ID (CPU’s manufacturer ID string) for the DHCP client.</td>
</tr>
</tbody>
</table>
Configuring a DHCP Server on Switches (CLI Procedure)

A Dynamic Host Configuration Protocol (DHCP) server can provide two valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients and it can also deliver software upgrades to clients.

DHCP configuration consists of two components, optional reconfiguration of default settings on DHCP clients and configuration of a DHCP server. This topic covers configuration of the DHCP server. For directions for reconfiguring a DHCP client, see “Configuring a DHCP Client (CLI Procedure)” on page 1249.

You can configure either of two versions of a DHCP server on a switch—either the extended server version or the legacy server version. We recommend that you use the extended server configuration unless you need to keep your DHCP server configuration backward-compatible with the legacy server version.

This topic includes the following tasks:

1. Configuring an Extended DHCP Server on a Switch on page 1250
2. Configuring a Legacy DHCP Server on a Switch (CLI Procedure) on page 1251

Configuring an Extended DHCP Server on a Switch

To configure an extended DHCP server, you must configure a DHCP pool, indicate IP addresses for the pool, and create a server group. Additional configurations are optional.

Do not assign addresses that are already in use in the network to address pools. The extended DHCP server does not check whether addresses are already in use before assigning them to clients.

1. Create an address pool for DHCP IP addresses:
   
   [edit]
   user@switch# set access address-pool address-pool

2. Configure addresses for DHCP dynamic assignment:
   
   [edit access address-assignment]
   user@switch# set pool address-pool-name

3. Create a server group on the switch, providing a group name and an interface for DHCP:
   
   [edit system services dhcp-local-server]
   user@switch# set group group-name interface interface-name

4. Optionally, process the information protocol data units (PDUs):
   
   [edit system services dhcp-local-server]
   user@switch# set overrides process-inform

5. Optionally, redefine the order of attribute matching for pool selection:
[edit system services dhcp-local-server]
user@switch# set pool-match-order ip-address-first

6. Optionally, enable dynamic reconfiguration triggered by the DHCP extended server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces:

[edit system services dhcp-local-server]
user@switch# set reconfigure

[edit system services dhcp-local-server group group-name]
user@switch# set reconfigure

Configuring a Legacy DHCP Server on a Switch (CLI Procedure)

To configure a legacy DHCP server, you must configure a pool of IP addresses for dynamic assignment. You only need to supply a series of network addresses. Additional configurations are optional.

1. Configure a pool of IP addresses for dynamic assignment:

[edit system services dhcp]
user@switch# set pool (Legacy DHCP) network-range

NOTE: Step 2 through step 15 assign global values at the [edit system services dhcp] hierarchy level. You can also assign the same values to a specific pool using those same commands at the [edit system services dhcp pool network-range] hierarchy level.

2. Optionally, change the domain search list used to resolve hostnames:

[edit system services dhcp]
user@switch# set domain-search [domain-list]

3. Optionally, change the domain name server (DNS) name that the DHCP server advertises to clients:

[edit system services dhcp]
user@switch# set name-server address

4. Optionally, change the DHCP options:

[edit system services dhcp]
user@switch# set option id-number

5. Optionally, change the devices advertised to clients:

[edit system services dhcp]
user@switch# set router address

6. Optionally, change the SIP server:

[edit system services dhcp]
user@switch# set sip-server addresses-or-names

For more information, see "Configuring a DHCP SIP Server (CLI Procedure)" on page 1248.

7. Optionally, change the DHCP client’s hardware address:
You can configure an EX Series switch to act as an extended DHCP relay agent. This means that a locally attached host can issue a DHCP request as a broadcast message and the switch configured for DHCP relay relays the message to a specified DHCP server. Configure a switch to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

Before you begin:

- Ensure that the switch can connect to the DHCP server.

To configure a switch to act as an extended DHCP relay agent server:

1. Create at least one DHCP server group, which is a group of 1 through 5 DHCP server IP addresses:

   ```
   [edit forwarding-options dhcp-relay]
   user@switch# set server-group server-group-name ip-address
   ```

2. Set the global active DHCP server group. The DHCP relay server relays DHCP client requests to the DHCP servers defined in the active server group:

   ```
   [edit forwarding-options dhcp-relay]
   user@switch# set active-server-group server-group-name
   ```

3. Create a DHCP relay group that includes at least one interface. DHCP relay runs on the interfaces defined in DHCP groups:

   ```
   [edit forwarding-options dhcp-relay]
   user@switch# set group group-name interface interface-name
   ```

4. (Optional) Configure overrides of default DHCP relay behaviors, at the global level. See the override options in the `overrides` statement.

   ```
   [edit forwarding-options dhcp-relay]
   user@switch# set overrides
   ```

5. (Optional) Configure DHCP relay to use the DHCP vendor class identifier option (option 60) in DHCP client packets, at the global level:

   ```
   [edit forwarding-options dhcp-relay]
   user@switch# set relay-option option-number 60
   ```

Related Documentation

- Configuring a DHCP Client (CLI Procedure) on page 1249
- Configuring a DHCP SIP Server (CLI Procedure) on page 1248
- Understanding DHCP Services for Switches
6. (Optional) Configure settings for a DHCP relay group that override the settings at the global level, using these statements:

   [edit forwarding-options dhcp-relaygroup group-name]
   user@switch# set active-server-group server-group-name
   user@switch# set overrides
   user@switch# set relay-option option-number 60

7. (Optional) Configure settings for a DHCP relay group interface that override the settings at the global and group levels, using these statements:

   [edit forwarding-options dhcp-relaygroup group-name interface interface-name]
   user@switch# exclude
   user@switch# set overrides
   user@switch# set trace
   user@switch# set upto upto-interface-name

Related Documentation
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
- Configuring a DHCP Client (CLI Procedure) on page 1249
- Understanding the Extended DHCP Relay Agent for EX Series Switches

Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)

You can use the system-generated self-signed certificate or a manually generated self-signed certificate to enable Web management HTTPS and XNM-SSL services.

- To enable HTTPS services using the automatically generated self-signed certificate:
  
  [edit]
  user@switch# set system services web-management https system-generated-certificate

- To enable HTTPS services using a manually generated self-signed certificate:
  
  [edit]
  user@switch# set system services web-management https pki-local-certificate certificate-id-name

  **NOTE:** The value of the `certificate-id-name` must match the name you specified when you generated the self-signed certificate manually.

- To enable XNM-SSL services using a manually generated self-signed certificate:
  
  [edit]
  user@switch# set system services xnm-ssl local-certificate certificate-id-name

  **NOTE:** The value of the `certificate-id-name` must match the name you specified when you generated the self-signed certificate manually.

Related Documentation
- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 1254
- Understanding Self-Signed Certificates on EX Series Switches on page 1227
Manually Generating Self-Signed Certificates on Switches (CLI Procedure)

EX Series switches allow you to generate custom self-signed certificates and store them in the file system. The certificate you generate manually can coexist with the automatically generated self-signed certificate on the switch. To enable secure access to the switch over SSL, you can use either the system-generated self-signed certificate or a certificate you have generated manually.

To generate self-signed certificates manually, you must complete the following tasks:

- Generating a Public-Private Key Pair on Switches on page 1254
- Generating Self-Signed Certificates on Switches on page 1254

Generating a Public-Private Key Pair on Switches

A digital certificate has an associated cryptographic key pair that is used to sign the certificate digitally. The cryptographic key pair comprises a public key and a private key. When you generate a self-signed certificate, you must provide a public-private key pair that can be used to sign the self-signed certificate. Therefore, you must generate a public-private key pair before you can generate a self-signed certificate.

To generate a public-private key pair:

```
user@switch> request security pki generate-key-pair certificate-id certificate-id-name
```

**NOTE:** Optionally, you can specify the encryption algorithm and the size of the encryption key. If you do not specify the encryption algorithm and encryption key size, default values are used. The default encryption algorithm is RSA, and the default encryption key size is 1024 bits.

After the public-private key pair is generated, the switch displays the following:

```
generated key pair certificate-id-name, key size 1024 bits
```

Generating Self-Signed Certificates on Switches

To generate the self-signed certificate manually, include the certificate ID name, the subject of the distinguished name (DN), the domain name, the IP address of the switch, and the e-mail address of the certificate holder:

```
user@switch> request security pki local-certificate generate-self-signed certificate-id certificate-id-name domain-name domain-name email email-address ip-address switch-ip-address subject subject-of-distinguished-name
```

The certificate you have generated is stored in the switch’s file system. The certificate ID you have specified while generating the certificate is a unique identifier that you can use to enable the HTTPS or XNM-SSL services.

To verify that the certificate was generated and loaded properly, enter the `show security pki local-certificate` operational command.

Related Documentation

- Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure) on page 1253
Deleting Self-Signed Certificates (CLI Procedure)

You can delete a self-signed certificate that is automatically or manually generated from the EX Series switch. When you delete the automatically generated self-signed certificate, the switch generates a new self-signed certificate and stores it in the file system.

- To delete the automatically generated certificate and its associated key pair from the switch:
  
  ```
  user@switch> clear security pki local-certificate system-generated
  ```

- To delete a manually generated certificate and its associated key pair from the switch:
  
  ```
  user@switch> clear security pki local-certificate certificate-id certificate-id-name
  ```

- To delete all manually generated certificates and their associated key pairs from the switch:
  
  ```
  user@switch> clear security pki local-certificate all
  ```

Related Documentation

- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 1254
- Understanding Self-Signed Certificates on EX Series Switches on page 1227

Configuration Tasks for DHCP Local Server

- Using External AAA Authentication Services with DHCP on page 1256
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 1257
- Configuring DHCP Duplicate Client Support on page 1258
- Grouping Interfaces with Common DHCP Configurations on page 1258
- Guidelines for Configuring Interface Ranges on page 1259
- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Specifying the Maximum Number of DHCP Clients Per Interface on page 1262
- Disabling ARP Table Population on page 1263
- Automatically Logging Out DHCP Clients on page 1264
- Enabling Processing of Client Information Requests on page 1265
- Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 1266
- Enabling DHCPv6 Rapid Commit Support on page 1267
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 1269
- Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 1270
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 1270
- Configuring a Token for DHCP Local Server Authentication on page 1271
Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 1271
Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings on page 1272
Configuring Detection of DHCP Local Server Client Connectivity on page 1273
Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 1274
Configuring Passwords for Usernames on page 1276
Creating Unique Usernames for DHCP Clients on page 1276
Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 1279

Using External AAA Authentication Services with DHCP

The extended DHCP local server, including DHCPv6 local server, and the extended DHCP relay agent, including DHCPv6 relay agent, support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

NOTE: This section uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and responds as though it were requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the authentication-server statement at the [edit access profile profile-name] hierarchy level.

You can configure either global authentication support or group-specific support.

You must configure the username-include statement to enable the use of authentication. The password statement is not required and does not cause DHCP to use authentication if the username-include statement is not included.

To configure DHCP local server and DHCP relay agent authentication support:

1. Specify that you want to configure authentication options.
   
   • For DHCP local server:
     
     [edit system services dhcp-local-server]
     user@host# edit authentication

   • For DHCP relay agent:
     
     [edit forwarding-options dhcp-relay]
     user@host# edit authentication
2. (Optional) Configure a password that authenticates the username to the external authentication service.
   See “Configuring Passwords for Usernames” on page 1276.

3. (Optional) Configure optional features to create a unique username.
   See “Creating Unique Usernames for DHCP Clients” on page 1276.

### Guidelines for Configuring Support for DHCP Duplicate Clients

This topic describes the guidelines for configuring DHCP to include the client subinterface in order to distinguish between duplicate clients (clients with the same MAC address or client ID) in a subscriber access or in a DHCP-managed environment.

When configuring DHCP duplicate client support, consider the following guidelines:

- The optional DHCP duplicate client support feature is used for DHCPv4 clients. For DHCPv6, client identification is independent of MAC address.
- For DHCP relay agent configuration:
  - DHCP relay must be configured to insert option 82, regardless of whether or not the incoming packet has option 82.
  - Option 82 must include the Agent Circuit ID suboption (suboption 1).
  - Option 82 must be the interface name, not the interface description.
  - DHCP server must echo option 82 in the server’s reply. This is required because of the following:
    - The giaddr inserted by DHCP relay is the same for duplicate clients on different subinterfaces. The DHCP local server uses option 82 when allocating the IP address.
    - DHCP relay uses the echoed option 82 to learn the client subinterface and to construct the client key.
For the Layer 3 wholesale model:

- The wholesaler and retailer logical system/routing instances must have the same `duplicate-clients-on-interface` statement configuration.
- For DHCP relay, the wholesaler and the retailer routing contexts must both be configured with the Agent Circuit ID suboption (suboption 1) in option 82.

**Related Documentation**
- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 1198
- Configuring DHCP Duplicate Client Support on page 1258

### Configuring DHCP Duplicate Client Support

You can optionally configure DHCP local server and DHCP relay to include a client subinterface when distinguishing between two clients that have the same MAC address or client ID. The configuration is a global setting for each logical system/routing instance.

To configure DHCP local server to include the client subinterface:

1. Specify that you want to configure DHCP local server.
   
   ```
   [edit system services]
   user@host# edit dhcp-local-server
   ```

2. Configure the optional duplicate client support.
   
   ```
   [edit system services dhcp-local-server]
   user@host# set duplicate-clients-on-interface
   ```

To configure DHCP relay agent to include the client subinterface:

1. Specify that you want to configure DHCP relay agent.
   
   ```
   [edit forwarding-options]
   user@host# edit dhcp-relay
   ```

2. Configure the optional duplicate client support.
   
   ```
   [edit system services dhcp-relay]
   user@host# set duplicate-clients-on-interface
   ```

**Related Documentation**
- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 1198
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 1257

### Grouping Interfaces with Common DHCP Configurations

You use the group feature to group together a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.
To configure a DHCP local server interface group:

1. Specify that you want to configure DHCP local server.

   [edit system services]
   user@host# edit dhcp-local-server

2. Create the group and assign a name.

   [edit system services dhcp-local-server]
   user@host# edit group boston

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the `interface interface-name` statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

   [edit system services dhcp-local-server group boston]
   user@host# set interface fe-1/0/1.1
   user@host# set interface fe-1/0/1.2

4. (Optional) You can use the `upto` option to specify a range of interfaces for a group.

   [edit system services dhcp-local-server group boston]
   user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9

5. (Optional) You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

   [edit system services dhcp-local-server group boston]
   user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
   user@host# set interface fe-1/0/1.6 exclude
   user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude

### Related Documentation

- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215
- DHCPv6 Local Server Overview on page 1196
- DHCPv6 Relay Agent Overview on page 1220
- Group-Specific DHCP Local Server Options on page 1199
- Group-Specific DHCP Relay Options on page 1221
- Guidelines for Configuring Interface Ranges on page 1259

### Guidelines for Configuring Interface Ranges

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

   user@host# set interface interface-name upto upto-interface-name
• The start subunit, interface interface-name, serves as the key for the stanza. The remaining configuration settings are considered attributes.

• If the subunit is not included, an implicit .0 subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, interface ge-2/2/2 is treated as interface ge-2/2/2.0.

• Ranged entries contain the upto option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a 0 (zero) subunit acts as a wildcard.

• Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.

• Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because ge-1/0/0.10 is the start subunit for both.

  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.10

• Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface ge-1/0/0.26 is common to all three.

  dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35

• Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.20 upto ge-1/0/0.40

• A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

  In the following example, the three ranges nest properly:

  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
  interface ge-1/0/0.25 upto ge-1/0/0.29 exclude

• Discrete interfaces take precedence over ranges. In the following example, interface ge-1/0/0.20 takes precedence and enforces an interface client limit of 5.

  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
  interface ge-1/0/0.20 overrides interface-client-limit 5

Related Documentation

• Grouping Interfaces with Common DHCP Configurations on page 1258
Overridding Default DHCP Local Server Configuration Settings

Subscriber management enables you to override certain default DHCP and DHCPv6 local server configuration settings. You can override settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP local server configuration options, include the `overrides` statement and its subordinate statements at the `[edit system services dhcp-local-server]` or `[edit system services dhcp-local-server dhcpv6]` hierarchy level.

- To override DHCP local server configuration options for a named group of interfaces, include the statements at the `[edit system services dhcp-local-server group group-name]` or `[edit system services dhcp-local-server dhcpv6 group]` hierarchy level.

- To override DHCP local server configuration options for a specific interface within a named group of interfaces, include the statements at the `[edit system services dhcp-local-server group group-name interface]` or `[edit system services dhcp-local-server dhcpv6 group group-name interface]` hierarchy level.

To override default DHCP local server configuration settings:

1. Specify that you want to configure override options.
   - Global override:
     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```
     - Group level override:
       ```
       [edit system services dhcp-local-server]
       user@host# edit group boston overrides
       ```
     - Per-interface override:
       ```
       [edit system services dhcp-local-server]
       user@host# edit group boston overrides interface fe-1/0/1.1
       ```

2. (Optional) Override the maximum number of DHCP clients allowed per interface.
   - See “Specifying the Maximum Number of DHCP Clients Per Interface” on page 1262.

3. (Optional) Configure DHCP client auto logout.
   - See “Automatically Logging Out DHCP Clients” on page 1264.

4. (Optional) Enable processing of information requests from clients.
   - See “Enabling Processing of Client Information Requests” on page 1265.

5. (Optional, DHCPv6 only) Specify a delegated pool name to use for DHCPv6 multiple address assignment.
   - See “Specifying the Delegated Address Pool for IPv6 Prefix Assignment” on page 1266.

6. (Optional, DHCPv6 only) Enable DHCPv6 rapid commit support.
See “Enabling DHCPv6 Rapid Commit Support” on page 1267.

7. (Optional) Delete DHCP override settings.

See “Deleting DHCP Local Server and DHCP Relay Override Settings” on page 1267.

**Specifying the Maximum Number of DHCP Clients Per Interface**

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.

NOTE: The maximum number of DHCP (and DHCPv6) local server clients or DHCP (and DHCPv6) relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the interface-client-limit statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.

To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.

   - For DHCP local server:
     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```

   - For DHCPv6 local server:
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit overrides
     ```

   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

   - For DHCPv6 relay agent:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Configure the maximum number of clients allowed per interface. (DHCP local server, DHCPv6 local server, DHCP relay agent and DHCPv6 relay agent all support the interface-client-limit statement.)
Disabling ARP Table Population

By default, DHCP populates the ARP table with the MAC address of a client when the client binding is established. However, you may choose to use the DHCP `no-arp` statement to hide the subscriber MAC address or the DHCP client MAC address, as it appears in ARP table entries.

When running in a trusted environment (that is, when not using the `no-arp` statement), DHCP populates the ARP table with unique MAC addresses contained within the DHCP PDU for each DHCP client:

**Table 167: ARP Table in Trusted Environment**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client 1 IP Address</td>
<td>MAC A</td>
</tr>
<tr>
<td>Client 2 IP Address</td>
<td>MAC B</td>
</tr>
<tr>
<td>Client 3 IP Address</td>
<td>MAC C</td>
</tr>
</tbody>
</table>

In distrusted environments, you can specify the `no-arp` statement to hide the MAC addresses of clients. When you specify the `no-arp` statement, DHCP does not automatically populate the ARP table with MAC address information from the DHCP PDU for each client. Instead, the system performs an ARP to obtain the MAC address of each client and obtains the MAC address of the immediately attached device (for example, a DSLAM). DHCP populates the ARP table with the same interface MAC address (for example, MAC X from a DSLAM interface) for each client:

**Table 168: ARP Table in Distrusted Environment**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client 1 IP Address</td>
<td>MAC X</td>
</tr>
<tr>
<td>Client 2 IP Address</td>
<td>MAC X</td>
</tr>
<tr>
<td>Client 3 IP Address</td>
<td>MAC X</td>
</tr>
</tbody>
</table>
To disable ARP table population:

1. Configure route suppression and specify that you want to suppress destination routes.
   
   • For DHCP local server:
     
     ```
     [edit system services dhcp-local-server]
     user@host# set route-suppression destination
     ```
   
   • For DHCP relay:
     
     ```
     [edit forwarding-options dhcp-relay]
     user@host# set route-suppression destination
     ```

Related Documentation

- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Extended DHCP Local Server Overview on page 1192
- DHCPv6 Local Server Overview on page 1196
- Extended DHCP Relay Agent Overview on page 1215
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet that has the same DHCP option 60 and DHCP option 82 information as the existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.

![i]

**NOTE:** When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.
   
   • For DHCP local server:
     
     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```
   
   • For DHCP relay agent:
     
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

2. Enable auto logout. (DHCP local server and DHCP relay agent both support the `client-discover-match` statement.)
   
   • For DHCP local server:
     
     ```
     [edit system services dhcp-local-server overrides]
     user@host# set client-discover-match
     ```
For DHCP relay:

[edit forwarding-options dhcp-relay overrides]
user@host# set client-discover-match

NOTE: If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

Related Documentation
- DHCP Auto Logout Overview on page 1204
- DHCP Relay Agent Option 82 Value for Auto Logout on page 1292
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215

Enabling Processing of Client Information Requests

By default, DHCP local server and DHCPv6 local server do not respond to information request messages from the client. You can enable DHCP local server and DHCPv6 local server to process these messages and respond to them with an acknowledgment (ack or reply message, respectively) and the requested information.

DHCP relay agent automatically forwards the information request messages without modification to the configured server group by means of the interfaces configured for the respective server group. The messages are dropped if they are received on an unconfigured interface. DHCP relay proxy also supports forwarding these messages. You cannot disable forwarding of the information request messages.

Configure one or more local address pools if you want to use a local pool rather than one provided by AAA. See Configuring an Address-Assignment Pool Name and Addresses. For processing information request messages, the address configuration is not necessary. For DHCP local server, you must specify the IPv4 family; for DHCPv6 local server, you must specify the IPv6 family.

See Configuring DHCP Client-Specific Attributes for details about how to configure the information sought by clients that send information request messages.

To enable processing of DHCP client information request messages:

1. Specify that you want to configure override options.
   - For DHCP local server:
     [edit system services dhcp-local-server overrides]
     user@host# set process-inform
   - For DHCPv6 local server:
     [edit system services dhcp-local-server dhcpv6 overrides]
     user@host# set process-inform
2. (Optional) Specify a pool name from which DHCP information is returned to the client.

   • For DHCP local server:
     ```
     [edit system services dhcp-local-server overrides process-inform]
     user@host# set pool pool-name
     ```

   • For DHCPv6 local server:
     ```
     [edit system services dhcp-local-server dhcpv6 overrides process-inform]
     user@host# set pool pool-name
     ```

**Related Documentation**

- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215

### Specifying the Delegated Address Pool for IPv6 Prefix Assignment

You can explicitly specify a delegated address pool:

- On routers—Subscriber management uses the pool to assign IPv6 prefixes for subscribers. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.

- On switches—DHCP management uses the pool to assign IPv6 prefixes for DHCP clients. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.

**NOTE:** You can also use by Juniper Networks VSA 26-161 to specify the delegated address pool. The VSA-specified value always takes precedence over the delegated-address statement.

To configure the delegated address pool for DHCPv6 local server:

1. Specify that you want to configure override options.
   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit overrides
   ```

2. Configure the delegated address pool.
   ```
   [edit system services dhcp-local-server dhcpv6 overrides]
   user@host# set delegated-pool paris-cable-12
   ```

**Related Documentation**

- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215
Enabling DHCPv6 Rapid Commit Support

You can configure the extended DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled on the extended DHCPv6 local server, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client. (DHCPv6 clients are configured separately to include the DHCPv6 Rapid Commit option in the Solicit messages.) The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-method exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. By default, Rapid Commit support is disabled on the DHCPv6 local server.

To configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option:

1. Specify that you want to configure override options.
   
   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# edit overrides
   ```

2. Enable rapid commit support.
   
   ```
   [edit system services dhcp-local-server dhcpv6 overrides]
   user@host# set rapid-commit
   ```

Related Documentation

- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Extended DHCP Local Server Overview on page 1192

Deleting DHCP Local Server and DHCP Relay Override Settings

You can delete override settings for DHCP local server and DHCP relay globally, for a named group, or for a specific interface within a named group. You can delete a specific override setting or all overrides.

- To delete a specific DHCP override setting at a particular hierarchy level, include the `overrides` statement with the appropriate subordinate statements. For example, to delete the DHCP local server override `interface-client-limit` setting for a group named `marin20`:

   ```
   [edit system services dhcp-local-server]
   user@host# delete group marin20 overrides interface-client-limit
   ```

- To delete all DHCP override settings at a hierarchy level, include the `overrides` statement without any subordinate statements. For example, to delete all DHCP relay overrides for interface `fxp0.0`, which is in group `marin20`:

   ```
   [edit forwarding-options dhcp-relay]
   user@host# delete group marin20 interface fkp0.0 overrides
   ```
Configuring Extended DHCP Local Server Dynamic Client Reconfiguration

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. In addition to requesting that the DHCP local server initiate reconfiguration, you can specify the reconfiguration behavior.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.
   For DHCPv4:
   ```
   [edit system services dhcp-local-server]
   user@host# set reconfigure
   ```
   For DHCPv6:
   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set reconfigure
   ```

2. (Optional) Override the global configuration for a particular group of clients.
   For DHCPv4:
   ```
   [edit system services dhcp-local-server group-name]
   user@host# set reconfigure
   ```
   For DHCPv6:
   ```
   [edit system services dhcp-local-server dhcpv6 group group-name]
   user@host# set reconfigure
   ```

3. (Optional) Configure how the server attempts reconfiguration.
   See "Configuring Dynamic Reconfiguration Attempts for DHCP Clients" on page 1269.

4. (Optional) Configure the response to a failed reconfiguration.
   See "Configuring Deletion of the Client When Dynamic Reconfiguration Fails" on page 1270.

5. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.
   See "Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect" on page 1270.

6. (Optional) Configure a token for rudimentary server authentication.
   See "Configuring a Token for DHCP Local Server Authentication" on page 1271.

7. (Optional) Initiate reconfiguration of some or all client bindings.
See “Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings” on page 1272.

8. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.

See “Preventing Binding of Clients That Do Not Support Reconfigure Messages” on page 1271.

Configuring Dynamic Reconfiguration Attempts for DHCP Clients

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending forcerenew messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.
   
   For DHCPv4:
   ```
   [edit system services dhcp-local-server reconfigure]
   user@host# set attempts 5
   ```
   
   For DHCPv6:
   ```
   [edit system services dhcp-local-server dhcpv6 reconfigure]
   user@host# set attempts 5
   ```

2. Specify the interval between reconfiguration attempts.
   
   For DHCPv4:
   ```
   [edit system services dhcp-local-server reconfigure]
   user@host# set timeout 8
   ```
   
   For DHCPv6:
   ```
   [edit system services dhcp-local-server dhcpv6 reconfigure]
   user@host# set timeout 8
   ```

To override the global configuration for a particular group of clients, include the statements at the [edit system services dhcp-local-server group group-name reconfigure] hierarchy level or the [edit system services dhcpv6 dhcp-local-server group group-name reconfigure] hierarchy level.

Related Documentation

• Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
• attempts on page 1314
Configuring Deletion of the Client When Dynamic Reconfiguration Fails

You can configure the local server to delete the client when the maximum number of reconfiguration attempts has been made without success. By default, the client’s original configuration is restored.

(Optional) To configure the DHCP local server to delete the client when reconfiguration is not successful, for all clients:

• Specify the client deletion.
  
  For DHCPv4:
  
  [edit system services dhcp-local-server reconfigure]
  user@host# set clear-on-abort
  
  For DHCPv6:
  
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set clear-on-abort

To override the global configuration for a particular group of clients, include the statement at the [edit system services dhcp-local-server group group-name reconfigure] hierarchy level or the [edit system services dhcpv6 dhcp-local-server group group-name reconfigure] hierarchy level.

Related Documentation

• Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
• clear-on-abort on page 1318

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

You can configure the local server to reconfigure the client when the client receives a RADIUS-initiated disconnect. By default, the client is deleted when a RADIUS-initiated disconnect is received.

(Optional) To configure the DHCP local server to reconfigure the client instead of deleting the client when a RADIUS-initiated disconnect is received, for all clients:

• Specify the RADIUS-initiated disconnect trigger.
  
  For DHCPv4:
  
  [edit system services dhcp-local-server reconfigure trigger]
  user@host# set radius-disconnect
  
  For DHCPv6:
  
  [edit system services dhcp-local-server dhcpv6 reconfigure trigger]
  user@host# set radius-disconnect

To override the global configuration for a particular group of clients, include the statement at the [edit system services dhcp-local-server group group-name reconfigure trigger]
hierarchy level or the `edit system services dhcpv6 dhcp-local-server group group-name reconfigure trigger` hierarchy level.

**Related Documentation**
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- radius-disconnect on page 1365
- trigger on page 1382

**Configuring a Token for DHCP Local Server Authentication**

You can configure the local server to include a constant, unencoded token in the DHCP forcerenew message as part of the authentication option it sends to clients. The client compares the received token with a token already configured on the client. If the tokens do not match, the DHCP client discards the forcerenew message. Use of the token provides rudimentary protection against inadvertently instantiated DHCP servers.

(Optional) To configure the DHCP local server to include a token in the forcerenew message sent to the client, for all clients:

- Specify the token.
  - For DHCPv4:
    ```
    [edit system services dhcp-local-server reconfigure]
    user@host# set token 8ysIU9E32k8r
    ```
  - For DHCPv6:
    ```
    [edit system services dhcp-local-server dhcpv6 reconfigure]
    user@host# set token 8ysIU9E32k8r
    ```

To override the global configuration for a particular group of clients, include the statement at the `edit system services dhcp-local-server group group-name reconfigure` hierarchy level or the `edit system services dhcpv6 dhcp-local-server group group-name reconfigure` hierarchy level.

**Related Documentation**
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- token on page 1377

**Preventing Binding of Clients That Do Not Support Reconfigure Messages**

The DHCPv6 client and server negotiate the use of reconfigure messages. When the client can accept reconfigure messages from the server, then the client includes the Reconfigure Accept option in both solicit and request messages sent to the server.

By default, the DHCPv6 server accepts solicit messages from clients regardless of whether they support reconfiguration. You can specify that the server require clients to accept reconfigure messages. In this case, the DHCPv6 server includes the Reconfigure Accept option in both advertise and reply messages when reconfiguration is configured for the client interface. Solicit messages from nonsupporting clients are discarded and the clients are not allowed to bind.
(Optional) To configure the DHCPv6 local server to require that all clients accept reconfiguration:

- Specify strict reconfiguration.

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set strict
  ```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]` hierarchy level.

The `show dhcpv6 server statistics` command displays a count of solicit messages that the server has discarded.

### Related Documentation
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- strict on page 1373

### Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings

You can request that the DHCP local server initiate reconfiguration of all of clients or only specified clients.

To request reconfiguration of all clients:

- Specify the `all` option.
  
  For DHCPv4:

  ```
  user@host> request dhcp server reconfigure all
  ```

  For DHCPv6:

  ```
  user@host> request dhcpv6 server reconfigure all
  ```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCP client.
  
  For DHCPv4:

  ```
  user@host> request dhcp server reconfigure 192.168.27.3
  ```

  For DHCPv6:

  ```
  user@host> request dhcpv6 server reconfigure 2001:bd8:1111:2222::
  ```

- Specify the client ID of a DHCPv6 client.

  ```
  user@host> request dhcpv6 server reconfigure LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
  ```

- Specify the session ID of a DHCPv6 client.

  ```
  user@host> request dhcpv6 server reconfigure 5
  ```

- Specify the MAC address of a DHCPv4 client.

  ```
  user@host> request dhcp server reconfigure 12:23:34:45:56:67
  ```
Specify an interface; reconfiguration is attempted for all clients on this interface.

user@host> request dhcp server reconfigure interface fe-0/0/0.100

Specify a logical system; reconfiguration is attempted for all clients or the specified clients in this logical system.

user@host> request dhcp server reconfigure all logical-system ls-bldg5

Specify a routing instance; reconfiguration is attempted for all clients or the specified clients in this routing instance.

user@host> request dhcp server reconfigure all routing-instance ri-boston

Related Documentation
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- request dhcp server reconfigure on page 1542

Configuring Detection of DHCP Local Server Client Connectivity

Liveness detection for DHCP subscriber IP sessions or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

NOTE: You can also configure DHCP liveness detection for DHCP relay.

To configure liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.
   - For DHCP global configuration:
     [edit system services dhcp-local-server]
     user@host# edit liveness-detection
   - For DHCP group configuration:
     [edit system services dhcp-local-server group group-name]
     user@host# edit liveness-detection

   NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the liveness-detection statement, and any subsequent configuration statements, at the [edit system services dhcp-local-server dhcpv6] or [edit system services dhcp-local-server dhcpv6 group group-name] hierarchy level.

2. Specify that you want to configure the liveness detection method.
   - For DHCP global configuration:
For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection]
user@host# edit method
```

3. Specify the liveness detection method that you want DHCP to use.

**NOTE:** In this release, the only method supported for liveness detection is Bidirectional Forwarding Detection (BFD).

For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection method]
user@host# edit bfd
```

For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# edit bfd
```

4. Configure the liveness detection method as desired.

See “Example: Configuring Group Liveness Detection for DHCP Local Server Clients” on page 1231 for an example of how to configure DHCPv4 groups for DHCP local server liveness detection.

5. Configure the action the router takes when a liveness detection failure occurs.

For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit failure-action action
```

For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection]
user@host# edit failure-action action
```

### Related Documentation

- DHCP Liveness Detection Overview on page 1309
- Extended DHCP Local Server Overview on page 1192
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 1310
- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

### Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server

You can configure how DHCP local server handles DHCP snooped packets. Depending on the configuration, DHCP local server either forwards or drops the snooped packets it receives.
Table 169 on page 1275 indicates the action the router takes for DHCP local server snooped packets.

NOTE: Configured interfaces are those interfaces that have been configured with the group statement in the [edit system services dhcp-local-server] hierarchy. Non-configured interfaces are those that are in the logical system-routing instance but have not been configured by the group statement.

<table>
<thead>
<tr>
<th>forward-snooped-clients Configuration</th>
<th>Action on Configured Interfaces</th>
<th>Action on Non-Configured Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-snooped-clients not configured</td>
<td>dropped</td>
<td>dropped</td>
</tr>
<tr>
<td>all-interfaces</td>
<td>forwarded</td>
<td>forwarded</td>
</tr>
<tr>
<td>configured-interfaces</td>
<td>forwarded</td>
<td>dropped</td>
</tr>
<tr>
<td>non-configured-interfaces</td>
<td>dropped</td>
<td>forwarded</td>
</tr>
</tbody>
</table>

To configure DHCP snooped packet forwarding for DHCP local server:

1. Specify that you want to configure DHCP local server.
   ```
   [edit]
   user@host# edit system services dhcp-local-server
   ```
2. Enable DHCP snooped packet forwarding for DHCP local server.
   ```
   [edit system services dhcp-local-server]
   user@host# edit forward-snooped-clients
   ```
3. Specify the interfaces that are supported for snooped packet forwarding.
   ```
   [edit system services dhcp-local-server forward-snooped-clients]
   user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
   ```

For example, to configure DHCP local server to forward DHCP snooped packets on only configured interfaces:

```
[edit]
system {
  services {
    dhcp-local-server {
      forward-snooped-clients configured-interfaces;
    }
  }
}
```

Related Documentation • DHCP Snooping Support on page 1203
Configuring Passwords for Usernames

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username:

1. Specify that you want to configure authentication options.
   - For DHCP local server:
     ```
     [edit system services dhcp-local-server]
     user@host# edit authentication
     ```
   - For DHCPv6 local server:
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit authentication
     ```
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit authentication
     ```

2. Configure the password. (DHCP local server, DHCPv6 local server, and DHCP relay agent all support the `password` statement.)
   ```
   [edit system services dhcp-local-server authentication]
   user@host# set password myPassword1234
   ```

Related Documentation
- Extended DHCP Local Server Overview on page 1192
- DHCPv6 Local Server Overview on page 1196
- Extended DHCP Relay Agent Overview on page 1215
- Using External AAA Authentication Services with DHCP on page 1256
- For information about supported characters in passwords, see “Configuring Special Requirements for Plain-Text Passwords” in the Junos OS Administration Library for Routing Devices

Creating Unique Usernames for DHCP Clients

You can configure the extended DHCP application to include additional information in the username that is passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers (DHCP clients).

NOTE: If you do not include a username in the authentication configuration, the router (or switch) does not perform authentication; however, the IP address is provided by the local pool if it is configured.

When you use the DHCPv6 local server, you must configure authentication and the client username; otherwise client login fails.
The following list describes the optional information that you can include as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example `enet`.
- **client-id**—The client identifier option (option 1). (DHCPv6 local server DHCPv6 relay agent only)
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The default delimiter is a period (.). The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as a string. The router adds the `@` delimiter to the username.
- **interface-name**—The interface name, including the interface device and associated VLAN IDs.
- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of the format `xxxx.xxxx.xxxx`. (Not supported for DHCPv6 local server)
- **option-60**—The portion of the option 60 payload that follows the length field. (Not supported for DHCPv6 local server)
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload. (Not supported for DHCPv6 local server)
  - **circuit-id**—The payload of the Agent Circuit ID suboption.
  - **remote-id**—The payload of the Agent Remote ID suboption.
  - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: `circuit-id[delimiter]remote-id`.
  - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.

**NOTE:** For DHCP relay agent, the option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

- **relay-agent-interface-id**—The Interface-ID option (option 18). (DHCPv6 local server only)
- **relay-agent-remote-id**—The DHCPv6 Relay Agent Remote-ID option (option 37). (DHCPv6 local server only)
- **relay-agent-subscriber-id**—(On routers only) The DHCPv6 Relay Agent Subscriber-ID option (option 38). (DHCPv6 local server only)
• **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.

• **user-prefix**—A string indicating the user prefix.

The router (switch) creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter.

For DHCP local server and DHCP relay agent:

```
```

For DHCPv6 local server:

```
```

To configure a unique username:

1. Specify that you want to configure authentication.

   • For DHCP local server:
     
     ```
     [edit system services dhcp-local-server]
     user@host# edit authentication
     ```

   • For DHCPv6 local server:
     
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit authentication
     ```

   • For DHCP relay agent:
     
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit authentication
     ```

2. Specify that you want to include optional information in the username. (DHCP local server, DHCPv6 local server, and DHCP relay agent all support the `username-include` statement.)

   ```
   [edit system services dhcp-local-server authentication]
   user@host# set username-include
   ```

3. (Optional) Specify the optional information you want to include in the username.

   ```
   [edit system services dhcp-local-server authentication username-include]
   user@host# set username-include circuit-type
   user@host# set username-include domain-name isp55.com
   user@host# set username-include mac-address
   user@host# set username-include user-prefix wallybrown
   ```

The previous `username-include` configuration produces this unique username:

```
wallybrown.0090.1a01.1234.enet@isp55.com
```

**Related Documentation**

- Extended DHCP Local Server Overview on page 1192
- DHCPv6 Local Server Overview on page 1196
Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use

You can specify the match order in which the extended DHCP local server uses the client data to determine the address-assignment pool that provides the IP address and configuration for a DHCP client. You use the `pool-match-order` statement to specify the match order. If you do not specify the `pool-match-order`, the router (or switch) uses the default `ip-address-first` matching to select the address pool. After DHCP local server determines the address assignment pool to use, the server performs the matching based on the criteria you specified in the pool configuration.

In the default `ip-address-first` matching, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool’s address. If there is no giaddr in the request, then the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

In `external-authority` matching, the DHCP local server receives the address assignment from an external authority, such as RADIUS or Diameter. If RADIUS is the external authority, the DHCP local server uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. If Diameter is the external authority, the server uses the Diameter counterpart of the Framed-IPv6-Pool attribute to determine the pool.

For IPv4 address-assignment pools, you can optionally configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, which you can configure when you create the address-assignment pool.

**NOTE:** To use the DHCP local server option 82 matching feature with an IPv4 address-assignment pool, you must ensure that the `option-82` statement is included in the `dhcp-attributes` statement for the address-assignment pool.

To configure the matching order the extended DHCP local server uses to determine the address-assignment pool used for a client:

1. Access the `pool-match-order` configuration.

   ```
   [edit system services dhcp-local-server] 
   user@host# edit pool-match-order 
   ```
2. Specify the pool matching methods in the order in which the router (switch) performs the methods. You can specify the methods in any order. All methods are optional—the router (switch) uses the ip-address-first method by default.

- Configure the router (switch) to use an external addressing authority.
  
  ```
  [edit system services dhcp-local-server pool-match-order]
  user@host# set external-authority
  ```

- Configure the router (switch) to use the ip-address-first method.
  
  ```
  [edit system services dhcp-local-server pool-match-order]
  user@host# set ip-address-first
  ```

- (IPv4 address-assignment pools only) Specify the option 82 matching method.
  
  ```
  [edit system services dhcp-local-server pool-match-order]
  user@host# set option-82
  ```

Related Documentation
- Address-Assignment Pools Overview on page 1206
- Configuring Address-Assignment Pools
- Extended DHCP Local Server Overview on page 1192
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 1230

Configuration Tasks for DHCP Relay Agent
- Using External AAA Authentication Services with DHCP on page 1281
- Configuring DHCP Duplicate Client Support on page 1282
- Grouping Interfaces with Common DHCP Configurations on page 1283
- Guidelines for Configuring Interface Ranges on page 1284
- Overriding the Default DHCP Relay Configuration Settings on page 1285
- Overwriting giaddr Information on page 1287
- Replacing the DHCP Relay Request and Release Packet Source Address on page 1287
- Overriding Option 82 Information on page 1287
- Using Layer 2 Unicast Transmission for DHCP Packets on page 1288
- Trusting Option 82 Information on page 1288
- Disabling ARP Table Population on page 1289
- Specifying the Maximum Number of DHCP Clients Per Interface on page 1290
- Automatically Logging Out DHCP Clients on page 1291
- DHCP Relay Agent Option 82 Value for Auto Logout on page 1292
- Configuring DHCP Snooping for DHCP Relay Agent on page 1293
- Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 1294
The extended DHCP local server, including DHCPv6 local server, and the extended DHCP relay agent, including DHCPv6 relay agent, support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.

**NOTE:** This section uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors thelogout and responds as though it were requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the authentication-server statement at the [edit access profile profile-name] hierarchy level.

You can configure either global authentication support or group-specific support.

You must configure the username-include statement to enable the use of authentication. The password statement is not required and does not cause DHCP to use authentication if the username-include statement is not included.

To configure DHCP local server and DHCP relay agent authentication support:

1. Specify that you want to configure authentication options.
   - For DHCP local server:
[edit system services dhcp-local-server]
user@host# edit authentication

- For DHCP relay agent:
  [edit forwarding-options dhcp-relay]
  user@host# edit authentication

- For DHCPv6 local server:
  [edit system services dhcp-local-server dhcpv6]
  user@host# edit authentication

- For DHCPv6 relay agent:
  [edit forwarding-options dhcp-relay dhcpv6]
  user@host# edit authentication

2. (Optional) Configure a password that authenticates the username to the external authentication service.
   See “Configuring Passwords for Usernames” on page 1276.

3. (Optional) Configure optional features to create a unique username.
   See “Creating Unique Usernames for DHCP Clients” on page 1276.

Related Documentation
- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215
- DHCPv6 Local Server Overview on page 1196
- DHCPv6 Relay Agent Overview on page 1220

Configuring DHCP Duplicate Client Support

You can optionally configure DHCP local server and DHCP relay to include a client subinterface when distinguishing between two clients that have the same MAC address or client ID. The configuration is a global setting for each logical system/routing instance.

To configure DHCP local server to include the client subinterface:

1. Specify that you want to configure DHCP local server.
   [edit system services]
   user@host# edit dhcp-local-server

2. Configure the optional duplicate client support.
   [edit system services dhcp-local-server]
   user@host# set duplicate-clients-on-interface

To configure DHCP relay agent to include the client subinterface:

1. Specify that you want to configure DHCP relay agent.
   [edit forwarding-options]
   user@host# edit dhcp-relay
2. Configure the optional duplicate client support.

[edit system services dhcp-relay]
user@host# set duplicate-clients-on-interface

Related Documentation

- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 1198
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 1257

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group together a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

1. Specify that you want to configure DHCP local server.

   [edit system services]
   user@host# edit dhcp-local-server

2. Create the group and assign a name.

   [edit system services dhcp-local-server]
   user@host# edit group boston

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

   [edit system services dhcp-local-server group boston]
   user@host# set interface fe-1/0/1.1
   user@host# set interface fe-1/0/1.2

4. (Optional) You can use the upto option to specify a range of interfaces for a group.

   [edit system services dhcp-local-server group boston]
   user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9

5. (Optional) You can use the exclude option to exclude a specific interface or a specified range of interfaces from the group. For example:

   [edit system services dhcp-local-server group boston]
   user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
   user@host# set interface fe-1/0/1.6 exclude
   user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude

Related Documentation

- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215
Guidelines for Configuring Interface Ranges

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

```plaintext
user@host# set interface interface-name upto interface-name
```

- The start subunit, `interface interface-name`, serves as the key for the stanza. The remaining configuration settings are considered attributes.

- If the subunit is not included, an implicit `.0` subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, `interface ge-2/2/2` is treated as `interface ge-2/2/2.0`.

- Ranged entries contain the `upto` option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a `0` (zero) subunit acts as a wildcard.

- Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.

- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because `ge-1/0/0.10` is the start subunit for both.

  ```plaintext
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.10
  ```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—`interface ge-1/0/0.26` is common to all three.

  ```plaintext
  dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
  ```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

  ```plaintext
  interface ge-1/0/0.10 upto ge-1/0/0.30
  interface ge-1/0/0.20 upto ge-1/0/0.40
  ```
• A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

In the following example, the three ranges nest properly:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
```

• Discrete interfaces take precedence over ranges. In the following example, interface `ge-1/0/0.20` takes precedence and enforces an interface client limit of 5.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

**Related Documentation**

- Grouping Interfaces with Common DHCP Configurations on page 1258

### Overriding the Default DHCP Relay Configuration Settings

You can override the default DHCP and DHCPv6 relay agent configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

• To override global default DHCP relay agent configuration options, include the `overrides` statement and its subordinate statements at the `[edit forwarding-options dhcp-relay]` hierarchy level.

• To override DHCP relay configuration options for a named group of interfaces, include the statements at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level.

• To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the `[edit forwarding-options dhcp-relay group group-name interface]` hierarchy level.

• To configure overrides for DHCPv6 relay, use the supported statements at the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level.

To override default DHCP relay agent configuration settings:

1. Specify that you want to configure override options.

   Global override:

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

   Group-level override:

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit group boston overrides
   ```

   Per-interface override:

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit group boston interface fe-1/0/1.2 overrides
   ```
2. (DHCPv4 only) Enable DHCP relay proxy mode.
   See “Enabling DHCP Relay Proxy Mode” on page 1307.

3. (DHCPv4 only) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.
   See “Overwriting giaddr Information” on page 1287.

4. (DHCPv4 only) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).
   See “Replacing the DHCP Relay Request and Release Packet Source Address” on page 1287.

5. (DHCPv4 only) Override the DHCP relay agent information option (option 82) in DHCP packets.
   See “Overriding Option 82 Information” on page 1287.

6. (DHCPv4 only) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.
   See “Using Layer 2 Unicast Transmission for DHCP Packets” on page 1288.

7. (DHCPv4 only) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.
   See “Trusting Option 82 Information” on page 1288.

8. (DHCPv4 and DHCPv6) Override the maximum number of DHCP clients allowed per interface.
   See “Specifying the Maximum Number of DHCP Clients Per Interface” on page 1262.

9. (DHCPv4 only) Configure client auto logout.
   See “DHCP Auto Logout Overview” on page 1204.

10. (DHCPv4 and DHCPv6) Enable or disable support for DHCP snooped clients on interfaces.
    See “Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 1294.

11. (DHCPv4 and DHCPv6) Send release messages to the DHCP server when clients are deleted.
    See “Sending Release Messages When Clients Are Deleted” on page 1301.

12. (DHCPv4 only) Disable the DHCP relay agent on specific interfaces.
    See “Disabling DHCP Relay” on page 1312.

13. (DHCPv4 and DHCPv6) Disable automatic binding of stray DHCP requests.
    See “Disabling Automatic Binding of Stray DHCP Requests” on page 1302.

Related Documentation

- Group-Specific DHCP Relay Options on page 1221
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
Overwriting giaddr Information

You can configure the DHCP relay agent to change the gateway IP address (giaddr) field in packets that it forwards between a DHCP client and a DHCP server.

To overwrite the giaddr of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the giaddr of DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-giaddr
```

Related Documentation

- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285

Replacing the DHCP Relay Request and Release Packet Source Address

You can configure the DHCP relay agent to replace request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

To replace the source address with giaddr:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

```
[edit forwarding-options dhcp-relay overrides]
user@host# set replace-ip-source-with giaddr
```

Related Documentation

- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285

Overriding Option 82 Information

You can configure the DHCP relay agent to add or remove the DHCP relay agent information option (option 82) in DHCP packets.
This feature causes the DHCP relay agent to perform one of the following actions, depending on the configuration:

- If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.
- If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

To override the default option 82 information in DHCP packets destined for a DHCP server:

1. Specify that you want to configure override options.
   
   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

2. Specify that the option 82 information in DHCP packets is overwritten.
   
   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set always-write-option-82
   ```

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285

**Using Layer 2 Unicast Transmission for DHCP Packets**

You can configure the DHCP relay agent to override the setting of the broadcast bit in DHCP request packets. DHCP relay agent then instead uses the Layer 2 unicast transmission method to send DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

To override the default setting of the broadcast bit in DHCP request packets:

1. Specify that you want to configure override options.
   
   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

2. Specify that the DHCP relay agent uses the Layer 2 unicast transmission method.
   
   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set layer2-unicast-replies
   ```

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285

**Trusting Option 82 Information**

By default, the DHCP relay agent treats client packets with a giaddr of 0 (zero) and option 82 information as if the packets originated at an untrusted source, and drops them...
without further processing. You can override this behavior and specify that the DHCP relay agent process DHCP client packets that have a giaddr of 0 (zero) and contain option 82 information.

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.
   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

2. Specify that the DHCP relay agent process DHCP client packets with a giaddr of 0 and that contain option 82 information.
   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set trust-option-82
   ```

Related Documentation
- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285

Disabling ARP Table Population

By default, DHCP populates the ARP table with the MAC address of a client when the client binding is established. However, you may choose to use the DHCP `no-arp` statement to hide the subscriber MAC address or the DHCP client MAC address, as it appears in ARP table entries.

When running in a trusted environment (that is, when not using the `no-arp` statement), DHCP populates the ARP table with unique MAC addresses contained within the DHCP PDU for each DHCP client:

Table 170: ARP Table in Trusted Environment

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client 1 IP Address</td>
<td>MAC A</td>
</tr>
<tr>
<td>Client 2 IP Address</td>
<td>MAC B</td>
</tr>
<tr>
<td>Client 3 IP Address</td>
<td>MAC C</td>
</tr>
</tbody>
</table>

In distrusted environments, you can specify the `no-arp` statement to hide the MAC addresses of clients. When you specify the `no-arp` statement, DHCP does not automatically populate the ARP table with MAC address information from the DHCP PDU for each client. Instead, the system performs an ARP to obtain the MAC address of each client and obtains the MAC address of the immediately attached device (for example, a DSLAM). DHCP populates the ARP table with the same interface MAC address (for example, MAC X from a DSLAM interface) for each client:
Table 171: ARP Table in Distrusted Environment

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client 1 IP Address</td>
<td>MAC X</td>
</tr>
<tr>
<td>Client 2 IP Address</td>
<td>MAC X</td>
</tr>
<tr>
<td>Client 3 IP Address</td>
<td>MAC X</td>
</tr>
</tbody>
</table>

To disable ARP table population:

1. Configure route suppression and specify that you want to suppress destination routes.
   - For DHCP local server:
     ```
     [edit system services dhcp-local-server]
     user@host# set route-suppression destination
     ```
   - For DHCP relay:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# set route-suppression destination
     ```

Related Documentation

- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Extended DHCP Local Server Overview on page 1192
- DHCPv6 Local Server Overview on page 1196
- Extended DHCP Relay Agent Overview on page 1215
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267

Specifying the Maximum Number of DHCP Clients Per Interface

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.

**NOTE:** The maximum number of DHCP (and DHCPv6) local server clients or DHCP (and DHCPv6) relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the interface-client-limit statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.
To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.
   - For DHCP local server:
     ```
     [edit system services dhcp-local-server]
     user@host# edit overrides
     ```
   - For DHCPv6 local server:
     ```
     [edit system services dhcp-local-server dhcpv6]
     user@host# edit overrides
     ```
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```
   - For DHCPv6 relay agent:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Configure the maximum number of clients allowed per interface. (DHCP local server, DHCPv6 local server, DHCP relay agent and DHCPv6 relay agent all support the `interface-client-limit` statement.)
   ```
   [edit system services dhcp-local-server overrides]
   user@host# set interface-client-limit number
   ```

Related Documentation
- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet that has the same DHCP option 60 and DHCP option 82 information as the existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.

**NOTE:** When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.
   - For DHCP local server:
For DHCP relay agent:

[edit forwarding-options dhcp-relay]
user@host# edit overrides

2. Enable auto logout. (DHCP local server and DHCP relay agent both support the client-discover-match statement.)

• For DHCP local server:

[edit system services dhcp-local-server overrides]
user@host# set client-discover-match

• For DHCP relay:

[edit forwarding-options dhcp-relay overrides]
user@host# set client-discover-match

---

**NOTE:** If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

---

**Related Documentation**

- DHCP Auto Logout Overview on page 1204
- DHCP Relay Agent Option 82 Value for Auto Logout on page 1292
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Extended DHCP Local Server Overview on page 1192
- Extended DHCP Relay Agent Overview on page 1215

---

**DHCP Relay Agent Option 82 Value for Auto Logout**

Table 172 on page 1292 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the right column.

**Table 172: DHCP Relay Agent Option 82 Value for Auto Logout**

<table>
<thead>
<tr>
<th>DHCP Relay Agent Configuration Settings</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Relay Configured with Option 82</td>
<td></td>
</tr>
<tr>
<td>Discover Packet Contains Option 82</td>
<td></td>
</tr>
<tr>
<td>Override &quot;trust-option-82&quot;</td>
<td></td>
</tr>
<tr>
<td>Override &quot;always-write-option-82&quot;</td>
<td></td>
</tr>
<tr>
<td>giaddr in non-snooped packet</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td></td>
</tr>
<tr>
<td>No secondary search performed</td>
<td></td>
</tr>
</tbody>
</table>
Table 172: DHCP Relay Agent Option 82 Value for Auto Logout (continued)

<table>
<thead>
<tr>
<th>DHCP Relay Agent Configuration Settings</th>
<th>giaddr in non-snooped packet</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Relay Configured with Option 82</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Drop packet</td>
</tr>
<tr>
<td></td>
<td>Non-zero</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td></td>
<td>Non-zero</td>
<td>Use configured option 82</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Drop packet</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Use configured option 82</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Use option 82 from packet</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Use option 82 from packet</td>
</tr>
</tbody>
</table>

Related Documentation
- DHCP Auto Logout Overview on page 1204
- Automatically Logging Out DHCP Clients on page 1264

Configuring DHCP Snooping for DHCP Relay Agent

DHCP relay agent uses a two-part configuration to determine how to handle DHCP snooped packets. First, you enable or disable snooping support for DHCP relay agent and, optionally, override the default snooping configuration. Then you configure the forwarding action for snooped clients, which specifies whether DHCP relay agent forwards or drops snooped traffic.

To configure DHCP snooping for DHCP relay agent:

1. (DHCPv4 and DHCPv6) Enable or disable DHCP snooping. You can configure DHCP snooping globally, for a named group of interfaces, or for a specific interface.
See “Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 1294.

2. (DHCPv4 only) Configure snooped packets forwarding support.

See “Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent” on page 1299.

Related Documentation

- DHCP Snooping Support on page 1203
- Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 1294
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 1299
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 1239

Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent

DHCP relay agent uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes the first procedure, in which you configure DHCP relay to either enable or disable support for snooped packets.

The second procedure, which applies only to DHCPv4 relay agent, is described in “Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent” on page 1299, and configures the forward-snooped-clients statement, which determines whether the snooped packets are forwarded or dropped, depending on the type of interface.

NOTE: The router has a default global setting that specifies whether DHCP snooping support is enabled or disabled for DHCP relay. In Junos OS Release 10.0 and earlier, DHCP snooping is enabled by default. In Junos OS Release 10.1 and later, DHCP snooping is disabled by default.

You can override the default global DHCP snooping configuration and explicitly enable or disable DHCP snooping support. You can configure the explicit snooping support globally, for a group of interfaces, or for a specific interface in a group.

- To enable DHCP relay or DHCPv6 relay snooping support, include the allow-snooped-clients option in the overrides statement.
- To disable DHCP relay or DHCPv6 relay snooping support, include the no-allow-snooped-clients option in the overrides statement.

To enable or disable DHCP snooping support globally:

1. Specify that you want to configure DHCP relay agent.

   - For DHCP relay agent:

   [edit]
user@host# edit forwarding-options dhcp-relay

• For DHCPv6 relay agent:

  [edit]
  user@host# edit forwarding-options dhcp-relay dhcpv6

2. Specify that you want to override the default configuration.

• For DHCP relay agent:

  [edit forwarding-options dhcp-relay
  user@host# edit overrides

• For DHCPv6 relay agent:

  [edit forwarding-options dhcp-relay dhcpv6
  user@host# edit overrides

3. Enable or disable DHCP snooping support.

• To enable DHCP snooping:

  • For DHCP relay agent:

    [edit forwarding-options dhcp-relay overrides
    user@host# set allow-snooped-clients

  • For DHCPv6 relay agent:

    [edit forwarding-options dhcp-relay dhcpv6 overrides
    user@host# set allow-snooped-clients

• To disable DHCP snooping:

  • For DHCP relay agent:

    [edit forwarding-options dhcp-relay overrides
    user@host# set no-allow-snooped-clients

  • For DHCPv6 relay agent:

    [edit forwarding-options dhcp-relay dhcpv6 overrides
    user@host# set no-allow-snooped-clients

For example, to enable global DHCP snooping support:

forwarding-options {
  dhcp-relay {
    overrides {
      allow-snooped-clients;
    }
  }
}
}
To enable or disable DHCP snooping support for a group of interfaces:

1. Specify that you want to configure DHCP relay agent.
   - For DHCP relay agent:
     ```
     [edit]
     user@host# edit forwarding-options dhcp-relay
     ```
   - For DHCPv6 relay agent:
     ```
     [edit]
     user@host# edit forwarding-options dhcp-relay dhcpv6
     ```

2. Specify the named group.
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name
     ```
   - For DHCPv6 relay agent:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit group group-name
     ```

3. Specify that you want to override the default configuration.
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay group group-name]
     user@host# edit overrides
     ```
   - For DHCPv6 relay agent:
     ```
     [edit forwarding-options dhcp-relay dhcpv6 group group-name]
     user@host# edit overrides
     ```

4. Enable or disable DHCP snooping support.
   - To enable DHCP snooping:
     ```
     - For DHCP relay agent:
       ```
       [edit forwarding-options dhcp-relay group group-name overrides]
       user@host# set allow-snooped-clients
       ```
     - For DHCPv6 relay agent:
       ```
       [edit forwarding-options dhcp-relay dhcpv6 group group-name overrides]
       user@host# set allow-snooped-clients
       ```
   - To disable DHCP snooping:
     ```
     - For DHCP relay agent:
       ```
       [edit forwarding-options dhcp-relay group group-name overrides]
       user@host# set no-allow-snooped-clients
       ```
     - For DHCPv6 relay agent:
       ```
       [edit forwarding-options dhcp-relay dhcpv6 group group-name overrides]
       user@host# set no-allow-snooped-clients
       ```
For example, to enable DHCP snooping support on all interfaces in group **boston**:

```conf
forwarding-options {
    dhcp-relay {
        group boston {
            overrides {
                allow-snooped-clients;
            }
        }
    }
}
```

To enable or disable DHCP snooping support on a specific interface:

1. Specify that you want to configure DHCP relay agent.
   - For DHCP relay agent:
     ```bash
     [edit]
     user@host# edit forwarding-options dhcp-relay
     ```
     - For DHCPv6 relay agent:
       ```bash
       [edit]
       user@host# edit forwarding-options dhcp-relay dhcpv6
       ```

2. Specify the named group containing the interface.
   - For DHCP relay agent:
     ```bash
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name
     ```
   - For DHCPv6 relay agent:
     ```bash
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit group group-name
     ```

3. Specify the interface for which you want to configure DHCP snooping.
   - For DHCP relay agent:
     ```bash
     [edit forwarding-options dhcp-relay group group-name]
     user@host# edit interface interface-name
     ```
   - For DHCPv6 relay agent:
     ```bash
     [edit forwarding-options dhcp-relay dhcpv6 group group-name]
     user@host# edit interface interface-name
     ```

4. Specify that you want to override the default configuration on the interface.
   - For DHCP relay agent:
     ```bash
     [edit forwarding-options dhcp-relay group group-name interface interface-name]
     user@host# edit overrides
     ```
   - For DHCPv6 relay agent:
     ```bash
     [edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name]
     user@host# edit overrides
     ```

5. Enable or disable DHCP snooping support.
• To enable DHCP snooping:
  • For DHCP relay agent:
    [edit forwarding-options dhcp-relay group group-name interface interface-name overrides]
    user@host# set allow-snooped-clients
  • For DHCPv6 relay agent:
    [edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides]
    user@host# set allow-snooped-clients
• To disable DHCP snooping:
  • For DHCP relay agent:
    [edit forwarding-options dhcp-relay group group-name interface interface-name overrides]
    user@host# set no-allow-snooped-clients
  • For DHCPv6 relay agent:
    [edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides]
    user@host# set no-allow-snooped-clients

For example, to disable DHCP snooping support on interface ge-2/1/8.0 in group boston:

forwarding-options {
  dhcp-relay {
    group boston {
      interface ge-2/1/8.0 {
        overrides {
          no-allow-snooped-clients;
        }
      }
    }
  }
}

To enable DHCPv6 snooping support on interface ge-3/2/1.1 in group sunnyvale:

forwarding-options {
  dhcp-relay {
    dhcpv6 {
      group sunnyvale {
        interface ge-3/2/1.1 {
          overrides {
            allow-snooped-clients;
          }
        }
      }
    }
  }
}

You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

DHCP relay uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes how you use the `forward-snooped-clients` statement to manage whether DHCP relay agent forwards or drops snooped packets, depending on the type of interface on which the packets are snooped. In the other part of the DHCP relay agent snooping configuration, which is described in “Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 1294, you enable or disable the DHCP relay snooping feature.

Table 173 on page 1299 shows the action the router or switch takes on snooped packets when DHCP snooping is enabled by the `allow-snooped-clients` statement. Table 174 on page 1300 shows the action the router (or switch) takes on snooped packets when DHCP snooping is disabled by the `no-allow-snooped-clients` statement.

The router or switch also uses the configuration of the DHCP relay agent forwarding support to determine how to handle snooped BOOTREPLY packets. Table 175 on page 1300 shows the action the router (or switch) takes for the snooped BOOTREPLY packets.

### Note

**Configured interfaces** have been configured with the group statement in the `[edit forwarding-options dhcp-relay]` hierarchy. Non-configured interfaces are in the logical system/routing instance but have not been configured by the group statement.

### Table 173: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled

<table>
<thead>
<tr>
<th>forward-snooped-clients Configuration</th>
<th>Action on Configured Interfaces</th>
<th>Action on Non-Configured Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-snooped-clients not configured</td>
<td>snooped packets result in subscriber (DHCP client) creation</td>
<td>dropped</td>
</tr>
<tr>
<td>all-interfaces</td>
<td>forwarded</td>
<td>forwarded</td>
</tr>
<tr>
<td>configured-interfaces</td>
<td>forwarded</td>
<td>dropped</td>
</tr>
</tbody>
</table>
Table 173: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled (continued)

<table>
<thead>
<tr>
<th>forward-snooped-clients Configuration</th>
<th>Action on Configured Interfaces</th>
<th>Action on Non-Configured Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-configured-interfaces</td>
<td>snooped packets result in subscriber (DHCP client) creation</td>
<td>forwarded</td>
</tr>
</tbody>
</table>

Table 174: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled

<table>
<thead>
<tr>
<th>forward-snooped-clients Configuration</th>
<th>Action on Configured Interfaces</th>
<th>Action on Non-Configured Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-snooped-clients not configured</td>
<td>dropped</td>
<td>dropped</td>
</tr>
<tr>
<td>all-interfaces</td>
<td>dropped</td>
<td>forwarded</td>
</tr>
<tr>
<td>configured-interfaces</td>
<td>dropped</td>
<td>dropped</td>
</tr>
<tr>
<td>non-configured-interfaces</td>
<td>dropped</td>
<td>forwarded</td>
</tr>
</tbody>
</table>

Table 175: Actions for Snooped BOOTREPLY Packets

<table>
<thead>
<tr>
<th>forward-snooped-clients Configuration</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-snooped-clients not configured</td>
<td>snooped BOOTREPLY packets dropped if client is not found</td>
</tr>
<tr>
<td>forward-snooped-clients all configurations</td>
<td>snooped BOOTREPLY packets forwarded if client is not found</td>
</tr>
</tbody>
</table>

To configure DHCP snooped packet forwarding and BOOTREPLY snooped packet forwarding for DHCP relay agent:

1. Specify that you want to configure DHCP relay agent.
   
   [edit]
   user@host# edit forwarding-options dhcp-relay

2. Enable DHCP snooped packet forwarding.
   
   [edit forwarding-options dhcp-relay]
   user@host# edit forward-snooped-clients

3. Specify the interfaces that are supported for snooped packet forwarding.
   
   [edit forwarding-options dhcp-relay forward-snooped-clients]
   user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
For example, to configure DHCP relay agent to forward DHCP snooped packets on only configured interfaces:

```
[edit]
forwarding-options {
  dhcp-relay {
    forward-snooped-clients configured-interfaces;
  }
}
```

Related Documentation

- DHCP Snooping Support on page 1203
- Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 1294

Sending Release Messages When Clients Are Deleted

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.

**NOTE:** In Junos OS Release 10.1 and earlier, DHCP relay sends a release message to the DHCP server when the client-discover-match statement is included as a DHCP relay override. In Junos OS Release 10.2 and later, you must include the send-release-on-delete statement to configure DHCP relay and relay proxy to send the release message when the client-discover-match statement is included.

You can use the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level to override the default behavior for DHCPv6 relay agent.

To send a release message:

1. Specify that you want to configure override options.
   
   - For DHCP relay agent:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```
   
   - For DHCPv6 relay agent:
     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Specify that you want DHCP relay and relay proxy (or DHCPv6 relay agent) to send a release message when clients are deleted.
   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set send-release-on-delete
   ```
Disabling Automatic Binding of Stray DHCP Requests

DHCP requests that are received but have no entry in the database are known as stray requests. By default, DHCP relay, DHCP relay proxy, and DHCPv6 relay agent attempt to bind the requesting client by creating a database entry and forwarding the request to the DHCP server. If the server responds with an ACK, the client is bound and the ACK is forwarded to the client. If the server responds with a NAK, the database entry is deleted and the NAK is forwarded to the client. This behavior occurs regardless of whether authentication is configured.

You can override the default configuration at the global level, for a named group of interfaces, or for a specific interface within a named group. Overriding the default causes DHCP relay, DHCP relay proxy, and DHCPv6 relay agent to drop all stray requests instead of attempting to bind the clients.

NOTE: In Junos OS Release 10.4 and later, automatic binding of stray requests is enabled by default.

In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default. In those releases, DHCP relay drops stray requests and forwards a NAK to the client when authentication is configured. Otherwise, DHCP relay attempts to bind the requesting client. In those releases, DHCP relay proxy always drops stray requests and forwards a NAK to the client, regardless of the authentication configuration.

To disable automatic binding behavior, include the no-bind-on-request statement when you configure DHCP overrides at the global, group, or interface level.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set no-bind-on-request
```

To override the default behavior for DHCPv6 relay agent, configure the override at the

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# set no-bind-on-request
```

The following two examples show a configuration that disables automatic binding of stray requests for a group of interfaces and a configuration that disables automatic binding on a specific interface.

To disable automatic binding of stray requests on a group of interfaces:

1. Specify the named group.

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston
```
2. Specify that you want to configure overrides.

   [edit forwarding-options dhcp-relay group boston]
   user@host# edit overrides

3. Disable automatic binding for the group.

   [edit forwarding-options dhcp-relay group boston overrides]
   user@host# set no-bind-on-request

To disable automatic binding of stray requests on a specific interface:

1. Specify the named group of which the interface is a member.

   [edit forwarding-options dhcp-relay]
   user@host# edit group boston

2. Specify the interface on which you want to disable automatic binding.

   [edit forwarding-options dhcp-relay group boston]
   user@host# edit interface fe-1/0/1.2

3. Specify that you want to configure overrides.

   [edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
   user@host# edit overrides

4. Disable automatic binding on the interface.

   [edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
   user@host# set no-bind-on-request

Related Documentation

- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285

Enabling and Disabling Insertion of Option 82 Information

You can enable or disable support for the DHCP relay agent information option (option 82) in packets destined for a DHCP server. You can configure option 82 support globally or for a named group of interfaces.

To restore the default behavior (option 82 information is not inserted into DHCP packets), you use the `delete relay-option-82` statement.

To configure support for the DHCP relay agent information option 82, you use the `relay-option-82` statement.

The following sections describe the option 82 operations you can configure:

- Configuring Agent Circuit ID Information on page 1304
- Configuring an Option 82 Prefix on page 1304
- Using a Textual Description in Option 82 on page 1306
Configuring Agent Circuit ID Information

You use the `relay-option-82` statement to enable insertion of option 82 information in DHCP packets. You must also specify at least the `circuit-id` statement to include the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option.

If you specify the `circuit-id` statement, the format of the Agent Circuit ID information for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces is one of the following, depending on your network configuration:

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual local area networks (VLANs) or stacked VLANs (S-VLANs):
  
  `(fe | ge)-fpc/pic/port`

- For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs:
  
  `(fe | ge)-fpc/pic/port:vlan-id`

- For Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs:
  
  `(fe | ge)-fpc/pic/port:svlan-id-vlan-id`

To enable insertion of option 82 information:

1. Specify that you want to configure option 82 support.
   
   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Specify insertion of the Agent Circuit ID suboption.
   
   ```
   [edit forwarding-options dhcp-relay relay-option-82]
   user@host# set circuit-id
   ```

Configuring an Option 82 Prefix

You can include an optional prefix to the base option 82 information in DHCP packets destined for a DHCP server.

The prefix is separated from the option 82 Agent Circuit ID information by a colon (:), and can include any combination of the `host-name`, `logical-system-name`, and `routing-instance-name` options. The DHCP relay agent obtains the values for the `host-name`, `logical-system-name`, and `routing-instance-name` as follows:

- If you include the `host-name` option, the DHCP relay agent uses the hostname of the router configured with the `host-name` statement at the [edit system] hierarchy level.

- If you include the `logical-system-name` option, the DHCP relay agent uses the logical system name configured with the `logical-system` statement at the [edit logical-system] hierarchy level.

- If you include the `routing-instance-name` option, the DHCP relay agent uses the routing instance name configured with the `routing-instance` statement at the [edit routing-instances] hierarchy level or at the [edit logical-system logical-system-name routing-instances] hierarchy level.
If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).

The following examples show several possible formats for the Agent Circuit ID information when you specify the prefix statement for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  **hostname:**(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  **logical-system-name:**(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  **routing-instance-name:**(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  **host-name/logical-system-name:**(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  **logical-system-name:/routing-instance-name:**(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:
  
  **host-name/logical-system-name:/routing-instance-name:**(fe | ge)-fpc/pic/port:svlan-id-vlan-id

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the vlan-id value appears in the Agent Circuit ID format. For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs or S-VLANs, neither the vlan-id value nor the svlan-id value appears.

To configure an optional prefix with the option 82 information:

1. Specify that you want to configure option 82 support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Specify insertion of the Agent Circuit ID information.

   ```
   [edit forwarding-options dhcp-relay relay-option-82]
   user@host# edit circuit-id
   ```

3. Specify that the prefix is included in the option 82 information. In this example, the prefix includes the hostname and logical system name.
Using a Textual Description in Option 82

By default, when DHCP option 82 is inserted into client packets, the Agent Circuit ID suboption includes the interface identifier. You can optionally configure that the Agent Circuit ID suboption include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the Agent Circuit ID suboption for static interfaces. The textual description is configured using the `description` statement at the `[edit interfaces interface-name]` hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the interface identifier.

To configure the DHCP relay option 82 suboption to include the textual interface description:

1. Specify that you want to configure option 82 support.
   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Specify insertion of the Agent Circuit ID information.
   ```
   [edit forwarding-options dhcp-relay relay-option-82]
   user@host# edit circuit-id
   ```

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.
   ```
   [edit forwarding-options dhcp-relay relay-option-82 circuit-id]
   user@host# set use-interface-description device
   ```

Configuring Server Groups

You can configure a named group of DHCP servers for use by the extended DHCP relay agent on the router or switch.

You specify the name of the DHCP server group and the IP addresses of one or more DHCP servers that belong to this group. You can configure a maximum of five IP addresses per named server group.

To configure a named server group:

1. Specify the name of the server group.
   ```
   [edit forwarding-options dhcp-relay]
   user@host# set server-group myServerGroup
   ```

2. Add the IP addresses of the DHCP servers belonging to the group.
   ```
   [edit forwarding-options dhcp-relay server-group myServerGroup]
   ```
Configuring Active Server Groups

You can configure an active server group. Using an active server group enables you to apply a common DHCP relay agent configuration to a named group of DHCP server addresses.

Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

To configure an active server group:

- Specify the name of the active server group.

```
[edit forwarding-options dhcp-relay]
user@host# set active-server-group myServerGroup
```

To create an active server group as a global DHCP relay agent configuration option, include the `active-server-group` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level. To have the group apply only to a named group of interfaces, include the `active-server-group` statement at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level.

Including the `active-server-group` statement at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level (as a group-specific option) overrides the effect of including the `active-server-group` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level as a global option.

Related Documentation
- Extended DHCP Relay Agent Overview on page 1215
- Grouping Interfaces with Common DHCP Configurations on page 1258

Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable DHCP relay proxy mode.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set proxy-mode
```

Related Documentation
- DHCP Relay Proxy Overview on page 1218
- Overriding the Default DHCP Relay Configuration Settings on page 1285
Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Interface-ID (option 18) in the packets that the relay sends to a DHCPv6 server. You can configure the option 18 support at either the DHCPv6 global or group level.

- Prefix—Specify the prefix option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- Interface description—Specify the use-interface-description option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.
- Option 82 Agent Circuit ID suboption (suboption 1)—Specify the use-option-82 option to use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 1 value and inserts it into the outgoing packets. If no DHCPv4 binding exists or if the binding does not have an option 82 suboption 1 value, the router sends the packets without adding an option 18.

**NOTE:** If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Interface-ID option (option 18) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 18.
   ```
   [edit forwarding-options dhcp-relay dhcpv6]
   user@host# edit relay-agent-interface-id
   ```

2. (Optional) Specify the prefix to include in option 18.
   ```
   [edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
   user@host# set prefix prefix
   ```

3. (Optional) Specify that option 18 include the textual description of the interface. You can specify either the logical interface description or the device interface description.
   ```
   [edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
   user@host# set use-interface-description (logical | device)
   ```

4. (Optional) Specify that option 18 use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1) value.
   ```
   [edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
   user@host# set use-option-82
   ```

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
DHCP Liveness Detection Overview

Unlike PPP, DHCP does not define a native keepalive mechanism as part of either the DHCPv4 or DHCPv6 protocols. Without a keepalive mechanism, DHCP local server, DHCP relay, or DHCP relay proxy is unable to quickly detect if it has lost connectivity with a subscriber or a DHCP client; and it must rely on standard DHCP subscriber session or DHCP client session termination messages.

DHCP clients often do not send DHCP release messages prior to exiting the network. The discovery of their absence is dependent on existing DHCP lease time and release request mechanisms. These mechanisms are often considered insufficient when serving as session health checks for clients in a DHCP subscriber access or a DHCP-managed network. Because DHCP lease times are typically too long to provide an adequate response time for a session health failure, and configuring short DHCP lease times can pose an undue burden on control plane processing, implementing a DHCP liveness detection mechanism enables better monitoring of bound DHCP clients. When configured with a liveness detection protocol, if a given subscriber (or client) fails to respond to a configured number of consecutive liveness detection requests, the subscriber (or client) binding is deleted and its resources released.

DHCP liveness detection for DHCP subscriber IP or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

Using DHCP liveness detection, IP sessions are acted upon as soon as liveness detection checks fail. This faster response time serves to:

- Provide more accurate time-based accounting of subscriber (or DHCP client) sessions.
- Better preserve router (switch) resources.
- Help to reduce the window of vulnerability to some security attacks.

Examples of liveness detection protocols include Bidirectional Forwarding Detection (BFD) for both DHCPv4 and DHCPv6 subscribers, IPv4 Address Resolution Protocol (ARP) for DHCPv4 subscribers, and IPv6 Neighbor Unreachability Detection for DHCPv6 subscribers.

NOTE: This release supports only BFD for DHCPv4 and DHCPv6 liveness detection.
When configuring BFD liveness detection, keep the following in mind:

- You can configure DHCPv4 and DHCPv6 liveness detection either globally or per DHCPv4 or DHCPv6 group.
- DHCPv4 or DHCPv6 subscriber access clients that do not support BFD are not affected by the liveness detection configuration. These clients can continue to access the network (once validated) even if BFD liveness detection is enabled on the router (or switch).
- When configured, DHCPv4 or DHCPv6 initiates liveness detection checks for relevant clients (that is, clients that support BFD) when those clients enter a bound state.
- After protocol-specific messages are initiated for a BFD client, they are periodically sent to the subscriber (or client) IP address of the client and responses to those liveness detection requests are expected within a configured amount of time.
- If liveness detection responses are not received from clients that support BFD within the configured amount of time for a configured number of consecutive attempts, the liveness detection check is deemed to have failed and a configured failure action is implemented.

Related Documentation

- Configuring Detection of DHCP Local Server Client Connectivity on page 1273
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 1310

**Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity**

Liveness detection for DHCP subscriber IP or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

**NOTE:** You can also configure DHCP liveness detection for DHCP local server.
To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.
   - For DHCP global configuration:
     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection
     ```
   - For DHCP group configuration:
     ```
     [edit forwarding-options dhcp-relay group group-name]
     user@host# edit liveness-detection
     ```

   **NOTE:** Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit forwarding-options dhcp-relay dhcpv6]` or `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level.

2. (Optional) Specify that you want to use DHCP relay proxy mode.
   ```
   [edit forwarding-options dhcp-relay group group-name]
   user@host# set overrides proxy-mode
   ```

3. Specify that you want to configure the liveness detection method.
   - For DHCP global configuration:
     ```
     [edit forwarding-options dhcp-relay liveness-detection]
     user@host# edit method
     ```
   - For DHCP group configuration:
     ```
     [edit forwarding-options dhcp-relay group group-name liveness-detection]
     user@host# edit method
     ```

4. Specify the liveness detection method that you want DHCP to use.
   **NOTE:** In this release, the only method supported for liveness detection is Bidirectional Forwarding Detection (BFD).

   - For DHCP global configuration:
     ```
     [edit forwarding-options dhcp-relay liveness-detection method]
     user@host# edit bfd
     ```
   - For DHCP group configuration:
     ```
     [edit forwarding-options dhcp-relay group group-name liveness-detection method]
     user@host# edit bfd
     ```

5. Configure the liveness detection method as desired.
See Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients for an example of how to globally configure DHCP relay liveness detection.

6. Configure the action the router takes when a liveness detection failure occurs.

   • For DHCP global configuration:
     ```
     [edit forwarding-options dhcp-relay liveness-detection]
     user@host# edit failure-action action
     ```

   • For DHCP group configuration:
     ```
     [edit forwarding-options dhcp-relay group group-name liveness-detection]
     user@host# edit failure-action action
     ```

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
- DHCP Liveness Detection Overview on page 1309
- Configuring Detection of DHCP Local Server Client Connectivity on page 1273
- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

### Disabling DHCP Relay

You can disable DHCP relay on all interfaces or a group of interfaces.

To disable DHCP relay agent:

1. Specify that you want to configure override options.
   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit overrides
   ```

2. Disable the DHCP relay agent.
   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set disable-relay
   ```

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
DHCP Local Server Configuration Statements
attempts (DHCP Local Server)

Syntax

attempts attempt-count;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit...dhcpv6...] hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure how many attempts are made to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.

Options

attempt-count—Maximum number of attempts.
Range: 1 through 10
Default: 8

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
• Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 1269
authentication (DHCP Local Server)

Syntax

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
    }
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

The remaining statements are explained separately.

Required Privilege

- Level

  - system—To view this statement in the configuration.
  - system-control—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP on page 1256
bfd

Syntax

```plaintext
bfd {
  version (0 | 1 | automatic);
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  detection-time {
    threshold milliseconds;
  }
  session-mode (automatic | multihop | singlehop);
  hold-down-interval milliseconds;
}
```

Hierarchy Level

- [edit system services dhcp-local-server liveness-detection method]
- [edit system services dhcp-local-server dhcpv6 liveness-detection method]
- [edit forwarding-options dhcp-relay liveness-detection method]
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
- [edit system services dhcp-local-server group group-name liveness-detection method]
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method]
- [edit forwarding-options dhcp-relay group group-name liveness-detection method]
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]

Release Information

- Statement introduced in Junos OS Release 12.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure Bidirectional Forwarding Detection (BFD) as the liveness detection method.

The remaining statements are explained separately.

Required Privilege

- Level routing—To view this statement in the configuration.
- Level routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
circuit-type (DHCP Local Server)

Syntax

circuit-type;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include],

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Using External AAA Authentication Services with DHCP on page 1256
**clear-on-abort (DHCP Local Server)**

**Syntax**

```
clear-on-abort;
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure]
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure]
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure]
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure]
- [edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure]
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure]
- [edit routing-instances routing-instance-name system services dhcp-local-server reconfigure]
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure]
- [edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure]
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure]
- [edit system services dhcp-local-server reconfigure]
- [edit system services dhcp-local-server dhcpv6 reconfigure]
- [edit system services dhcp-local-server group group-name reconfigure]
- [edit system services dhcp-local-server dhcpv6 group group-name reconfigure]

**Release Information**

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

**Description**

Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.

**Default**

Restores the original client configuration when reconfiguration fails.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 1270
# client-discover-match (DHCP Local Server)

**Syntax**
```
client-discover-match <option60-and-option82>;
```

**Hierarchy Level**
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server overrides]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name overrides]`
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name overrides]`
- `[edit system services dhcp-local-server overrides]`
- `[edit system services dhcp-local-server group group-name overrides]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server overrides]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name overrides]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server interface interface-name overrides]`

**Release Information**
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Configure DHCP local server to use option 60 and option 82 information to uniquely identify DHCP subscribers or clients when primary subscriber or client identification fails. The statement always uses the `option60-and-option82` option. Specifying the option has no effect.

**Required Privilege Level**
- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**
- Extended DHCP Local Server Overview on page 1192
- Overriding Default DHCP Local Server Configuration Settings on page 1261
- DHCP Auto Logout Overview on page 1204
# client-id (DHCP Local Server)

**Syntax**
```
client-id;
```

**Hierarchy Level**
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]`

**Release Information**
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Specify that the DHCPv6 Client-ID option (option 1) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process.

**Required Privilege Level**
- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**
- [Creating Unique Usernames for DHCP Clients on page 1276](#)
delegated-pool (DHCP Local Server)

Syntax

```
delegated-pool pool-name;
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6 overrides],
[edit system services dhcp-local-server dhcpv6 group group-name overrides],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 ...],
[edit logical-systems logical-system-name system services system services dhcp-local-server dhcpv6 ...],
[edit routing-instances routing-instance-name system services system services dhcp-local-server dhcpv6 ...]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the address pool that assigns the IA_PD address. A pool specified by RADIUS VSA 26-161 takes precedence over the pool specified by this `delegated-pool` statement.

Options

```
pool-name—Name of the address-assignment pool.
```

Required Privilege

```
Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
```

Related Documentation

- Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 1266
- Overriding Default DHCP Local Server Configuration Settings on page 1261
### delimiter (DHCP Local Server)

**Syntax**

```
delimiter delimeter-character;```

**Hierarchy Level**
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit system services dhcp-local-server authentication username-include]`
- `[edit system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit system services dhcp-local-server group group-name authentication username-include]`
- `[edit system services dhcp-local-server group group-name authentication username-include]`

**Release Information**
- Statement introduced in Junos OS Release 9.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Specify the character used as the delimiter between the concatenated components of the username.

**Options**
- `delimiter-character`—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

**Required Privilege Level**
- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.
**detection-time**

**Syntax**

detection-time {
    threshold milliseconds;
}

**Hierarchy Level**

- [edit system services dhcp-local-server liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
- [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
- [edit system services dhcp-local-server group group-name liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Enable failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the one configured.

The remaining statement is explained separately.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
**dhcp (DHCP Client)**

**Syntax**

```plaintext
dhcp {
    client-identifier (ascii ascii | hexadecimal hexadecimal);
    lease-time (seconds | infinite);
    retransmission-attempt number;
    retransmission-interval seconds;
    server-address ip-address;
    update-server;
    vendor-id vendor-id;
}
```

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number family inet]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure a DHCP client for an IPv4 interface.

The remaining statements are described separately.

**Required Privilege Level**

- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**Related Documentation**

- Configuring a DHCP Client (CLI Procedure) on page 1249
**dhcp-local-server**

Syntax

```
dhcp-local-server {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-name;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
}
dhcpv6 {
  authentication {
    ...
  }
  group group-name {
    authentication {
      ...
    }
  }
  interface interface-name {
    exclude;
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode (automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
        ...  
      }
    }
    ...
  }
  overrides {
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
  }
}
```
rapid-commit;
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
delegated-pool;
interface-client-limit number;
process-inform {
    pool pool-name;
}
    rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {
delegated-pool;
interface-client-limit number;
process-inform {
    pool pool-name;
}
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
     service-profile dynamic-profile-name;
 }

duplicate-clients-on-interface;
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary primary-profile-name >;
forward-snoopied-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
group group-name {
     authentication {
         ...
     }
     dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary primary-profile-name >;
interface interface-name {
     exclude;
     liveness-detection {
         failure-action (clear-binding | clear-binding-if-interface-up | log-only);
         method {
             bfd {
                 version (0 | 1 | automatic);
                 minimum-interval milliseconds;
                 minimum-receive-interval milliseconds;
                 multiplier number;
                 no-adaptation;
                 transmit-interval {
                     minimum-interval milliseconds;
                     threshold milliseconds;
                 }
                 detection-time {
                     threshold milliseconds;
                 }
                 session-mode (automatic | multihop | singlehop);
                 holddown-interval milliseconds;
             }
         }
     }
     overrides {
         client-discover-match <option60-and-option82>;
         interface-client-limit number;
         process-inform {
             pool pool-name;
         }
     }
     service-profile dynamic-profile-name;
     trace;
     upto upto-interface-name;
 }
overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name system services],
[edit logical-systems logical-system-name system services],
[edit routing-instances routing-instance-name system services],
[edit system services]
Release Information
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch and enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The extended DHCP local server is incompatible with the DHCP server on J Series routers and so is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, which are configured under the [edit forwarding-options helpers] hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The dhcpv6 stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.

NOTE: When you configure the dhcp-local-server statement at the routing instance hierarchy level, you must use a routing instance type of virtual-router.

The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• Extended DHCP Local Server Overview on page 1192
• DHCPv6 Local Server Overview on page 1196
• Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
dhcpv6 (DHCP Local Server)

Syntax
dhcpv6 {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  group group-name {
    authentication {
      ...
    }
  }
  interface interface-name {
    exclude;
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode (automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
        detection-time {
          threshold milliseconds;
        }
        session-mode (automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
    }
  }
  overrides {
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
    rapid-commit;
  }
  service-profile dynamic-profile-name;
  trace;
  upto upto-interface-name;
overrides {
  delegated-pool;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
  }
}
overrides {
  delegated-pool;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
  }
}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
token token-value;
trigger {
    radius-disconnect;
}
}
route-suppression;
service-profile dynamic-profile-name;
}

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]

Release Information
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description
Configure DHCPv6 local server options on the router or switch and enable the router or switch to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining statements are explained separately.

Required Privilege
Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• DHCPv6 Local Server Overview on page 1196
## domain-name (DHCP Local Server)

**Syntax**

```plaintext
domain-name domain-name-string;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`
- `[edit system services dhcp]`
- `[edit system services dhcp-local-server authentication username-include]`
- `[edit system services dhcp-local-server dhcpv6 authentication username-include]`
- `[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]`
- `[edit system services dhcp-local-server group group-name authentication username-include]`
- `[edit system services dhcp-local-server group group-name authentication username-include]`

**Release Information**

- Statement introduced in Junos OS Release 9.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

**Options**

- `domain-name-string`—Domain name formatted string.

**Required Privilege Level**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.
duplicate-clients-on-interface (DHCP Local Server)

**Syntax**

duplicate-clients-on-interface;

**Hierarchy Level**

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]

**Release Information**

Statement introduced in Junos OS Release 10.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure DHCP local server to include the client subinterface when distinguishing between duplicate DHCP clients (clients with the same MAC address or client ID) in the same subnet. By default, DHCP distinguishes clients by subnet. This feature is supported on DHCPv4 only.

**Required Privilege Level**

system—To view this statement in the configuration.

**Related Documentation**

- Using External AAA Authentication Services with DHCP on page 1256
- Configuring DHCP Duplicate Client Support on page 1258
### dynamic-profile (DHCP Local Server)

**Syntax**

```plaintext
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
```

**Hierarchy Level**

- `[edit system services dhcp-local-server]`
- `[edit system services dhcp-local-server dhcpv6]`
- `[edit system services dhcp-local-server dhcpv6 group group-name]`
- `[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name]`
- `[edit system services dhcp-local-server group group-name]`
- `[edit system services dhcp-local-server group group-name interface interface-name]`
- `[edit logical-systems logical-system-name system services dhcp-local-server ...]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...]`

**Release Information**

- Statement introduced in Junos OS Release 9.2.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
- Options `aggregate-clients` and `use-primary` introduced in Junos OS Release 9.3.
- Support at the `[edit ... interface]` hierarchy levels introduced in Junos OS Release 11.2.

**Description**

Specify the dynamic profile that is attached to all interfaces, a named group of interfaces, or a specific interface.

**Options**

- `profile-name`—Name of the dynamic profile.

  The remaining statements are explained separately.

**Required Privilege Level**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces](#)
- [Configuring a Default Subscriber Service](#)
external-authority

**Syntax**  
external-authority;

**Hierarchy Level**  
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]

**Release Information**  
Statement introduced in Junos OS Release 10.0.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**  
Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment.

When RADIUS is the external authority, the router uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. When Diameter is the external authority, the router uses the Diameter counterpart of RADIUS Framed-IPv6-Pool attribute.

**Required Privilege**  
Level  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**  
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 1279
- Extended DHCP Local Server Overview on page 1192
- Address-Assignment Pools Overview on page 1206
failure-action

Syntax  
failure-action (clear-binding | clear-binding-if-interface-up | log-only);

Hierarchy Level  
[edit system services dhcp-local-server liveness-detection],
[edit system services dhcp-local-server dhcpv6 liveness-detection],
[edit forwarding-options dhcp-relay liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection],
[edit system services dhcp-local-server group group-name liveness-detection],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection],
[edit forwarding-options dhcp-relay group group-name liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection]

Release Information  
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  
Configure the action the router (or switch) takes when a liveness detection failure occurs.

Options  
clear-binding—The client session is cleared when a liveness detection failure occurs.

clear-binding-if-interface-up—The client session is cleared only when a liveness detection failure occurs and the local interface is detected as being up.

log-only—A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure.

Required Privilege Level  
routing—To view this statement in the configuration.
            routing-control—To add this statement to the configuration.

Related Documentation  
• DHCP Liveness Detection Overview on page 1309
• Configuring Detection of DHCP Local Server Client Connectivity on page 1273
• Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 1310
• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
**forward-snooped-clients (DHCP Local Server)**

**Syntax**

```
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

**Release Information**

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure how the DHCP local server handles DHCP snooped packets on specific interfaces.

**Options**

- **all-interfaces**—Perform the action on all interfaces.
- **configured-interfaces**—Perform the action only on configured interfaces.
- **non-configured-interfaces**—Perform the action only on nonconfigured interfaces.

**Required Privilege Level**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- DHCP Snooping Support on page 1203
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 1274
group (DHCP Local Server)

Syntax

```
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            relay-agent-interface-id
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary primary-profile-name>;
    interface interface-name {
        exclude;
        overrides {
            client-discover-match <option60-and-option82>;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit;
        }
        service-profile dynamic-profile-name;
        trace;
        upto upto-interface-name;
    }
    liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
            bfd {
                version (0 | 1 | automatic);
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
                transmit-interval {
                    minimum-interval milliseconds;
                    threshold milliseconds;
                }
                detection-time {
                    threshold milliseconds;
                }
            session-mode (automatic | multihop | singlehop):
```
holddown-interval milliseconds;

overrides {
  client-discover-match <option60-and-option82>;
  delegated-pool;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
route-suppression;
service-profile dynamic-profile-name;

Hierarchy Level
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.

Options

  group-name—Name of the group.

The remaining statements are explained separately.

Required Privilege Level
  system—To view this statement in the configuration.
  system-control—To add this statement to the configuration.
Related Documentation

- Extended DHCP Local Server Overview on page 1192
- Grouping Interfaces with Common DHCP Configurations on page 1258
- Using External AAA Authentication Services with DHCP on page 1256
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250

**holddown-interval**

**Syntax**

holddown-interval milliseconds;

**Hierarchy Level**

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure the time (in milliseconds) for which Bidirectional Forwarding Detection (BFD) holds a session up notification.

**Options**

milliseconds—Interval specifying how long a BFD session must remain up before a state change notification is sent.

**Range:** 0 through 255,000

**Default:** 0

**Required Privilege Level**

routing—To view this statement in the configuration.
route-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
interface (DHCP Local Server)

Syntax

interface interface-name {
  exclude;
  overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    rapid-commit;
  }
  service-profile dynamic-profile-name;
  trace;
  upto upto-interface-name;
}

Hierarchy Level

[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Options upto and exclude introduced in Junos OS Release 9.1.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.

NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see the Ethernet Networking Feature Guide for MX Series Routers.

Options

exclude—Exclude an interface or a range of interfaces from the group. This option and the overrides option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the upto-interface-name must be the same as the device name of the interface-name.
The remaining statements are explained separately.

**Required Privilege**

- system — To view this statement in the configuration.
- system-control — To add this statement to the configuration.

**Related Documentation**

- Extended DHCP Local Server Overview on page 1192
- Grouping Interfaces with Common DHCP Configurations on page 1258
- Using External AAA Authentication Services with DHCP on page 1256
interface-client-limit (DHCP Local Server)

Syntax

interface-client-limit number;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name system services dhcp-local-server overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name overrides],

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Set the maximum number of DHCP subscribers or DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.

Default

No limit

Options

number—Maximum number of clients allowed.
Range: 1 through 500,000

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Specifying the Maximum Number of DHCP Clients Per Interface on page 1262
- Overriding Default DHCP Local Server Configuration Settings on page 1261

interface-delete (Subscriber Management or DHCP Client Management)

Syntax  interface-delete;

Hierarchy Level  [edit system services subscriber-management maintain-subscriber]

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  On router—Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.

On switch—Configure the switch to maintain rather than log out DHCP clients when the client interface is deleted. By default, the switch logs out DHCP clients when the client interface is deleted.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events
# interface-name (DHCP Local Server)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>interface-name;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit system services dhcp-local-server authentication username-include],</td>
</tr>
<tr>
<td></td>
<td>[edit system services dhcp-local-server dhcpv6 authentication username-include],</td>
</tr>
<tr>
<td></td>
<td>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</td>
</tr>
<tr>
<td></td>
<td>[edit system services dhcp-local-server group group-name authentication username-include],</td>
</tr>
<tr>
<td></td>
<td>[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],</td>
</tr>
<tr>
<td></td>
<td>[edit logical-systems logical-system-name system services dhcp-local-server ...],</td>
</tr>
<tr>
<td></td>
<td>[edit routing-instances routing-instance-name system services dhcp-local-server ...]</td>
</tr>
</tbody>
</table>

| Release Information | Statement introduced in Junos OS Release 11.4. |
|                     | Statement introduced in Junos OS Release 12.3R2 for EX Series switches. |

| Description | Specify that the interface name is concatenated with the username during the subscriber authentication or DHCP client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support. |

| Required Privilege Level | interface—To view this statement in the configuration. |
|                         | interface-control—To add this statement to the configuration. |

| Related Documentation | Creating Unique Usernames for DHCP Clients on page 1276 |
### ip-address-first

**Syntax**

```plaintext
ip-address-first;
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name system services dhcp-local-server
pool-match-order],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server
pool-match-order],
[edit system services dhcp-local-server pool-match-order]
```

**Release Information**

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**

Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the gateway IP address if one is present in the DHCP client PDU. If no gateway IP address is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.

**Required Privilege**

- **Level**
  - system—To view this statement in the configuration.
  - system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 1279
- Extended DHCP Local Server Overview on page 1192
- Address-Assignment Pools Overview on page 1206
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
The remaining statements are explained separately.

Required Privilege Level
- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

Related Documentation
- [DHCP Liveness Detection Overview on page 1309](#)
- [Configuring Detection of DHCP Local Server Client Connectivity on page 1273](#)
- [Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 1310](#)
- [Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231](#)
Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

**mac-address (DHCP Local Server)**

**Syntax**
```
mac-address;
```

**Hierarchy Level**
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include]`,
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include]`,
- `[edit system services dhcp-local-server group group-name authentication username-include]`,
- `[edit system services dhcp-local-server group group-name authentication username-include]`.

**Release Information**
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

**Required Privilege Level**
- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 1256](#)
method

Syntax

```
method {
    bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        detection-time {
            threshold milliseconds;
        }
        session-mode (automatic | multihop | singlehop);
        holddown-interval milliseconds;
    }
}
```

Hierarchy Level

- [edit system services dhcp-local-server liveness-detection]
- [edit system services dhcp-local-server dhcpv6 liveness-detection]
- [edit forwarding-options dhcp-relay liveness-detection]
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection]
- [edit system services dhcp-local-server group group-name liveness-detection]
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection]
- [edit forwarding-options dhcp-relay group group-name liveness-detection]
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection]

Release Information

- Statement introduced in Junos OS Release 12.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the liveness detection method.

The remaining statements are explained separately.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
## minimum-interval

**Syntax**

```
minimum-interval milliseconds;
```

**Hierarchy Level**

```
[edit system services dhcp-local-server liveness-detection-method bfd],
[edit system services dhcp-local-server liveness-detection-method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 liveness-detection-method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection-method bfd transmit-interval],
[edit forwarding-options dhcp-relay liveness-detection-method bfd],
[edit forwarding-options dhcp-relay liveness-detection-method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection-method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection-method bfd transmit-interval],
[edit system services dhcp-local-server group group-name liveness-detection-method bfd],
[edit system services dhcp-local-server group group-name liveness-detection-method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection-method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection-method bfd transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection-method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection-method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection-method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection-method bfd transmit-interval]
```

**Release Information**

Statement introduced in Junos OS Release 12.1.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure the minimum intervals at which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the `transmit-interval minimal-interval` and `minimum-receive-interval` statements.

**Options**

- `milliseconds` — Specify the minimum interval value for BFD liveliness detection.  
  **Range:** 1 through 255,000

**Required Privilege Level**

- routing — To view this statement in the configuration.  
- routing-control — To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231  
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
minimum-receive-interval

Syntax

minimum-receive-interval milliseconds;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the minimum interval at which the local routing device (or switch) must receive a reply from a neighbor with which it has established a BFD session.

Options

milliseconds — Specify the minimum receive interval value.
Range: 1 through 255,000

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
multiplier

Syntax  multiplier number;

Hierarchy Level  [edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  Configure the number of hello packets not received by the neighbor before Bidirectional
Forwarding Detection (BFD) declares the neighbor down.

Options  number—Maximum allowable number of hello packets missed by the neighbor.
Range: 1 through 255
Default: 3

Required Privilege  routing—To view this statement in the configuration.
Level routing-control—To add this statement to the configuration.

Related Documentation
•  Example: Configuring Group Liveness Detection for DHCP Local Server Clients on
  page 1231
•  Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
no-adaptation

Syntax

```
no-adaptation;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure Bidirectional Forwarding Detection (BFD) sessions to not adapt to changing network conditions.

Required Privilege

```
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
```

Related Documentation

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
option-60 (DHCP Local Server)

Syntax

```
option-60;
```

Hierarchy Level

- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include`
- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include`
- `edit logical-systems logical-system-name system services dhcp-local-server authentication username-include`
- `edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include`
- `edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include`
- `edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include`
- `edit system services dhcp-local-server authentication username-include`
- `edit system services dhcp-local-server group group-name authentication username-include`

Release Information

- Statement introduced in Junos OS Release 9.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

Required Privilege Level

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP on page 1256
### option-82 (DHCP Local Server Authentication)

**Syntax**
```
option-82 <circuit-id> <remote-id>;
```

**Hierarchy Level**
- edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include
- edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include
- edit logical-systems logical-system-name system services dhcp-local-server authentication username-include
- edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include
- edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include
- edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include
- edit system services dhcp-local-server authentication username-include
- edit system services dhcp-local-server group group-name authentication username-include

**Release Information**
- Statement introduced in Junos OS Release 9.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication or DHCP client authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.

**Options**
- `circuit-id`—(Optional) Agent Circuit ID suboption (suboption 1).
- `remote-id`—(Optional) Agent Remote ID suboption (suboption 2).

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Using External AAA Authentication Services with DHCP on page 1256
option-82 (DHCP Local Server Pool Matching)

Syntax

```
option-82;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the `ip-address-first` statement before configuring the `option-82` statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool. This statement is supported for IPv4 address-assignment pools only.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 1279
- Extended DHCP Local Server Overview on page 1192
- Address-Assignment Pools Overview on page 1206
overrides (DHCP Local Server)

Syntax
overrides {
  client-discover-match;
  delegated-pool;
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
}

Hierarchy Level
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcv6],
[edit system services dhcp-local-server dhcv6 group group-name],
[edit system services dhcp-local-server dhcv6 group group-name interface interface-name],
[edit system services dhcp-local-server group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]

Release Information
Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description
Override the default configuration settings for the extended DHCP local server. Specifying the overrides statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

- To override global DHCP local server configuration options, include the overrides statement and its subordinate statements at the [edit system services dhcp-local-server] hierarchy level.

- To override configuration options for a named group of interfaces, include the statements at the [edit system services dhcp-local-server group group-name] hierarchy level.

- To override configuration options for a specific interface within a named group of interfaces, include the statements at the [edit system services dhcp-local-server group group-name interface interface-name] hierarchy level.

- Use the [edit system services dhcp-local-server dhcv6] hierarchy level to override DHCPv6 configuration options.

The remaining statements are explained separately.

The interface-client-limit statement is not supported in the [edit system services dhcp-local-server dhcv6] hierarchy level.

The delegated-pool and the rapid-commit statements are supported in the [edit system services dhcp-local-server dhcv6 ...] hierarchy level only.
Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Extended DHCP Local Server Overview on page 1192
- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
password (DHCP Local Server)

Syntax

```
password password-string;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication],
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.

Options

```
password-string — Authentication password.
```

Required Privilege Level

```
system — To view this statement in the configuration.
system-control — To add this statement to the configuration.
```

Related Documentation

- Using External AAA Authentication Services with DHCP on page 1256
## pool (DHCP Local Server Overrides)

**Syntax**
```
pool pool-name;
```

**Hierarchy Level**
- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server overrides process-inform`
- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides process-inform`
- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides process-inform`
- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides process-inform`
- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name overrides process-inform`
- `edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name interface interface-name overrides process-inform`
- `edit logical-systems logical-system-name system services dhcp-local-server overrides process-inform`
- `edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 overrides process-inform`
- `edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name overrides process-inform`
- `edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides process-inform`
- `edit logical-systems logical-system-name system services dhcp-local-server group group-name overrides process-inform`
- `edit logical-systems logical-system-name system services dhcp-local-server group group-name interface interface-name overrides process-inform`
- `edit routing-instances routing-instance-name system services dhcp-local-server overrides process-inform`
- `edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides process-inform`
- `edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides process-inform`
- `edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides process-inform`
- `edit routing-instances routing-instance-name system services dhcp-local-server group group-name overrides process-inform`
- `edit routing-instances routing-instance-name system services dhcp-local-server group group-name interface interface-name overrides process-inform`
- `editsystemservicesdhcp-local-serveroverrides process-inform`
- `editsystemservicesdhcp-local-serverdhcpv6overrides process-inform`
- `editsystemservicesdhcp-local-serverdhcpv6group group-name overrides process-inform`
- `editsystemservicesdhcp-local-serverdhcpv6group group-name interface interface-name overrides process-inform`
- `editsystemservicesdhcp-local-servergroup group-name overrides process-inform`
- `editsystemservicesdhcp-local-servergroup group-name interface interface-name overrides process-inform`

**Release Information**
- Statement introduced in Junos OS Release 11.4.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
**Description** Configure DHCP or DHCPv6 local server to reply to DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) with information taken from the specified pool without interacting with AAA.

**Options** *pool-name*—Name of the address pool, which must be configured within *family inet* for DHCP local server and within *family inet6* for DHCPv6 local server.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Enabling Processing of Client Information Requests on page 1265
- Overriding Default DHCP Local Server Configuration Settings on page 1261

---

**pool-match-order**

**Syntax**
```
pool-match-order {
  external-authority;
  ip-address-first;
  option-82;
}
```

**Hierarchy Level**
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
- [edit logical-systems logical-system-name system services dhcp-local-server],
- [edit routing-instances routing-instance-name system services dhcp-local-server],
- [edit system services dhcp-local-server]

**Release Information**
- Statement introduced in Junos OS Release 9.0.
- Statement introduced in Junos OS Release 12.1.

**Description** Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client.

The remaining statements are explained separately.

**Default** DHCP local server uses the *ip-address-first* method to determine which address pool to use.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 1279
- Extended DHCP Local Server Overview on page 1192
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
### process-inform

**Syntax**

```plaintext
process-inform {
    pool pool-name;
}
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server overrides]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name overrides]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name interface interface-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name interface interface-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name overrides]`,
- `[edit logical-systems logical-system-name system services dhcp-local-server group group-name interface interface-name overrides]`

**Release Information**

- Statement introduced in Junos OS Release 11.4.
- Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**

Enable the processing of DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) sent from the client to request DHCP options. For DHCP local servers, the messages are also passed to the configured server list.
The remaining statement is explained separately.

**Default**
Information request messages are not processed.

**Required Privilege**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Enabling Processing of Client Information Requests on page 1265
- Overriding Default DHCP Local Server Configuration Settings on page 1261
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
radius-disconnect (DHCP Local Server)

Syntax
radius-disconnect;

Hierarchy Level
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure trigger],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpcv6 reconfigure trigger],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure trigger],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpcv6 group group-name reconfigure trigger],
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure trigger],
- [edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure trigger],
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpcv6 group group-name reconfigure trigger],
- [edit routing-instances routing-instance-name system services dhcp-local-server reconfigure trigger],
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpcv6 reconfigure trigger],
- [edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure trigger],
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpcv6 group group-name reconfigure trigger],
- [edit system services dhcp-local-server reconfigure trigger],
- [edit system services dhcp-local-server dhcpcv6 reconfigure trigger],
- [edit system services dhcp-local-server group group-name reconfigure trigger],
- [edit system services dhcp-local-server dhcpcv6 group group-name reconfigure trigger],
- [edit system services dhcp-local-server dhcpv6 group group-name reconfigure trigger],
- [edit system services dhcp-local-server dhcpcv6 group group-name reconfigure trigger],
- [edit system services dhcp-local-server dhcpcv6 group group-name reconfigure trigger]

Release Information
Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit...] hierarchy levels introduced in Junos OS Release 10.4.

Description
Configure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces to be reconfigured when a RADIUS-initiated disconnect is received by the DHCP client or group of clients. A group configuration takes precedence over a DHCP local server configuration.

Default
The client is deleted when a RADIUS-initiated disconnect is received.

Required Privilege Level
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 1270
**rapid-commit (DHCPv6 Local Server)**

**Syntax**
```plaintext
rapid-commit;
```

**Hierarchy Level**
- [edit system services dhcp-local-server dhcpv6 overrides],
- [edit system services dhcp-local-server dhcpv6 group group-name overrides],
- [edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 ...],
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 ...],
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 ...]

**Release Information**
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Configure DHCPv6 local server to recognize the Rapid Commit option (DHCPv6 option 14) in DHCPv6 solicit messages sent from the DHCPv6 client. When rapid commit is enabled for both DHCPv6 local server and the DHCPv6 client, a two-message handshake is used instead of the standard four-message handshake. You can enable rapid commit support on DHCPv6 local server globally, for a named group, or for a specific interface.

**Default**
Rapid commit support is not enabled.

**Required Privilege**
- **Level**
  - system—To view this statement in the configuration.
  - system-control—To add this statement to the configuration.

**Related Documentation**
- Enabling DHCPv6 Rapid Commit Support on page 1267
- Overriding Default DHCP Local Server Configuration Settings on page 1261
reconfigure (DHCP Local Server)

**Syntax**

```
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name]
```

**Release Information**

Statement introduced in Junos OS Release 10.0.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**

Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration. The `strict` statement is available only for DHCPv6.

The remaining statements are explained separately.

**Required Privilege**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
Related Documentation

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250

**relay-agent-interface-id (DHCP Local Server)**

Syntax

```
relay-agent-interface-id;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
```

Release Information

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the DHCPv6 Relay Agent Interface-ID option (option 18) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Creating Unique Usernames for DHCP Clients on page 1276
relay-agent-remote-id (DHCP Local Server)

**Syntax**

```plaintext
relay-agent-remote-id;
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include]
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include]
- [edit system services dhcp-local-server dhcpv6 authentication username-include]
- [edit system services dhcp-local-server dhcpv6 group group-name authentication username-include]

**Release Information**

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Creating Unique Usernames for DHCP Clients on page 1276
**routing-instance-name (DHCP Local Server)**

**Syntax**

```
routing-instance-name;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include],
```

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify that the routing instance name be concatenated with the username during the subscriber authentication or DHCP client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
Related Documentation

- Using External AAA Authentication Services with DHCP on page 1256

**service-profile (DHCP Local Server)**

**Syntax**

```
service-profile dynamic-profile-name;
```

**Hierarchy Level**

- `[edit system services dhcp-local-server]`
- `[edit system services dhcp-local-server dhcpv6]`
- `[edit system services dhcp-local-server dhcpv6 group group-name]`
- `[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name]`
- `[edit system services dhcp-local-server dhcpv6 group group-name]`
- `[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name]`
- `[edit logical-systems logical-system-name system services dhcp-local-server ...]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...]`
- `[edit routing-instances routing-instance-name system services dhcp-local-server ...]`

**Release Information**

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify the default subscriber service or DHCP client management service, which is activated when the subscriber or client logs in and no other service is activated by a RADIUS server or a provisioning server.

- To specify the default service for all DHCP local server clients, include the `service-profile` statement at the `[edit system services dhcp-local-server]` hierarchy level.
- To specify the default service for a named group of interfaces, include the `service-profile` statement at the `[edit system services dhcp-local-server group group-name]` hierarchy level.
- To specify the default service for a particular interface within a named group of interfaces, include the `service-profile` statement at the `[edit system services dhcp-local-server group group-name interface interface-name]` hierarchy level.
- For DHCPv6 clients, use the `service-profile` statement at the `[edit system services dhcp-local-server dhcpv6]` hierarchy level.

**Options**

- `dynamic-profile-name`—Name of the dynamic profile that defines the service.

**Required Privilege Level**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- Extended DHCP Local Server Overview on page 1192
  - Default Subscriber Service Overview
  - Configuring a Default Subscriber Service
**session-mode**

Syntax

```
session-mode (automatic | multihop | singlehop);
```

Hierarchy Level

- [edit system services dhcp-local-server liveness-detection method bfd]
- [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd]
- [edit forwarding-options dhcp-relay liveness-detection]
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd]
- [edit system services dhcp-local-server group group-name liveness-detection method bfd]
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd]
- [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd]
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the session mode.

Options

- **automatic**—Configure single-hop BFD sessions if the peer is directly connected to the router interface and multihop BFD sessions if the peer is not directly connected to the router interface.
- **multihop**—Configure multihop BFD sessions.
- **single-hop**—Configure single hop BFD sessions.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
strict (DHCP Local Server)

**Syntax**
strict;

**Hierarchy Level**
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
- [edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
- [edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
- [edit system services dhcp-local-server dhcpv6 reconfigure],
- [edit system services dhcp-local-server dhcpv6 group group-name reconfigure]

**Release Information**
Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Specify whether the server denies a client to bind when the client does not indicate that it accepts reconfigure messages. This feature is available only for DHCPv6.

**Default**
Accept solicit messages from clients that do not support reconfiguration and permit them to bind.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 1271
threshold (detection-time)

Syntax

threshold milliseconds;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd detection-time],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd
detection-time],
[edit forwarding-options dhcp-relay liveness-detection method bfd detection-time],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd
detection-time],
[edit system services dhcp-local-server group group-name liveness-detection method bfd
detection-time],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd
detection-time],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd
detection-time],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd
detection-time]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the threshold for the adaptation of the detection time. When the BFD session
detection time adapts to a value equal to or greater than the threshold, a single trap and
and a single system log message are sent.

NOTE: The threshold time must be greater than or equal to the
minimum-interval or the minimum-receive-interval.

Options

milliseconds—Value for the detection time adaptation threshold.

Range: 1 through 255,000

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on
  page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
threshold (transmit-interval)

Syntax

threshold milliseconds;

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd transmit-interval], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval], [edit system services dhcp-local-server group group-name liveness-detection method bfd transmit-interval], [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd transmit-interval]

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Specify the threshold for detecting the adaptation of the transmit interval. When the BFD session transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.

Options

milliseconds — Threshold value.

Range: 0 through 4,294,967,295 (2^{32} – 1)

NOTE: The threshold value specified in the threshold statement must be greater than the value specified in the minimum-interval statement for the transmit-interval statement.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231

• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
timeout (DHCP Local Server)

Syntax

```
timeout timeout-value;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

Release Information

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the `edit ... dhcpv6 ...` hierarchy levels introduced in Junos OS Release 10.4.

Description

Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.

Options

```
timeout-value—Initial retry timeout value.
```

Range: 1 through 10 seconds
Default: 2 seconds

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 1269
### token (DHCP Local Server)

**Syntax**

```
token token-value;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure]
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure]
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure]
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure]
- `[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure]
- `[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure]
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure]
- `[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure]
- `[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure]
- `[edit system services dhcp-local-server reconfigure]
- `[edit system services dhcp-local-server dhcpv6 reconfigure]
- `[edit system services dhcp-local-server group group-name reconfigure]
- `[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]

**Release Information**

- Statement introduced in Junos OS Release 10.0.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
- Support at the `[edit...dhcpv6...]` hierarchy levels introduced in Junos OS Release 10.4.

**Description**

Configure a plain-text token for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. The token enables rudimentary entity authentication to protect against inadvertently instantiated DHCP servers. A null token (empty string) indicates that the configuration token functionality is not enabled. A group configuration takes precedence over a DHCP local server configuration. For more information about tokens, see RFC 3118, *Authentication for DHCP Messages*, section 4.

**Options**

- `token-value`—Plain-text alphanumeric string.

**Default**: null (empty string)

**Required Privilege Level**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
- Configuring a Token for DHCP Local Server Authentication on page 1271
traceoptions (DHCP Server)

Syntax

traceoptions {
  file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
  flag flag;
}

Hierarchy Level

[edit system services dhcp]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Define tracing operations for DHCP processes for J Series Services Routers and EX Series switches.

Options

file filename—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory /var/log.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

Range: 2 through 1000
Default: 3 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- all—All tracing operations
- binding—Trace binding operations
- config—Log reading of configuration
- conflict—Trace user-detected conflicts for IP addresses
- event—Trace important events
- ifdb—Trace interface database operations
- io—Trace I/O operations
- lease—Trace lease operations
- main—Trace main loop operations
- misc—Trace miscellaneous operations
- packet—Trace DHCP packets
• **options**—Trace DHCP options
• **pool**—Trace address pool operations
• **protocol**—Trace protocol operations
• **rtsock**—Trace routing socket operations
• **scope**—Trace scope operations
• **signal**—Trace DHCP signal operations
• **trace**—All tracing operations
• **ui**—Trace user interface operations

**match regex**—(Optional) Refine the output to include lines that contain the regular expression.

• **all**—All tracing operations
• **binding**—Trace binding operations
• **config**—Log reading of configuration
• **conflict**—Trace user-detected conflicts for IP addresses
• **event**—Trace important events
• **ifdb**—Trace interface database operations
• **io**—Trace I/O operations
• **lease**—Trace lease operations
• **main**—Trace main loop operations
• **match regex**—Refine the output to include lines that contain the regular expression.
• **misc**—Trace miscellaneous operations
• **packet**—Trace DHCP packets
• **options**—Trace DHCP options
• **pool**—Trace address pool operations
• **protocol**—Trace protocol operations
• **rtsock**—Trace routing socket operations
• **scope**—Trace scope operations
• **signal**—Trace DHCP signal operations
• **trace**—All tracing operations
• **ui**—Trace user interface operations

**no-world-readable**—(Optional) Disable unrestricted file access.
size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When the `trace-file` again reaches its maximum size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option and filename.

Syntax: `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Configuring Tracing Operations for DHCP Processes
- System Management Configuration Statements
transmit-interval

Syntax
transmit-interval {
  threshold milliseconds;
  minimum-interval milliseconds;
}

Hierarchy Level
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure the Bidirectional Forwarding Detection (BFD) transmit interval.
The remaining statements are explained separately.

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
  • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
trigger (DHCP Local Server)

Syntax
trigger {
   radius-disconnect;
}

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]

Release Information
Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

Description
Configure behavior in response to a trigger for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.

The remaining statement is explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268
• Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 1270
• radius-disconnect on page 1365
use-primary (DHCP Local Server)

Syntax

use-primary primary-profile-name;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name system services dhcp-local-server dynamic-profile profile-name],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name system services dhcp-local-server dynamic-profile profile-name],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name dynamic-profile profile-name],
[edit system services dhcp-local-server dynamic-profile profile-name],
[edit system services dhcp-local-server group group-name dynamic-profile profile-name]

Release Information

Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber or DHCP client logs in. Subsequent subscribers (or clients) are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber (or client) logs out, the next subscriber (or client) that logs in is assigned the primary dynamic profile.

Options

primary-profile-name—Name of the dynamic profile to configure as the primary dynamic profile

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
**user-prefix (DHCP Local Server)**

**Syntax**

```
user-prefix user-prefix-string;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
```

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

**Options**

```
user-prefix-string—User prefix string.
```

**Required Privilege Level**

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.
**Username-Include (DHCP Local Server)**

**Syntax**
```
username-include {
  circuit-type;
  client-id;
  delimiter delimiter-character;
  domain-name domain-name-string;
  interface-name;
  logical-system-name;
  mac-address;
  option-60;
  option-82 <circuit-id> <remote-id>;
  relay-agent-interface-id;
  relay-agent-remote-id;
  relay-agent-subscriber-id;
  routing-instance-name;
  user-prefix user-prefix-string;
}
```

**Hierarchy Level**
- [edit system services dhcp-local-server authentication],
- [edit system services dhcp-local-server dhcpv6 authentication],
- [edit system services dhcp-local-server dhcpv6 group group-name authentication],
- [edit system services dhcp-local-server group group-name authentication],
- [edit logical-systems logical-system-name routing-instances routing-instance-name system services dhcp-local-server ...],
- [edit logical-systems logical-system-name system services dhcp-local-server ...],
- [edit routing-instances routing-instance-name system services dhcp-local-server ...]

**Release Information**
- Statement introduced in Junos OS Release 9.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Configure the username that the router or switch passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The statements are explained separately. The `option-60` and `option-82` statements are not supported in the DHCPv6 hierarchy levels. The `client-id`, `relay-agent-interface-id`, `relay-agent-remote-id` and `relay-agent-subscriber-id` statements are supported in the DHCPv6 hierarchy levels only.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Using External AAA Authentication Services with DHCP on page 1256
- Creating Unique Usernames for DHCP Clients on page 1276
version (BFD)

Syntax

version (0 | 1 | automatic):

Hierarchy Level

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the BFD protocol version to detect.

Options

0—Use BFD protocol version 0.
1—Use BFD protocol version 1.

automatic—Autodetect the BFD protocol version.

Default: automatic

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

DHCP Relay Agent Configuration Statements

• [edit forwarding-options dhcp-relay] Hierarchy Level on page 1386

[edit forwarding-options dhcp-relay] Hierarchy Level

This topic lists supported and unsupported configuration statements in the [edit forwarding-options dhcp-relay] hierarchy level on EX Series switches.

• Supported statements are those that you can use to configure some aspect of a software feature on the switch.
• Unsupported statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see "EX Series Switch Software Features Overview" on page 27.

This topic lists:

• Supported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level on page 1387
• Unsupported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level on page 1391

Supported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level

The following hierarchy shows the [edit forwarding-options dhcp-relay] configuration statements supported on EX Series switches:

```plaintext
forwarding-options {
    dhcp-relay {
        active-server-group server-group-name;
        arp-inspection;
        authentication {
            ...;
        }
    }
    authentication {
        password password-string;
    }
    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
    }
    dhcpv6 {
        active-server-group server-group-name;
        authentication {
            ...
        }
        dynamic-profile profile-name {
            aggregate-clients (merge | replace);
            use-primary primary-profile-name;
        }
        group group-name {
            ...
        }
    }
}
```
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    ...
  }
  ...
}
overrides {
  ...
}
relay-agent-interface-id;
relay-option {
  ...
}
server-group {
  server-group-name {
    server-ip-address;
  }
  server-group-name {
    server-ip-address;
  }
  ...
}
service-profile dynamic-profile-name;
duplicate-clients-on-interface;
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
group group-name {
  active-server-group server-group-name;
  authentication {
    ...
  }
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
}
interface interface-name {
  exclude;
  liveness-detection {
    ...
  }
  ...
}
overrides {
  ...
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
overrides {
  allow-snooped-clients;
  always-write-giaddr;
  always-write-option-82;
client-discover-match <option60-and-option82>;
disable-relay;
interface-client-limit number;
layer2-unicast-replies;
no-allow-snoop-clients;
no-bind-on-request;
proxy-mode;
replace-ip-source-with;
send-release-on-delete;
trust-option-82;
}
relay-agent-interface-id {
  prefix prefix;
  use-interface-description (logical | device):
}
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
  drop;
  forward-only;
  local-server-group local-server-group;
  relay-server-group relay-server-group;
}
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
  drop;
  forward-only;
  local-server-group local-server-group;
  relay-server-group relay-server-group;
}
}
relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
}

service-profile dynamic-profile-name;

liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
```
detection-time {
  threshold milliseconds;
}

session-mode (automatic | multihop | singlehop);
  holddown-interval milliseconds;
}

overrides {
  allow-snooped-clients;
  interface-client-limit number;
  no-allow-snooped-clients;
  no-bind-on-request;
  send-release-on-delete;
}

relay-agent-interface-id {
  prefix prefix;
  use-interface-description (logical | device);
}

relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  equals (ascii asci-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  starts-with (ascii asci-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
}

relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
}

server-group {
  server-group-name {
    server-ip-address;
  }
}

service-profile dynamic-profile-name;
}
Unsupported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level

All statements in the [edit forwarding-options dhcp-relay] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 176: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>logical-system-name</td>
<td>[edit forwarding-options dhcp-relay authentication]</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Notational Conventions Used in Junos OS Configuration Hierarchies
access (Dynamic Access Routes)

Syntax

```
access {
  route prefix {
    next-hop next-hop;
    metric route-cost;
    preference route-distance;
    tag route-tag;
  }
}
```

Hierarchy Level

- [edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options],
- [edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name],
- [edit dynamic-profiles profile-name routing-options]

Release Information


Description

Dynamically configure access routes.

BEST PRACTICE: We recommend that you always include the access-internal stanza in the dynamic-profile when the access stanza is present for framed-route support.

Options

The remaining statements are explained separately.

Required Privilege Level

- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

Related Documentation

- Configuring Dynamic Access Routes for Subscriber Management
access-internal (Dynamic Access-Internal Routes)

**Syntax**

```
access-internal {
    route subscriber-ip-address {
        qualified-next-hop underlying-interface {
            mac-address address;
        }
    }
}
```

**Hierarchy Level**

- `[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options]`
- `[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name]`
- `[edit dynamic-profiles routing-options]`

**Release Information**


**Description**

Dynamically configure access-internal routes. Access-internal routes are optional, but are used instead of access routes if the next-hop address is not specified in the Framed-Route Attribute [22] for IPv4 or the Framed-IPv6-Route attribute [99] for IPv6.

---

**BEST PRACTICE:** We recommend that you always include the access-internal stanza in the dynamic-profile when the access stanza is present for framed-route support.

The remaining statements are explained separately.

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- *Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management*
- *Configuring Dynamic Access-Internal Routes for PPP Subscriber Management*
### active-server-group

**Syntax**

```plaintext
active-server-group server-group-name;
```

**Hierarchy Level**

- `[edit forwarding-options dhcp-relay]`
- `[edit forwarding-options dhcp-relay dhcpv6]`
- `[edit forwarding-options dhcp-relay group group-name]`
- `[edit forwarding-options dhcp-relay group group-name dhcpv6]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay]`
- `[edit logical-systems logical-system-name forwarding-options dhcpv6]`
- `[edit logical-systems logical-system-name forwarding-options group group-name]`
- `[edit logical-systems logical-system-name forwarding-options group group-name dhcpv6]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options group group-name dhcpv6]`
- `[edit routing-instances routing-instance-name forwarding-options group group-name]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name]`

**Release Information**

Statement introduced in Junos OS Release 8.3.
Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**

Apply a DHCP relay agent configuration to the named group of DHCP server addresses.
Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.
A group-specific configuration overrides a global option.

**Options**

- `server-group-name`—Name of the group of DHCP or DHCPv6 server addresses to which the DHCP or DHCPv6 relay agent configuration applies.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- [Extended DHCP Relay Agent Overview on page 1215](#)
- [Configuring Active Server Groups on page 1307](#)
- [Group-Specific DHCP Relay Options on page 1221](#)
- [dhcp-relay on page 1406](#)
allow-snooped-clients

Syntax  
allow-snooped-clients;

Hierarchy Level  
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides],  
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],  
[edit forwarding-options dhcp-relay dhcpv6 overrides],  
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],  
[edit forwarding-options dhcp-relay group group-name overrides],  
[edit forwarding-options dhcp-relay overrides],  
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],  
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],  
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information  
Statement introduced in Junos OS Release 10.2.  
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 12.1.

Description  
Explicitly enable DHCP snooping support on the router.

Use the statement at the [edit ... dhcpv6] hierarchy levels to explicitly enable snooping support on the router for DHCPv6 relay agent.

NOTE: In Junos OS Release 10.0 and earlier, DHCP snooping is enabled by default. In Release 10.1 and later, DHCP snooping is disabled by default.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  
- Extended DHCP Relay Agent Overview on page 1215  
- Overriding the Default DHCP Relay Configuration Settings on page 1285  
- DHCP Snooping Support on page 1203
always-write-giaddr

Syntax  always-write-giaddr;

Hierarchy Level  [edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information  Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description  Overwrite the gateway IP address (giaddr) of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  • Extended DHCP Relay Agent Overview on page 1215
• dhcp-relay on page 1406
always-write-option-82

Syntax  always-write-option-82;

Hierarchy Level  [edit forwarding-options dhcp-relay overrides],
  [edit forwarding-options dhcp-relay group-group-name overrides],
  [edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
  [edit logical-systems logical-system-name forwarding-options dhcp-relay group-group-name overrides],
  [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
  [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group-group-name overrides],
  [edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
  [edit routing-instances routing-instance-name forwarding-options dhcp-relay group-group-name overrides],
  [edit routing-instances routing-instance-name forwarding-options dhcp-relay group-group-name interface interface-name overrides]

Release Information  Statement introduced in Junos OS Release 8.3.
  Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. The use of this option causes the DHCP relay agent to perform one of the following actions, depending on how it is configured:

  • If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.

  • If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

Required Privilege Level  interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

Related Documentation  • Extended DHCP Relay Agent Overview on page 1215
authentication (DHCP Relay Agent)

Syntax  

authentication {  
  password password-string;  
  username-include {  
    circuit-type;  
    client-id;  
    delimiter delimiter-character;  
    domain-name domain-name-string;  
    interface-name;  
    logical-system-name;  
    mac-address;  
    option-60;  
    option-82 [circuit-id] [remote-id];  
    relay-agent-interface-id;  
    relay-agent-remote-id;  
    relay-agent-subscriber-id;  
    routing-instance-name;  
    user-prefix user-prefix-string;  
  }  
}

Hierarchy Level  
[edit forwarding-options dhcp-relay],  
[edit forwarding-options dhcp-relay dhcpv6],  
[edit forwarding-options dhcp-relay dhcpv6 group group-name],  
[edit forwarding-options dhcp-relay group group-name],  
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],  
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],  
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information  
Statement introduced in Junos OS Release 9.1.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.  
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

Description  
Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay configuration. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

The remaining statements are explained separately.

Required Privilege  
Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  
• dhcp-relay on page 1406  
• Using External AAA Authentication Services with DHCP on page 1256
bfo

Syntax  bfd {
  version (0 | 1 | automatic);
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  detection-time {
    threshold milliseconds;
  }
  session-mode (automatic | multihop | singlehop);
  holddown-interval milliseconds;
}

Hierarchy Level  [edit system services dhcp-local-server liveness-detection method],
[edit system services dhcp-local-server dhcpv6 liveness-detection method],
[edit forwarding-options dhcp-relay liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method],
[edit system services dhcp-local-server group group-name liveness-detection method],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method],
[edit forwarding-options dhcp-relay group group-name liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  Configure Bidirectional Forwarding Detection (BFD) as the liveness detection method.
The remaining statements are explained separately.

Required Privilege  routing—To view this statement in the configuration.
Level  routing-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
  • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
circuit-id (DHCP Relay Agent)

**Syntax**

```plaintext
circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
}
```

**Hierarchy Level**

- `[edit forwarding-options dhcp relay relay-option-82]`,
- `[edit forwarding-options dhcp-relay group group-name relay-option-82]`,
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82]`,
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name relay-option-82]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82]`,
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82]`,
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82]`

**Release Information**

- Statement introduced in Junos OS Release 8.3.
- Statement introduced in Junos OS Release 12.3 for EX Series switches.

**Description**

Specify the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) to include in DHCP packets destined for a DHCP server. Optionally specify that the suboption includes a prefix or textual description, or both, instead of `circuit-id`.

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual LANs (VLANs) or stacked VLANs (S-VLANs) is as follows:

```plaintext
(fe | ge)-fpc/pic/port
```

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use VLANs is as follows:

```plaintext
(fe | ge)-fpc/pic/port:vlan-id
```

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs is as follows:

```plaintext
(fe | ge)-fpc/pic/port:svlan-id:vlan-id
```

The remaining statements are explained separately.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- [Enabling and Disabling Insertion of Option 82 Information on page 1303](#)
- [Configuring Agent Circuit ID Information on page 1304](#)
# circuit-type (DHCP Relay Agent)

**Syntax**
circuit-type;

**Hierarchy Level**
- [edit forwarding-options dhcp-relay authentication username-include],
- [edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
- [edit forwarding-options dhcp-relay group group-name authentication username-include],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

**Release Information**
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

**Description**
Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

**Required Privilege**
- **Level**: interface—To view this statement in the configuration.
- **Level**: interface-control—To add this statement to the configuration.

**Related Documentation**
- Using External AAA Authentication Services with DHCP on page 1256
- Creating Unique Usernames for DHCP Clients on page 1276
client-discover-match (DHCP Relay Agent)

Syntax
client-discover-match <option60-and-option82>;

Hierarchy Level
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Configure DHCP relay to use option 60 and option 82 information to uniquely identify DHCP subscribers or clients when primary subscriber or client identification fails. The statement always uses the option60-and-option82 option. Specifying the option has no effect.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285
- DHCP Auto Logout Overview on page 1204
client-id (DHCP Relay Agent)

Syntax  
client-id;

Hierarchy Level  
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...]

Release Information  
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  
Specify that the client ID is concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege Level  
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  
• Using External AAA Authentication Services with DHCP on page 1256
• Creating Unique Usernames for DHCP Clients on page 1276
delimiter (DHCP Relay Agent)

Syntax  
delimiter delimiter-character;

Hierarchy Level  
[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]

Release Information  
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

Description  
Specify the character used as the delimiter between the concatenated components of the username. Use the statement at the [edit... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options  
delimiter-character—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

Required Privilege Level  
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  
• Using External AAA Authentication Services with DHCP on page 1256
• Creating Unique Usernames for DHCP Clients on page 1276
**detection-time**

**Syntax**

detection-time {
  threshold milliseconds;
}

**Hierarchy Level**

- [edit system services dhcp-local-server liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
- [edit forwarding-options dhcp-relay liveness-detection method bfd],
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
- [edit system services dhcp-local-server group group-name liveness-detection method bfd],
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Enable failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the one configured.

The remaining statement is explained separately.

**Required Privilege**

- **Level**
  - routing—to view this statement in the configuration.
  - routing-control—to add this statement to the configuration.

**Related Documentation**

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
dhcp-relay

Syntax
dhcp-relay {  
  active-server-group server-group-name;  
  authentication {  
    password password-string;  
    username-include {  
      circuit-type;  
      delimiter delimiter-character;  
      domain-name domain-name-string;  
      interface-name;  
      logical-system-name;  
      mac-address;  
      option-60;  
      option-82 <circuit-id> <remote-id>;  
      routing-instance-name;  
      user-prefix user-prefix-string;  
    }  
  }  
}  
dhcpv6 {  
  active-server-group server-group-name;  
  authentication {  
    password password-string;  
    username-include {  
      circuit-type;  
      client-id;  
      delimiter delimiter-character;  
      domain-name domain-name-string;  
      interface-name;  
      logical-system-name;  
      relay-agent-interface-id;  
      relay-agent-remote-id;  
      relay-agent-subscriber-id;  
      routing-instance-name;  
      user-prefix user-prefix-string;  
    }  
  }  
}  
dynamic-profile profile-name {  
  aggregate-clients (merge | replace);  
  use-primary primary-profile-name;  
}  
group group-name {  
  active-server-group server-group-name;  
  authentication {  
  }  
}  
dynamic-profile profile-name {  
  ...  
}  
interface interface-name {  
  exclude;  
  liveness-detection {  
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);  
    method {  
  
}
bfd {
  version (0 | 1 | automatic);
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  detection-time {
    threshold milliseconds;
  }
  session-mode (automatic | multihop | singlehop);
  holddown-interval milliseconds;
}
}
overrides {
  ...
}
relay-option {
  ...
}
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
route-suppression:
service-profile dynamic-profile-name;
overrides {
  ...
}
relay-agent-interface-id {
  ...
}
relay-option {
  ...
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time [1407]
threshold milliseconds;
    }
session-mode (automatic | multihop | singlehop);
    holddown-interval milliseconds;
    }
    }
overrides {
    allow-snooped-clients;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
    }
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
    }
server-group {
    server-group-name {
    server-ip-address;
    }
    }
duplicate-clients-on-interface;
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
    }
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    active-server-group server-group-name;
    authentication {
    ...
    }
    }
dynamic-profile profile-name {
    ...
    }
interface interface-name {
    exclude;
    liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
    bfd {
    version (0 | 1 | automatic);
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
    }
    detection-time {
    threshold milliseconds;
    }
} function-mode (automatic | multihop | singlehop);
holddown-interval milliseconds;
}
}
overrides {
...}

service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
...}
}
relay-option {
...}
relay-option-82 {
...}
route-suppression:
service-profile dynamic-profile-name;
}
liveness-detection {
failure-action (clear-binding | clear-binding-if-interface-up | log-only);
method {
    bfd {
        version (0 | 1 | automatic);
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        detection-time {
            threshold milliseconds;
        }
        session-mode (automatic | multihop | singlehop);
        holddown-interval milliseconds;
    }
}
overrides {
    allow-snooped-clients;
    always-write-gladdr;
    always-write-option-82;
    client-discover-match <option60-and-option82>;
    disable-relay;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
proxy-mode;
replace-ip-source-with;
send-release-on-delete;
trust-option-82;
}
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    relay-server-group group-name;
  }
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
  drop;
  forward-only;
  relay-server-group relay-server-group;
}
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
  drop;
  forward-only;
  local-server-group local-server-group;
  relay-server-group relay-server-group;
}
relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
}
server-group {
  server-group-name {
    server-ip-address;
  }
}
route-suppression;
  service-profile dynamic-profile-name;
}

Hierarchy Level
[edit forwarding-options],
[edit logical-systems logical-system-name forwarding-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options],
[edit routing-instances routing-instance-name forwarding-options]

Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

The extended DHCP and DHCPv6 relay agent options configured with the `dhcp-relay` and `dhcpv6` statements are incompatible with the DHCP/BOOTP relay agent options configured with the `bootp` statement. As a result, the extended DHCP or DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot both be enabled on the router (or switch) at the same time.

The remaining statements are explained separately.

**Required Privilege**

- **Level**
  - `interface`—To view this statement in the configuration.
  - `interface-control`—To add this statement to the configuration.

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
- DHCPv6 Relay Agent Overview on page 1220
- DHCP Relay Proxy Overview on page 1218
- Using External AAA Authentication Services with DHCP on page 1256
dhcpv6 (DHCP Relay Agent)

Syntax

```
dhcpv6 {
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
}
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}

group group-name {
  active-server-group server-group-name;
  authentication {
    ...
  }
  dynamic-profile profile-name {
    ...
  }
  interface interface-name {
    exclude;
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
          session-mode (automatic | multihop | singlehop);
          holddown-interval milliseconds;
        }
      }
    }
  }
}
```
overrides {
    ...
} service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
}
overrides {
    ...
}
relay-agent-interface-id {
    ...
}
relay-option {
    ...
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    ...
}
overrides {
    allow-snooped-clients;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
}
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
}
}
server-group {
    server-group-name {
        server-ip-address;
route-suppression;
    service-profile dynamic-profile-name;
}

Hierarchy Level
[edit forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay]

Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description
Configure DHCPv6 relay options on the router or switch and enable the router or switch
to function as a DHCPv6 relay agent. A DHCPv6 relay agent forwards DHCPv6 request
and reply packets between a DHCPv6 client and a DHCPv6 server.

The DHCPv6 relay agent server is fully compatible with the extended DHCP local server
and DHCP relay agent. However, the options configured with the dhcpv6 statement are
incompatible with the DHCP/BOOTP relay agent options configured with the bootp
statement. As a result, the DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot
be enabled on the router or switch at the same time.

The remaining statements are explained separately.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• dhcp-relay on page 1406
• DHCPv6 Relay Agent Overview on page 1220
• Using External AAA Authentication Services with DHCP on page 1256
### disable-relay

**Syntax**

disable-relay;

**Hierarchy Level**

- [edit forwarding-options dhcp-relay overrides],
- [edit forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides],

**Release Information**

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Disable DHCP relay on specific interfaces in a group.

**Required Privilege**

- **Level**
  - interface—To view this statement in the configuration.
  - interface-control—To add this statement to the configuration.

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
domain-name (DHCP Relay Agent)

Syntax

```bash
domain-name domain-name-string;
```

Hierarchy Level

- `[edit forwarding-options dhcp-relay authentication]`
- `[edit forwarding-options dhcp-relay dhcpv6 authentication]`
- `[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication]`

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Description

Specify the domain name that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.

Options

- `domain-name-string`—Domain name formatted string.

Required Privilege Level

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

Related Documentation

- Using External AAA Authentication Services with DHCP on page 1256
- Creating Unique Usernames for DHCP Clients on page 1276
drop (DHCP Relay Agent Option)

Syntax

drop;

Hierarchy Level

[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option (default-action | equals | starts-with)],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 12.3.

Description

Drop (discard) specified DHCP client packets when you use DHCP relay agent selective processing. You can configure the drop operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.

Required Privilege

Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

• Using DHCP Option Information to Selectively Process DHCP Client Traffic

duplicate-clients-on-interface (DHCP Relay Agent)

Syntax
duplicate-clients-on-interface;

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay]

Release Information

Statement introduced in Junos OS Release 10.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure DHCP relay agent to include the client subinterface when distinguishing between duplicate DHCP clients (clients with the same MAC address or client ID) in the same subnet. By default, DHCP relay distinguishes clients by subnet. This feature is supported on DHCPv4 only.

Required Privilege

Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

• Configuring DHCP Duplicate Client Support on page 1258
• Enabling and Disabling Insertion of Option 82 Information on page 1303
**dynamic-profile (DHCP Relay Agent)**

**Syntax**

```plaintext
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
```

**Hierarchy Level**

- [edit forwarding-options dhcp-relay],
- [edit forwarding-options dhcp-relay dhcpv6],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
- [edit forwarding-options dhcp-relay group group-name],
- [edit forwarding-options dhcp-relay group group-name interface interface-name],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

**Release Information**


**Description**

Specify the dynamic profile that is attached to all interfaces, to a named group of interfaces, or to a specific interface.

M120 and M320 routers do not support DHCPv6.

**Options**

- **profile-name**—Name of the dynamic profile.

The remaining statements are explained separately.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- dhcp-relay on page 1406
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
- Grouping Interfaces with Common DHCP Configurations on page 1258
- Configuring a Default Subscriber Service
**failure-action**

**Syntax**

failure-action (clear-binding | clear-binding-if-interface-up | log-only);

**Hierarchy Level**

[edit system services dhcp-local-server liveness-detection],
[edit system services dhcp-local-server dhcpv6 liveness-detection],
[edit forwarding-options dhcp-relay liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection],
[edit system services dhcp-local-server group group-name liveness-detection],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection],
[edit forwarding-options dhcp-relay group group-name liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure the action the router (or switch) takes when a liveness detection failure occurs.

**Options**

- **clear-binding**—The client session is cleared when a liveness detection failure occurs.

- **clear-binding-if-interface-up**—The client session is cleared only when a liveness detection failure occurs and the local interface is detected as being up.

- **log-only**—A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure.

**Required Privilege**

- **routin**g—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- **DHCP Liveness Detection Overview on page 1309**

- **Configuring Detection of DHCP Local Server Client Connectivity on page 1273**

- **Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 1310**

- **Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231**

- **Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients**
forward-snooped-clients (DHCP Relay Agent)

**Syntax**
```
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

**Hierarchy Level**
- `[edit forwarding-options dhcp-relay]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay]`

**Release Information**
- Statement introduced in Junos OS Release 10.4.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Configure how DHCP relay agent handles DHCP snooped packets on specific interfaces. The router or switch determines the DHCP snooping action to perform based on a combination of the `forward-snooped-clients` configuration and the configuration of either the `allow-snooped-clients` statement or the `no-allow-snooped-clients` statement.

The router (or switch) also uses this statement to determine how to handle snooped BOOTREPLY packets received on nonconfigured interfaces.

**Options**
- `all-interfaces`—Perform the action on all interfaces.
- `configured-interfaces`—Perform the action only on configured interfaces.
- `non-configured-interfaces`—Perform the action only on nonconfigured interfaces.

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- DHCP Snooping Support on page 1203
- Configuring DHCP Snooping for DHCP Relay Agent on page 1293
group (DHCP Relay Agent)

Syntax

```plaintext
group group-name {
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 [circuit-id] [remote-id];
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
  }
  interface interface-name {
    exclude;
    liveness-detection {
      failure-action (clear-binding | clear-binding-if-interface-up | log-only);
      method {
        bfd {
          version (0 | 1 | automatic);
          minimum-interval milliseconds;
          minimum-receive-interval milliseconds;
          multiplier number;
          no-adaptation;
          transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
          }
          detection-time {
            threshold milliseconds;
          }
        }
        session-mode (automatic | multihop | singlehop);
        holddown-interval milliseconds;
      }
    }
  }
  overrides {
    ...
  }
  service-profile dynamic-profile-name;
  trace;
}
```
upto upto-interface-name;
}

overrides {
  allow-snooped-clients;
  always-write-giaddr;
  always-write-option-82;
  client-discover-match <option60-and-option82>;
  disable-relay;
  interface-client-limit number;
  layer2-unicast-replies;
  no-allow-snooped-clients;
  no-bind-on-request;
  proxy-mode;
  replace-ip-source-with;
  send-release-on-delete;
  trust-option-82;
}

relay-agent-interface-id {
  prefix prefix;
  use-interface-description (logical | device);
  use-option-82;
}

relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }

  equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }

  starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }
}

relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
  }

  route-suppression;
  service-profile dynamic-profile-name;
}
Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Specify the name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration. A group must contain at least one interface. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options

group-name—Name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- dhcp-relay on page 1406
- Extended DHCP Relay Agent Overview on page 1215
- Group-Specific DHCP Relay Options on page 1221
- Grouping Interfaces with Common DHCP Configurations on page 1258
- Using External AAA Authentication Services with DHCP on page 1256
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces
holddown-interval

Syntax

```
holddown-interval milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection-method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection-method bfd],
[edit forwarding-options dhcp-relay liveness-detection-method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection-method bfd],
[edit system services dhcp-local-server group group-name liveness-detection-method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection-method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection-method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection-method bfd]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure the time (in milliseconds) for which Bidirectional Forwarding Detection (BFD) holds a session up notification.

Options

```
milliseconds — Interval specifying how long a BFD session must remain up before a state change notification is sent.
```

Range: 0 through 255,000
Default: 0

Required Privilege Level

```
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
```

Related Documentation

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
interface (DHCP Relay Agent)

Syntax

```text
interface interface-name {
    exclude;
    overrides {
        allow-snooped-clients;
        always-write-giaddr;
        always-write-option-82;
        client-discover-match <option60-and-option82>;
        disable-relay;
        interface-client-limit number;
        layer2-unicast-replies;
        no-allow-snooped-clients;
        proxy-mode;
        replace-ip-source-with;
        send-release-on-delete;
        trust-option-82;
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
```

Hierarchy Level

- [edit forwarding-options dhcp-relay dhcpv6 group group-name],
- [edit forwarding-options dhcp-relay group group-name],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 8.3.
Options upto and exclude introduced in Junos OS Release 9.1.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP or DHCPv6 relay agent is enabled. You can repeat the `interface` statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP local server. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see the Ethernet Networking Feature Guide for MX Series Routers.
Options  

- **exclude**—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

- **interface-name**—Name of the interface. You can repeat this option multiple times.

- **overrides**—Override the specified default configuration settings for the interface. The **overrides** statement is described separately.

- **upto-interface-name**—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the **upto-interface-name** must be the same as the device name of the **interface-name**.

The remaining statements are explained separately.

**Required Privilege**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- [Extended DHCP Relay Agent Overview on page 1215](#)
- [Grouping Interfaces with Common DHCP Configurations on page 1258](#)
- [Using External AAA Authentication Services with DHCP on page 1256](#)
interface-client-limit (DHCP Relay Agent)

Syntax

```
interface-client-limit number;
```

Hierarchy Level

- [edit forwarding-options dhcp dhcpv6 overrides],
- [edit forwarding-options dhcp dhcpv6 group group-name overrides],
- [edit forwarding-options dhcp dhcpv6 group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],

Release Information

Statement introduced in Junos OS Release 9.2.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Set the maximum number of DHCP (or DHCPv6) subscribers or clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

Default

No limit

Options

- `number`—Maximum number of clients allowed.
  - Range: 1 through 500,000

Required Privilege Level

- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.
interface-delete (Subscriber Management or DHCP Client Management)

Syntax

interface-delete;

Hierarchy Level

[edit system services subscriber-management maintain-subscriber]

Release Information

Statement introduced in Junos OS Release 11.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

On router—Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.

On switch—Configure the switch to maintain rather than log out DHCP clients when the client interface is deleted. By default, the switch logs out DHCP clients when the client interface is deleted.

Required Privilege Level

system—to view this statement in the configuration.
system-control—to add this statement to the configuration.

Related Documentation

• Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events
interface-name (DHCP Relay Agent)

Syntax

interface-name;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 11.4
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the interface name is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Required Privilege

level  interface—to view this statement in the configuration.
level  interface-control—to add this statement to the configuration.

Related Documentation

• Creating Unique Usernames for DHCP Clients on page 1276
layer2-unicast-replies

Syntax  
layer2-unicast-replies;

Hierarchy Level  
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information  
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description  
Override the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

Required Privilege Level  
interface—for viewing this statement in the configuration.
interface-control—for adding this statement to the configuration.

Related Documentation  
• Extended DHCP Relay Agent Overview on page 1215
• dhcp-relay on page 1406
liveness-detection

Syntax

liveness-detection {  
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);  
  method {  
    bfd {  
      version (0 | 1 | automatic);  
      minimum-interval milliseconds;  
      minimum-receive-interval milliseconds;  
      multiplier number;  
      no-adaptation;  
      transmit-interval {  
        minimum-interval milliseconds;  
        threshold milliseconds;  
      }  
      detection-time {  
        threshold milliseconds;  
      }  
      session-mode (automatic | multihop | singlehop);  
      holddown-interval milliseconds;  
    }  
  }  
}

Hierarchy Level

[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name]

Release Information

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Configure bidirectional failure detection timers and authentication criteria for static routes.

The remaining statements are explained separately.

Required Privilege

Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- DHCP Liveness Detection Overview on page 1309
- Configuring Detection of DHCP Local Server Client Connectivity on page 1273
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 1310
- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

**local-server-group (DHCP Relay Agent Option)**

**Syntax**

```plaintext
local-server-group
local-server-group;
```

**Hierarchy Level**

- `[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with)]`,
- `[edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals | starts-with)]`,
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay ...]`,
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...]`,
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]`

**Release Information**

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Forward DHCP client packets to the specified group of DHCP local servers when you use the DHCP relay selective processing feature. You can configure the forwarding operation globally or for a group of interfaces.

The `local-server-group` option is not supported for DHCPv6 relay agent.

**Options**

- `local-server-group`—Name of DHCP local server group.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- *Using DHCP Option Information to Selectively Process DHCP Client Traffic*
mac-address (DHCP Relay Agent)

Syntax

mac-address;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

• Using External AAA Authentication Services with DHCP on page 1256
**method**

**Syntax**
```
method {
  bfd {
    version (0 | 1 | automatic);
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    detection-time {
      threshold milliseconds;
    }
    session-mode (automatic | multihop | singlehop);
    holddown-interval milliseconds;
  }
}
```

**Hierarchy Level**
- [edit system services dhcp-local-server liveness-detection]
- [edit system services dhcp-local-server dhcpv6 liveness-detection]
- [edit forwarding-options dhcp-relay liveness-detection]
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection]
- [edit system services dhcp-local-server group group-name liveness-detection]
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection]
- [edit forwarding-options dhcp-relay group group-name liveness-detection]
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection]

**Release Information**
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
Configure the liveness detection method.

The remaining statements are explained separately.

**Required Privilege**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring Group Liveness Detection for DHCP Local Server Clients* on page 1231
- *Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients*
**minimum-interval**

**Syntax**

minimum-interval milliseconds;

**Hierarchy Level**

[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd transmit-interval]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure the minimum intervals at which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the transmit-interval minimal-interval and minimum-receive-interval statements.

**Options**

milliseconds — Specify the minimum interval value for BFD liveliness detection.

**Range:** 1 through 255,000

**Required Privilege Level**

routing—To view this statement in the configuration.
routeing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
minimum-receive-interval

Syntax  
minimum-receive-interval milliseconds;

Hierarchy Level  
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Release Information  
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  
Configure the minimum interval at which the local routing device (or switch) must receive a reply from a neighbor with which it has established a BFD session.

Options  
milliseconds — Specify the minimum receive interval value.
Range: 1 through 255,000

Required Privilege  
Level  
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  
• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
### multiplier

**Syntax**

```
multiplier number;
```

**Hierarchy Level**

- [edit system services dhcp-local-server liveness-detection method bfd]
- [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd]
- [edit forwarding-options dhcp-relay liveness-detection method bfd]
- [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd]
- [edit system services dhcp-local-server group group-name liveness-detection method bfd]
- [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd]
- [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd]
- [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

**Release Information**

- Statement introduced in Junos OS Release 12.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure the number of hello packets not received by the neighbor before Bidirectional Forwarding Detection (BFD) declares the neighbor down.

**Options**

`number`—Maximum allowable number of hello packets missed by the neighbor.

- **Range:** 1 through 255
- **Default:** 3

**Required Privilege**

- **Level:** routing—To view this statement in the configuration.
- **Level:** routing-control—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231](#)
- [Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients](#)
# next-hop (Dynamic Access-Internal Routes)

**Syntax**
```
next-hop next-hop;
```

**Hierarchy Level**
- `[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options access route prefix]`
- `[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name access route prefix]`
- `[edit dynamic-profiles profile-name routing-options access route prefix]`

**Release Information**

**Description**
Dynamically configure the next-hop address for an access route. Access routes are typically unnumbered interfaces.

**Options**
- **next-hop**—Either the specific next-hop address you want to assign to the access route or one of the following next-hop address predefined variables.
  - For IPv4 access routes, use the variable, `$junos-framed-route-nexthop`. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
  - For IPv6 access routes, use the variable, `$junos-framed-route-ipv6-nexthop`. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- `Configuring Dynamic Access Routes for Subscriber Management`
no-adaptation

Syntax  no-adaptation;

Hierarchy Level  [edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  Configure Bidirectional Forwarding Detection (BFD) sessions to not adapt to changing network conditions.

Required Privilege  Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  •  Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231

•  Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
no-allow-snooped-clients

Syntax  
no-allow-snooped-clients;

Hierarchy Level  
[edit forwarding-options dhcp relay dhcpv6 group group-name interface interface-name overrides],
[edit forwarding-options dhcp relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp relay dhcpv6 overrides],
[edit forwarding-options dhcp relay group group-name interface interface-name overrides],
[edit forwarding-options dhcp relay group group-name overrides],
[edit forwarding-options dhcp relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information  
Statement introduced in Junos OS Release 10.2.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description  
Explicitly disable DHCP snooping support on the router or switch.
Use the statement at the [edit ... dhcpv6] hierarchy levels to explicitly disable snooping support on the router or switch for DHCPv6 relay agent.

NOTE: In Junos OS Release 10.0 and earlier, DHCP snooping is enabled by default. In Release 10.1 and later, DHCP snooping is disabled by default.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  
• Extended DHCP Relay Agent Overview on page 1215  
• Overriding the Default DHCP Relay Configuration Settings on page 1285  
• DHCP Snooping Support on page 1203
**Syntax**

```plaintext
no-bind-on-request;
```

**Hierarchy Level**

- [edit forwarding-options dhcp-relay dhcpv6 overrides],
- [edit forwarding-options dhcp-relay overrides],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay interface interface-name overrides],

**Release Information**

Statement introduced in Junos OS Release 10.4.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

**Description**

Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (stray requests). Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

**NOTE:** Beginning with Junos OS Release 10.4, automatic binding of stray requests is enabled by default. In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.
option-60 (DHCP Relay Agent)

**Syntax**

```plaintext
option-60;
```

**Hierarchy Level**

```
[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]
```

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify that the payload of the Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication or client authentication process.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- Using External AAA Authentication Services with DHCP on page 1256
option-82 (DHCP Relay Agent)

Syntax

option-82 <circuit-id> <remote-id>;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Specify the option 82 that is concatenated with the username during the subscriber authentication or client authentication process. You can specify either, both, or neither the Agent Circuit ID and the Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If neither suboption is supplied, the raw payload of option 82 is concatenated to the username.

NOTE: The option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

Options

circuit-id—(Optional) The string for the Agent Circuit ID suboption (suboption 1).

remote-id—(Optional) The string for the Agent Remote ID suboption (suboption 2).

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

• Using External AAA Authentication Services with DHCP on page 1256
option-number (DHCP Relay Agent Option)

Syntax

```
option-number option-number;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option],
[edit forwarding-options dhcp-relay dhcpv6 relay-option],
[edit forwarding-options dhcp-relay group group-name relay-option],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information

Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Specify the DHCP option DHCP relay agent uses for selective processing of client traffic. You can configure support globally or for a named group of interfaces. You can also configure support for the extended DHCP relay agent on a per logical system and per routing instance basis.

Use the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level to configure the DHCPv6 relay agent support.

Options

```
option-number—The DHCP or DHCPv6 option in the incoming traffic.
```

**NOTE:** EX Series switches do not support the User Class Options.

- 15 (DHCPv6 only)—Use DHCPv6 option 15 (User Class Option) in packets
- 16 (DHCPv6 only)—(MX Series routers and EX Series switches only) Use DHCPv6 option 16 (Vendor Class Option) in packets
- 60 (DHCPv4 only)—(MX Series routers and EX Series switches only) Use DHCP option 60 (Vendor Class Identifier) in DHCP packets
- 77 (DHCPv4 only)—Use DHCP option 77 (User Class Identifier) in packets

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Using DHCP Option Information to Selectively Process DHCP Client Traffic
- Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 1252
overrides (DHCP Relay Agent)

Syntax

overrides {
  allow-snooped-clients;
  always-write-giaddr;
  always-write-option-82;
  client-discover-match <option60–and-option82>;
  disable-relay;
  interface-client-limit number;
  layer2-unicast-replies;
  no-allow-snooped-clients;
  no-bind-on-request;
  proxy-mode;
  replace-ip-source-with;
  send-release-on-delete;
  trust-option-82;
}

Hierarchy Level

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Override the default configuration settings for the extended DHCP relay agent. Specifying the overrides statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

The following statements are supported at both the [edit ... dhcp-relay] and [edit ... dhcpv6] hierarchy levels. All other statements are supported at the dhcp-relay hierarchy levels only.

- allow-snooped-clients
- interface-client-limit
- no-allow-snooped-clients
- no-bind-on-request
- send-release-on-delete
The remaining statements are explained separately.

<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>interface-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 1267
- dhcp-relay on page 1406
password (DHCP Relay Agent)

Syntax

```
password password-string;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay group group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name forwarding-options dhcpt-relay authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication]
```

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

Description

Configure the password that is sent to the external AAA authentication server for subscriber authentication or client authentication. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options

```
password-string—Authentication password.
```

Required Privilege Level

```
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
```

Related Documentation

- Using External AAA Authentication Services with DHCP on page 1256
- Configuring Passwords for Usernames on page 1276
### preference (Subscriber Management)

**Syntax**

```plaintext
preference route-distance
```

**Hierarchy Level**

```plaintext
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options access route prefix],
[edit dynamic-profiles profile-name routing-instances $junos-routing-instance routing-options rib routing-table-name access route prefix],
[edit dynamic-profiles profile-name routing-options access route prefix]
```

**Release Information**

Statement introduced in Junos OS Release 9.5.

**Description**

Dynamically configure the distance for an access route.

**Options**

- **route-distance**—Either the specific distance you want to assign to the access route or either of the following distance variables:
  - ```$junos-framed-route-distance```—Distance of an IPv4 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-Route attribute [22].
  - ```$junos-framed-route-ipv6-distance```—Distance of an IPv6 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-IPv6-Route attribute [99].

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Dynamic Access Routes for Subscriber Management
prefix (DHCP Relay Agent)

Syntax

```markdown
prefix prefix;
```

Hierarchy Level

- `[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]`
- `[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id]`
- `[edit forwarding-options dhcp-relay relay-option-82 circuit-id]`
- `[edit forwarding-options dhcp-relay group-name relay-option-82 circuit-id]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82 circuit-id]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group-name relay-option-82 circuit-id]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay group-name relay-option-82 circuit-id]`

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Add a prefix to the base option 82 Agent Circuit ID information in DHCP packets destined for a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name. Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.

If you include only the hostname, only the logical system name, or only the routing instance name in the prefix, the format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces with stacked virtual LANs (S-VLANs) is one of the following:

```markdown
host-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

If you include both the logical system name and the routing instance name in the prefix, the format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs is as follows:

```markdown
logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```
**logical-system-name:** routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id

If you include the hostname, logical system name, and routing instance name in the prefix, the format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs is as follows:

```
host-name/logical-system-name:routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

For Fast Ethernet or Gigabit Ethernet interfaces that use virtual LANs (VLANs) but not S-VLANs, only the **vlan-id** value appears in the Agent Circuit ID format. For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs or S-VLANs, neither the **vlan-id** value nor the **svlan-id** value appears.

**Options**  
**prefix**—Any of the following:

- **host-name**—Prepend the hostname of the router configured with the `host-name` statement at the [edit system] hierarchy level to the Agent Circuit ID information.
- **logical-system-name**—Prepend the name of the logical system to the Agent Circuit ID information.
- **routing-instance-name**—Prepend the name of the routing instance to the Agent Circuit ID information.

**Required Privilege Level**  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**  
- Enabling and Disabling Insertion of Option 82 Information on page 1303  
- Configuring an Option 82 Prefix on page 1304  
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 1308
proxy-mode

**Syntax**

proxy-mode;

**Hierarchy Level**

- [edit forwarding-options dhcp-relay overrides],
- [edit forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

**Release Information**

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Enable DHCP relay proxy mode on the extended DHCP relay. Proxy mode supports all extended DHCP relay functionality.

The extended DHCP relay proxy is not supported for the J Series routers DHCP server. Also, you cannot configure both the DHCP relay proxy and the extended DHCP local server on the same interface.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- DHCP Relay Proxy Overview on page 1218
- Extended DHCP Relay Agent Overview on page 1215
- Enabling DHCP Relay Proxy Mode on page 1307
relay-agent-interface-id (DHCPv6 Relay Agent)

Syntax
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}

Hierarchy Level
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...]

Release Information
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description
Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.

The remaining statements are explained separately.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- dhcp-relay on page 1406
- Extended DHCP Relay Agent Overview on page 1215
- DHCPv6 Relay Agent Overview on page 1220
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 1308
relay-agent-remote-id (DHCPv6 Relay Agent)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>relay-agent-remote-id;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include], [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include], [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include]</td>
</tr>
<tr>
<td>Description</td>
<td>Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• DHCPv6 Relay Agent Overview on page 1220  • Creating Unique Usernames for DHCP Clients on page 1276</td>
</tr>
</tbody>
</table>
relay-option (DHCP Relay Agent)

Syntax

```
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}
```

Hierarchy Level
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information
Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description
Configure the extended DHCP relay agent selective processing that is based on DHCP options in DHCP client packets and specify the action to perform on client traffic. You can configure support globally or for a named group of interfaces, and for either DHCP or DHCPv6 relay agent.

The remaining statements are explained separately.

Required Privilege
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

Related Documentation
- Using DHCP Option Information to Selectively Process DHCP Client Traffic
### relay-option-82

#### Syntax
```
relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
}
```

#### Hierarchy Level
- `[edit forwarding-options dhcp-relay]`
- `[edit forwarding-options dhcp-relay group group-name]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name]`
- `[edit logical-systems logical-system-name forwarding-options routing-instance-name forwarding-options dhcp-relay group group-name]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name]`

#### Release Information
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

#### Description
Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

If you enable insertion of option 82 information in DHCP packets, you must specify at least the `circuit-id` statement to include the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option.

You can use the `relay-option-82` statement and its subordinate statements at the `[edit forwarding-options dhcp-relay]` hierarchy level to control insertion of option 82 information globally, or at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level to control insertion of option 82 information for a named group of interfaces.

To restore the default behavior (option 82 information is not inserted into DHCP packets), use the `delete relay-option-82` statement.

The remaining statements are explained separately.

#### Required Privilege Level
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

#### Related Documentation
- Enabling and Disabling Insertion of Option 82 Information on page 1303
- dhcp-relay on page 1406
relay-server-group (DHCP Relay Agent Option)

Syntax
```
relay-server-group relay-server-group;
```

Hierarchy Level
```
[edit forwarding-options dhcp relay relay-option (default-action | equals | starts-with),
 [edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action | equals | starts-with),
 [edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals | starts-with),
 [edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option (default-action | equals | starts-with),
 [edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
 [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
 [edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Release Information
Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Relay DHCP client packets to the specified group of DHCP servers when you use the DHCP relay selective processing feature. You can configure the relay operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.

Options
```
relay-server-group—Name of DHCP server group.
```

Required Privilege Level
```
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.
```

Related Documentation
- Using DHCP Option Information to Selectively Process DHCP Client Traffic
replace-ip-source-with

Syntax

```
replace-ip-source-with giaddr;
```

Hierarchy Level

- [edit forwarding-options dhcp-relay overrides],
- [edit forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name overrides]

Release Information

- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

Required Privilege

- Level interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Extended DHCP Relay Agent Overview on page 1215
- Replacing the DHCP Relay Request and Release Packet Source Address on page 1287
**routing-instance-name (DHCP Relay Agent)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>routing-instance-name;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include], [edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include], [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include], [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include], [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include], [edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include], [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include], [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]</td>
</tr>
</tbody>
</table>

**Release Information**
- Statement introduced in Junos OS Release 9.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
- Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

**Description**
Specify that the routing instance name is concatenated with the username during the subscriber authentication or client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Using External AAA Authentication Services with DHCP on page 1256
- Creating Unique Usernames for DHCP Clients on page 1276
**send-release-on-delete (DHCP Relay Agent)**

**Syntax**
```
send-release-on-delete;
```

**Hierarchy Level**
- [edit forwarding-options dhcp-relay dhcpv6 overrides],
- [edit forwarding-options dhcp-relay overrides],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit forwarding-options dhcp-relay group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group overrides],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name overrides]

**Release Information**
Statement introduced in Junos OS Release 10.2.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

**Description**
Send a release message to the DHCP (or DHCPv6) server whenever DHCP relay or relay proxy deletes a client. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Extended DHCP Relay Agent Overview on page 1215
- Overriding the Default DHCP Relay Configuration Settings on page 1285
- Sending Release Messages When Clients Are Deleted on page 1301
server-group

Syntax

```
server-group {
    server-group-name {
        server-ip-address;
    }
}
```

Hierarchy Level

- [edit forwarding-options dhcp-relay],
- [edit forwarding-options dhcp-relay dhcpv6],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6]

Release Information

Statement introduced in Junos OS Release 8.3.
Support at the [edit... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent. Use the statement at the [edit... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options

- **server-group-name**—Name of the group of DHCP or DHCPv6 server addresses.
- **server-ip-address**—IP address of the DHCP server belonging to this named server group. Use IPv6 addresses when configuring DHCPv6 support. You can configure a maximum of five IP addresses in each named server group.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- dhcp-relay on page 1406
- Extended DHCP Relay Agent Overview on page 1215
- Configuring Server Groups on page 1306
service-profile (DHCP Relay Agent)

Syntax

```
service-profile dynamic-profile-name;
```

Hierarchy Level

- [edit forwarding-options dhcp-relay],
- [edit forwarding-options dhcp-relay dhcpv6],
- [edit forwarding-options dhcp-relay group group-name],
- [edit forwarding-options dhcp-relay group group-name interface interface-name],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name],
- [edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
- [edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit forwarding-options dhcp-relay...] hierarchy levels introduced in Junos OS Release 11.4.

Description

Specify the default subscriber service (or the default DHCP client management service), which is activated when the subscriber (or client) logs in and no other service is activated by a RADIUS server or a provisioning server.

- To specify the default service for all DHCP relay agent clients, include the `service-profile` statement at the [edit forwarding-options dhcp-relay] hierarchy level.
- To specify the default service for a named group of interfaces, include the `service-profile` statement at the [edit forwarding-options dhcp-relay group group-name] hierarchy level.
- To specify the default service for a particular interface within a named group of interfaces, include the `service-profile` statement at the [edit forwarding-options dhcp-relay group group-name interface interface-name] hierarchy level.

Options

- `dynamic-profile-name`—Name of the dynamic profile.

Required Privilege Level

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

Related Documentation

- `dhcp-relay on page 1406`
- `Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces`
- `Grouping Interfaces with Common DHCP Configurations on page 1258`
- `Default Subscriber Service Overview`
- `Configuring a Default Subscriber Service`
session-mode

Syntax  session-mode (automatic | multihop | singlehop);

Hierarchy Level  [edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  Configure the session mode.

Options  automatic—Configure single-hop BFD sessions if the peer is directly connected to the router interface and multihop BFD sessions if the peer is not directly connected to the router interface.

multihop—Configure multihop BFD sessions.

single-hop—Configure single hop BFD sessions.

Required Privilege  Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  •  Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
•  Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
threshold (detection-time)

Syntax
threshold milliseconds;

Hierarchy Level
[edit system services dhcp-local-server liveness-detection method bfd detection-time],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd
detection-time],
[edit forwarding-options dhcp-relay liveness-detection method bfd detection-time],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd detection-time],
[edit system services dhcp-local-server group group-name liveness-detection method bfd
detection-time],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd
detection-time],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd
detection-time],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd
detection-time]

Release Information
Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Specify the threshold for the adaptation of the detection time. When the BFD session
detection time adapts to a value equal to or greater than the threshold, a single trap and
and a single system log message are sent.

NOTE: The threshold time must be greater than or equal to the
minimum-interval or the minimum-receive-interval.

Options
milliseconds—Value for the detection time adaptation threshold.
Range: 1 through 255,000

Required Privilege
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on
  page 1231
• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
threshold (transmit-interval)

Syntax

```
threshold milliseconds;
```

Hierarchy Level

```
[edit system services dhcp-local-server liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server group group-name liveness-detection method bfd transmit-interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd transmit-interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd transmit-interval]
```

Release Information

Statement introduced in Junos OS Release 12.1.

Description

Specify the threshold for detecting the adaptation of the transmit interval. When the BFD session transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.

Options

- `milliseconds` — Threshold value.
- `Range`: 0 through 4,294,967,295 ($2^{32} - 1$)

NOTE: The threshold value specified in the threshold statement must be greater than the value specified in the minimum-interval statement for the transmit-interval statement.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
trace (DHCP Relay Agent)

Syntax

```
trace;
```

Hierarchy Level

- `[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name]`
- `[edit forwarding-options dhcp-relay group group-name interface interface-name]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name]`
- `[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name interface interface-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name]`
- `[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name]`

Release Information

- Statement introduced in Junos OS Release 10.4.
- Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.
- Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Enable trace operations for a group of interfaces or for a specific interface within a group. Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.

Required Privilege

- Interface—To view this statement in the configuration.
- Interface-control—To add this statement to the configuration.

Related Documentation

- Tracing Extended DHCP Operations
- Tracing Extended DHCP Operations for Specific Interfaces
transmit-interval

Syntax  transmit-interval {
  threshold milliseconds;
  minimum-interval milliseconds;
}

Hierarchy Level  [edit system services dhcp-local-server liveness-detection method bfd],
  [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
  [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
  [edit system services dhcp-local-server group group-name liveness-detection method bfd],
  [edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
  [edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
  [edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]

  Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  Configure the Bidirectional Forwarding Detection (BFD) transmit interval.

The remaining statements are explained separately.

Required Privilege Level  routing—To view this statement in the configuration.
  routing-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
  • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
trust-option-82

Syntax  
trust-option-82;

Hierarchy Level  
- [edit forwarding-options dhcp-relay]
- [edit forwarding-options dhcp-relay group group-name]
- [edit logical-systems logical-system-name forwarding-options dhcp-relay]
- [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name]
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay]
- [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name]
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay]
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name]
- [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name interface interface-name]

Release Information  
Statement introduced in Junos OS Release 8.3.  
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  
Enable processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information. By default, the DHCP relay agent treats such packets as if they originated at an untrusted source, and drops them without further processing.

Required Privilege Level  
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation  
- Trusting Option 82 Information on page 1288
- Overriding the Default DHCP Relay Configuration Settings on page 1285
use-interface-description

Syntax

use-interface-description (logical | device);

Hierarchy Level

[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id],
[edit forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit forwarding-options dhcp-relay group group-name relay-option-82 circuit-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82 circuit-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name relay-agent-interface-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82 circuit-id]

Release Information

Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description

Use the textual interface description instead of the interface identifier when creating the agent-circuit-id suboption of the DHCP relay agent option 82. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the interface identifier. The textual description is configured using the description statement at the [edit interfaces interface-name] hierarchy level.

NOTE: By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description is longer than 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.
**Options**

- **logical**—Use the textual description that is configured for the logical interface.
- **device**—Use the textual description that is configured for the device interface.

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- Enabling and Disabling Insertion of Option 82 Information on page 1303
- Using a Textual Description in Option 82 on page 1306
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 1308
**use-primary (DHCP Relay Agent)**

**Syntax**

```
use-primary primary-profile-name;
```

**Hierarchy Level**

```
[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name dynamic-profile profile-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.3.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**

Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.

Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

**Options**

- **primary-profile-name**—Name of the dynamic profile to configure as the primary dynamic profile

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
Related Documentation

• Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

user-prefix (DHCP Relay Agent)

Syntax

user-prefix user-prefix-string;

Hierarchy Level

[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

Description

Specify the user prefix that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.

Options

user-prefix-string—User prefix string.

Required Privilege Level

interface—To view this statement in the configuration.
ininterface-control—To add this statement to the configuration.

Related Documentation

• Using External AAA Authentication Services with DHCP on page 1256
username-include (DHCP Relay Agent)

Syntax
username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-name;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
}

Hierarchy Level
[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit forwarding-options dhcp-relay group group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

Description
Configure the username that the router (or switch) passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS. Use the statement at the [edit...dhcppv6] hierarchy levels to configure DHCPv6 support.

The following statements are not supported in the DHCPv6 hierarchy levels:

- mac-address
- option-60
- option-82

The following statements are supported in the DHCPv6 hierarchy levels only:

- relay-agent-interface-id
- relay-agent-remote-id
- relay-agent-subscriber-id
The remaining statements are explained separately.

**Required Privilege**

- **Level**
  - interface—to view this statement in the configuration.
  - interface-control—to add this statement to the configuration.

**Related Documentation**

- Creating Unique Usernames for DHCP Clients on page 1276
- Using External AAA Authentication Services with DHCP on page 1256

### version (BFD)

**Syntax**

```
version (0 | 1 | automatic);
```

**Hierarchy Level**

```
[edit system services dhcp-local-server liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],
[edit forwarding-options dhcp-relay liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

**Release Information**

- Statement introduced in Junos OS Release 12.1.
- Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Configure the BFD protocol version to detect.

**Options**

- **0**—Use BFD protocol version 0.
- **1**—Use BFD protocol version 1.
- **automatic**—Autodetect the BFD protocol version.

**Default:** automatic

**Required Privilege**

- **Level**
  - routing—to view this statement in the configuration.
  - routing-control—to add this statement to the configuration.

**Related Documentation**

- Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 1231
- Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients
Other Configuration Statements

cache-size

Syntax  cache-size bytes;

Hierarchy Level  [edit security certificates]

Release Information  Statement introduced before Junos OS Release 7.4.
  Statement introduced in Junos OS Release 9.0 for EX Series switches.
  Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  (Encryption interface on M Series and T Series routers and EX Series switches only)
  Configure the cache size for digital certificates.

Options  bytes—Cache size for digital certificates.
  Range:  64 through 4,294,967,295
  Default:  2 megabytes (MB)

NOTE:  We recommend that you limit your cache size to 4 MB.

Required Privilege Level
  admin—To view this statement in the configuration.
  admin-control—To add this statement to the configuration

Related Documentation
  •  Configuring Digital Certificates for an ES PIC
**cache-timeout-negative**

**Syntax**
cache-timeout-negative seconds;

**Hierarchy Level**
[edit security certificates]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
(Encryption interface on M Series and T Series routers and EX Series switches only)
Configure a negative cache for digital certificates.

**Options**
seconds—Negative time to cache digital certificates, in seconds.
Range: 10 through 4,294,967,295
Default: 20

---

**CAUTION:** Configuring a large negative cache value can lead to a denial-of-service attack.

**Required Privilege Level**
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration

**Related Documentation**
• Configuring Digital Certificates for an ES PIC
certificates

**Syntax**

```
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
```

**Hierarchy Level**

[edit security]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

(Encryption interface on M Series and T Series routers and EX Series switches only)

Configure the digital certificates for IPsec.

The remaining statements are explained separately.

**Required Privilege Level**

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Digital Certificates for an ESPIC
certification-authority

Syntax  
certification-authority ca-profile-name {  
  ca-name ca-identity;  
  crl file-name;  
  encoding (binary | pem);  
  enrollment-url url-name;  
  file certificate-filename;  
  ldap-url url-name;  
}

Hierarchy Level  [edit security certificates]

Release Information  Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  (Encryption interface on M Series and T Series routers and EX Series switches only)  
Configure a certificate authority profile name.

  The remaining statements are explained separately.

Required Privilege Level  
admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration

Related Documentation  
  • Configuring Digital Certificates for an ES PIC
## connection-limit

### Syntax

```
connection-limit limit;
```

### Hierarchy Level

- [edit system services finger]
- [edit system services ftp]
- [edit system services netconf ssh]
- [edit system services ssh]
- [edit system services telnet]
- [edit system services xnm-clear-text]
- [edit system services xnm-ssl]

### Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

### Description

Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).

### Options

- **limit**—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).
  - **Range**: 1 through 250
  - **Default**: 75

### Required Privilege

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

### Related Documentation

- Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
- Configuring DTCP-over-SSH Service for the Flow-Tap Application
- Configuring Finger Service for Remote Access to the Router
- Configuring FTP Service for Remote Access to the Router or Switch
- Configuring SSH Service for Remote Access to the Router or Switch
- Configuring Telnet Service for Remote Access to a Router or Switch

---

**NOTE:** The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured connection-limit value if the system resources are limited.
crl (Encryption Interface)

Syntax  
crl file-name;

Hierarchy Level  
[edit security certificates]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
(Encryption interface on M Series and T Series routers and EX Series switches only)  
Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying  
revoked certificates, which is signed by a CA and made available to the participating  
IPsec peers on a regular periodic basis.

Options  
file-name—Specify the file from which to read the CRL.

Required Privilege  
Level  
admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration

Related Documentation  
• Configuring Digital Certificates for an ESPIC

domain-search

Syntax  
domain-search [ domain-list ];

Hierarchy Level  
[edit system],  
[edit system services dhcp],  
[edit system services dhcp],  
[edit system services dhcp pool],  
[edit system services dhcp static-binding]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Configure a list of domains to be searched.

Options  
domain-list—A list of domain names to search. The list can contain up to six domain  
names, with a total of up to 256 characters.

Required Privilege  
Level  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

Related Documentation  
• Configuring the Domains to Search When a Router or Switch Is Included in Multiple  
Domains
• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers
• Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
encoding

Syntax  encoding (binary | pem);

Hierarchy Level  [edit security ike policy ike-peer-address],
                 [edit security certificates certification-authority ca-profile-name]

Release Information  Statement introduced before Junos OS Release 7.4.
                      Statement introduced in Junos OS Release 9.0 for EX Series switches.
                      Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  (Encryption interface on M Series and T Series routers and EX Series switches only)
             Specify the file format used for the local-certificate and local-key-pair
             statements.

Options  binary—Binary file format.
         pem—Privacy-enhanced mail (PEM), an ASCII base 64 encoded format.
         Default: binary

Required Privilege
Level  admin—To view this statement in the configuration.
       admin-control—To add this statement to the configuration.

Related Documentation  • Configuring Digital Certificates for an ES PIC
                       • Configuring an IKE Policy for Digital Certificates for an ES PIC

enrollment-retry

Syntax  enrollment-retry attempts;

Hierarchy Level  [edit security certificates]

Release Information  Statement introduced before Junos OS Release 7.4.
                      Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  (Encryption interface on M Series and T Series routers and EX Series switches only)
             Specify how many times a router or switch can resend a digital certificate request.

Options  attempts—Number of enrollment retries.
         Range: 0 through 100
         Default: 0

Required Privilege
Level  admin—To view this statement in the configuration.
       admin-control—To add this statement to the configuration.

Related Documentation  • Configuring Digital Certificates for an ES PIC
enrollment-url

Syntax enrollment-url url-name;

Hierarchy Level [edit security certificates certification-authority ca-profile-name]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only)
Specify where your router or switch sends Simple Certificate Enrollment Protocol-based
(SCEP-based) certificate enrollment requests (certificate authority URL).

Options url-name—Certificate authority URL.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • Configuring Digital Certificates for an ES PIC
family (for EX Series switches)

Syntax

family ccc on page 1482
family ethernet-switching on page 1482
family inet on page 1482
family inet6 on page 1483
family iso on page 1483
family mpls on page 1483
family ccc

family ethernet-switching {
  filter [input | output] filter-name:
  native-vlan-id vlan-id;
  port-mode mode;
  vlan (802.1Q Tagging) {
    members [ (all | names | vlan-ids)];
  }
}

family inet {
  address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast;
    preferred;
    primary;
    vrrp-group group-id {
      advertise-interval milliseconds;
      preempt | no-preempt {
        hold-time seconds;
      }
      priority number;
      virtual-address [addresses];
      virtual-link-local-address ip-address;
    }
  }
  dhcp {
    client-identifier (ascii ascii | hexadecimal hexadecimal);
    lease-time (seconds | infinite);
    retransmission-attempt number;
    retransmission-interval seconds;
    server-address ip-address;
    update-server;
    vendor-id vendor-id;
  }
  filter [input filter-name;
    output filter-name;
  }
  mtu bytes;
  no-redirects;
  no-neighbor-learn;
  primary;
  rpf-check;
}
targeted-broadcast;
}

family inet6 family inet6 {
  address address {
    eui-64;
    nd6-stale-time seconds;
    ndp ip-address (mac | multicast-mac) mac-address <publish>;
    preferred;
    primary;
    vrrp-inet6-group group-id {
      inet6-advertise-interval milliseconds;
      preempt | preempt {
        hold-time seconds;
      }
      priority number;
      virtual-inet6-address [addresses];
      virtual-link-local-address ipv6~address;
    }
  }
  (dad-disable | no-dad-disable);
  filter {
    input filter-name;
    output filter-name;
  }
  mtu bytes;
  no-neighbor-learn
  rpf-check;
}

family iso family iso {
  address interface-address;
  mtu bytes;
}

family mpls family mpls {
  mtu bytes;
}

Hierarchy Level [edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-range name unit logical-unit-number]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches, including options ethernet-switching, inet, and iso.
Option inet6 introduced in Junos OS Release 9.3 for EX Series switches.
Options ccc and mpls introduced in Junos OS Release 9.5 for EX Series switches.

Description Configure protocol family information for the logical interface on the switch.
You must configure a logical interface to be able to use the physical device.
**Default**  Interfaces on EX2200, EX3200, EX3300, EX4200, and EX4500 switches are set to family ethernet-switching by the default factory configuration. Before you can change the family setting for an interface to another family type, you must delete this default setting or any user-configured family setting. EX6200 and EX8200 switch interfaces do not have a default family setting.

**Options**  See Table 177 on page 1484 for protocol families available on the switch interfaces. Different protocol families support different subsets of the interface types on the switch. Interface types on the switch are:

- Aggregated Ethernet (ae)
- Gigabit Ethernet (ge)
- Interface-range configuration (interface-range)
- Loopback (lo0)
- Management Ethernet (me0)
- Routed VLAN interface (RVI) (vlan)
- Virtual management Ethernet (vme)
- 10-Gigabit Ethernet (xe)

If you are using an interface range, the supported protocol families are the ones supported by the interface types that compose the range.

Not all interface types support all family substatements. Check your switch CLI for supported substatements for a particular protocol family configuration.

### Table 177: Protocol Families and Supported Interface Types

<table>
<thead>
<tr>
<th>Family</th>
<th>Description</th>
<th>Supported Interface Types</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ae</td>
</tr>
<tr>
<td>ccc</td>
<td>Circuit cross-connect protocol family</td>
<td>✓</td>
</tr>
<tr>
<td>ethernet-switching</td>
<td>Ethernet switching protocol family</td>
<td>✓</td>
</tr>
<tr>
<td>inet</td>
<td>IPv4 protocol family</td>
<td>✓</td>
</tr>
<tr>
<td>inet6</td>
<td>IPv6 protocol family</td>
<td>✓</td>
</tr>
<tr>
<td>iso</td>
<td>Junos OS protocol family for IS-IS traffic</td>
<td>✓</td>
</tr>
<tr>
<td>mpls</td>
<td>MPLS protocol family</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Supported on EX8200 switches only

The remaining statements are explained separately.
file

Syntax file certificate-filename;

Hierarchy Level [edit security certificates certification-authority ca-profile-name]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only)
Specify the file from which to read the digital certificate.

Options certificate-filename—File from which to read the digital certificate.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • Configuring Digital Certificates for an ES PIC
ftp

Syntax  ftp {
connection-limit limit;
rate-limit limit;
}

Hierarchy Level  [edit system services]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Allow FTP requests from remote systems to the local router or switch.

Options  The remaining statements are explained separately.

Required Privilege Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  • Configuring FTP Service for Remote Access to the Router or Switch
http

Syntax:

```
http {
  interfaces [ interface-names ];
  port port;
}
```

Hierarchy Level: [edit system services web-management]


Description: Configure the port and interfaces for HTTP service, which is unencrypted.

Options:

```
interfaces [ interface-names ]—Name of one or more interfaces on which to allow the HTTP service. By default, HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.
```

The remaining statement is explained separately.

Required Privilege Level:

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation:

- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 415
- J-Web Interface User Guide
- https on page 1488
- port on page 1500
- web-management on page 1524
https

**Syntax**

```plaintext
https {
    interfaces [ interface-names ];
    local-certificate name;
    port port;
}
```

**Hierarchy Level**

[edit system services web-management]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure the secure version of HTTP (HTTPS) service, which is encrypted.

**Options**

- `interfaces [ interface-names ]`—Name of one or more interfaces on which to allow the HTTPS service. By default, HTTPS access is allowed through any ingress interface, but HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.

- `local-certificate name`—Name of the X.509 certificate for a Secure Sockets Layer (SSL) connection. An SSL connection is configured at the [edit security certificates local] hierarchy.

The remaining statements are explained separately.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Management Access for the EX Series Switch (J-Web Procedure) on page 415
- *J-Web Interface User Guide*
- http on page 1487
- port on page 1500
- web-management on page 1524
ldap-url

Syntax  
<ldap-url url-name>;

Hierarchy Level  
[edit security certificates certification-authority ca-profile-name]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
(Encryption interface on M Series and T Series routers and EX Series switches only) 

Options  
url-name—Name of the LDAP URL.

Required Privilege Level  
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  
• Configuring Digital Certificates for an ES PIC
**lease-time**

**Syntax**  
`lease-time (seconds | infinite);`

**Hierarchy Level**  
`[edit interfaces interface-name unit logical-unit-number family inet dhcp]`

**Release Information**  
Statement introduced in Junos OS Release 8.5 for J Series devices.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 9.2 for SRX Series devices.

**Description**  
Request a specific lease time for the IP address. The lease time is the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server.

**Default**  
If no lease time is requested by client, then the server sends the lease time. The default lease time on a JUNOS OS DHCP server is one day.

**Options**  
- `seconds` — Request a lease time of a specific duration.  
  - **Range:** 60 through 2147483647 seconds
- `infinite` — Request that the lease never expire.

**Required Privilege Level**  
- `interface` — To view this statement in the configuration.  
- `interface-control` — To add this statement to the configuration.

**Related Documentation**  
- Configuring a DHCP Client (CLI Procedure) on page 1249
- Example: Configuring the Device as a DHCP Client
- `interfaces`
- `unit` on page 2458
- `family` on page 1482
load-key-file

Syntax
load-key-file URL filename;

Hierarchy Level
[edit system root-authentication],
[edit system login user {username} authentication]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Load RSA (SSH version 1 and SSH version 2) and DSA or ECDSA (SSH version 2) public keys from a previously-generated named file at a specified URL location. The file contains one or more SSH keys that are copied into the configuration when the command is issued.

Required Privilege
Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
• Configuring the Root Password
• Configuring the Root Password
• Configuring Junos OS User Accounts
• Configuring Junos OS User Accounts
local

Syntax

local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
}

Hierarchy Level
[edit security certificates]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

Options
certificate-name certificate-key-string—String of alphanumeric characters that constitute the private key and certificate.

certificate-name—Name that uniquely identifies the certificate.

load-key-file URL filename—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router’s or switch’s local disk)

- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

Required Privilege Level
system—to view this statement in the configuration.
system-control—to add this statement to the configuration.

Related Documentation
• Importing SSL Certificates for Junos XML Protocol Support
local-certificate

**Syntax**
local-certificate;

**Hierarchy Level**
[edit system services service-deployment],
[edit system services web-management https],
[edit system services xnm-ssl]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Import or reference an SSL certificate.

**Required Privilege Level**
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**
• Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
• Generating SSL Certificates to Be Used for Secure Web Access on page 418
• Importing SSL Certificates for Junos XML Protocol Support

maximum-certificates

**Syntax**
maximum-certificates number;

**Hierarchy Level**
[edit security certificates]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
(Encryption interface on M Series and T Series routers and EX Series switches only)
Configure the maximum number of peer digital certificates to be cached.

**Options**
number—Maximum number of peer digital certificates to be cached.

**Range:** 64 through 4,294,967,295 peer certificates

**Default:** 1024 peer certificates

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
• Configuring Digital Certificates for an ES PIC
**maximum-hop-count**

Syntax  
maximum-hop-count *number*;

Hierarchy Level  
[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootpinterface (interface-name | interface-group)]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

Description  
Specify the maximum number of hops allowed.

Options  
*number*—Maximum number of hops.
Default: 4 hops

Required Privilege Level  
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  
- Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents

**maximum-lease-time (DHCP)**

Syntax  
maximum-lease-time *seconds*;

Hierarchy Level  
[edit system services dhcp],

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.
An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.

Options  
*seconds*—The maximum number of seconds the lease can be held.

Required Privilege Level  
system—To view this statement in the configuration.
system-control—To add this statement to the configuration

Related Documentation  
- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers
- default-lease-time
**minimum-wait-time**

**Syntax**  
minimum-wait-time seconds;

**Hierarchy Level**  
[edit forwarding-options helpers bootp],  
[edit forwarding-options helpers bootpinterface (interface-name | interface-group)]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description**  
Specify the minimum time allowed.

**Options**  
seconds—Minimum time.  
Default: 0 seconds

**Required Privilege Level**  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

**Related Documentation**  
• Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents

**name-server**

**Syntax**  
name-server {  
  address;  
}

**Hierarchy Level**  
[edit system],  
[edit system services dhcp],  
[edit system services dhcp],  
[edit system services dhcp pool],  
[edit system services dhcp static-binding]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Configure one or more Domain Name System (DNS) name servers.

**Options**  
address—Address of the name server. To configure multiple name servers, include a maximum of three address options.

**Required Privilege Level**  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**  
• Configuring a DNS Name Server for Resolving a Hostname into Addresses  
• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers  
• Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
no-listen

**Syntax**

no-listen;

**Hierarchy Level**

[edit forwarding-options helpers bootp interface (interface-name | interface-group)],
[edit forwarding-options helpers domain interface interface-name],
[edit forwarding-options helpers tftp interface interface-name]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.

**Description**

Disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, a router, or a switch.

**Required Privilege**

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring DNS and TFTP Packet Forwarding
- Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents
**outbound-ssh**

**Syntax**

```plaintext
[edit system services]
outbound-ssh {
  client client-id {
    address {
      port port-number;
      retry number;
      timeout seconds;
    }
    device-id device-id;
    keep-alive {
      retry number;
      timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret password;
    services netconf;
  }
  traceoptions {
    file filename <files number> <match regex> <size size> <world-readable |
    no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
```

**Hierarchy Level**

[edit system services]

**Release Information**

Statement introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure a router or switch running the Junos OS behind a firewall to communicate with client management applications on the other side of the firewall.

**Default**

To configure transmission of the router’s or switch’s device ID to the application, include the `device-id` statement at the `[edit system services]` hierarchy level.

**Options**

- **client-id**—Identifies the `outbound-ssh` configuration stanza on the router or switch. Each `outbound-ssh` stanza represents a single outbound SSH connection. This attribute is not sent to the client.

- **device-id**—Identifies the router or switch to the client during the initiation sequence.

- **keep-alive**—(Optional) When configured, specifies that the router or switch send keepalive messages to the management server. To configure the keepalive message, you must set both the `timeout` and `retry` attributes.

- **reconnect-strategy**—(Optional) Specify the method the router or switch uses to reestablish a disconnected outbound SSH connection. Two methods are available:
• **in-order**—Specify that the router or switch first attempt to establish an outbound SSH session based on the management server address list. The router or switch attempts to establish a session with the first server on the list. If this connection is not available, the router or switch attempts to establish a session with the next server, and so on down the list until a connection is established.

• **sticky**—Specify that the router or switch first attempt to reconnect to the management server that it was last connected to. If the connection is unavailable, it attempts to establish a connection with the next client on the list and so forth until a connection is made.

**retry**—Number of keepalive messages the router or switch sends without receiving a response from the client before the current SSH connection is disconnected. The default is three messages.

**secret**—(Optional) Router's or switch's public SSH host key. If added to the `outbound-ssh` statement, during the initialization of the outbound SSH service, the router or switch passes its public key to the management server. This is the recommended method of maintaining a current copy of the router's or switch's public key.

**timeout**—Length of time that the Junos server waits for data before sending a keep alive signal. The default is 15 seconds.

When reconnecting to a client, the router or switch attempts to reconnect to the client based on the **retry** and **timeout** values for each client listed.

**address**—Hostname or the IPv4 address of the NSM application server. You can list multiple clients by adding each client's IP address or hostname along with the following connection parameters:

• **port**—Outbound SSH port for the client. The default is port 22.

• **retry**—Number of times the router or switch attempts to establish an outbound SSH connection before giving up. The default is three tries.

• **timeout**—Length of time that the router or switch attempts to establish an outbound SSH connection before giving up. The default is fifteen seconds.

**filename**—(Optional) By default, the filename of the log file used to record the trace options is the name of the traced process (for example, `mib2d` or `snmpd`). Use this option to override the default value.

**files**—(Optional) Maximum number of trace files generated. By default, the maximum number of trace files is 10. Use this option to override the default value.

When a trace file reaches its maximum size, the system archives the file and starts a new file. The system archives trace files by appending a number to the filename in sequential order from 1 to the maximum value (specified by the default value or the options value set here). Once the maximum value is reached, the numbering sequence is restarted at 1, overwriting the older file.
size—(Optional) Maximum size of the trace file in kilobytes (KB). Once the maximum file size is reached, the system archives the file. The default value is 1000 KB. Use this option to override the default value.

match—(Optional) When used, the system only adds lines to the trace file that match the regular expression specified. For example, if the match value is set to =error, the system only records lines to the trace file that include the string error.

services—Services available for the session. Currently, NETCONF is the only service available.

world-readable | no-world-readable—(Optional) Whether the files are accessible by the originator of the trace operation only or by any user. By default, log files are only accessible by the user that started the trace operation (no-world-readable).

all | configuration | connectivity—(Optional) Type of tracing operation to perform.

all—Log all events.

configuration—Log all events pertaining to the configuration of the router or switch.

connectivity—Log all events pertaining to the establishment of a connection between the client server and the router or switch.

no-remote-trace—(Optional) Disable remote tracing.

**Required Privilege**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Outbound SSH Service
- System Management Configuration Statements
**path-length**

**Syntax**

```
path-length certificate-path-length;
```

**Hierarchy Level**

```
[edit security certificates]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

(Encryption interface on M Series and T Series routers and EX Series switches only)
Configure the digital certificate path length.

**Options**

- `certificate-path-length`—Digital certificate path length.
  - **Range:** 2 through 15 certificates
  - **Default:** 15 certificates

**Required Privilege**

- `admin`—To view this statement in the configuration.
- `admin-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring Digital Certificates for an ESPIC](http://link)

---

**port (HTTP/HTTPS)**

**Syntax**

```
port port-number;
```

**Hierarchy Level**

```
[edit system services web-management]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure the port on which the HTTP or HTTPS service is connected.

**Options**

- `port-number`—The TCP port number on which the specified service listens.

**Required Privilege**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- [Table 82 on page 416](http://link)
- [J-Web Interface User Guide](http://link)
- [http on page 1487](http://link)
- [https on page 1488](http://link)
- [web-management on page 1524](http://link)
port (SRC Server)

**Syntax**
```
port port-number;
```

**Hierarchy Level**
```
[edit system services service-deployment servers server-address]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the port number on which to contact the SRC server.

**Options**
- `port-number`—(Optional) The TCP port number for the SRC server.
  - Default: 3333

**Required Privilege**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring the Junos OS to Work with SRC Software

process-inform

**Syntax**
```
process-inform {
  pool pool-name network address-range
}
```

**Hierarchy Level**
```
[edit system services dhcp-local-server overrides]
```

**Release Information**
Statement introduced in Junos OS Release 12.1 for EX Series switches.

**Description**
For extended Dynamic Host Configuration Protocol (DHCP) servers, enable the processing of DHCP information request messages sent from the client to the server to request DHCP options. The messages are also passed to the configured server list.

**Default**
Information request messages are not processed.

**Required Privilege**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
**protocol-version**

**Syntax**  
protocol-version version;

**Hierarchy Level**  
[edit system services ssh]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**  
Specify the secure shell (SSH) protocol version.

**Default**  
v2—SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.

**Options**  
version—SSH protocol version: v1, v2, or both.

**Required Privilege Level**  
admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration.

**Related Documentation**  
- Configuring SSH Service for Remote Access to the Router or Switch
rate-limit

Syntax
rate-limit limit;

Hierarchy Level
[edit system services finger],
[edit system services ftp],
[edit system services netconf ssh],
[edit system services ssh],
[edit system services telnet],
[edit system services xnm-clear-text],
[edit system services xnm-ssl]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure the maximum number of connections attempts per protocol (either IPv6 or IPv4) on an access service.

Default
150 connections

Options
rate-limit limit—(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6).
Range: 1 through 250
Default: 150

Required Privilege
system—To view this statement in the configuration.

Level
system-control—To add this statement to the configuration.

Related Documentation
• Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
reconfigure

Syntax reconfigure {
  attempts attempts;
  clear-on-abort;
  timeout interval;
  token token;
}

Hierarchy Level [edit system services dhcp-local-server ]

Release Information Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description For extended Dynamic Host Configuration Protocol (DHCP) servers, enable dynamic reconfiguration triggered by the server of all DHCP clients.

Options attempts—Number of attempts made to reconfigure all DHCP clients.

  clear-on-abort—Delete all DHCP clients when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success.

  timeout interval—Initial value (in seconds) between attempts to reconfigure all DHCP clients. Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

  token—Configure a plain-text token for all DHCP clients. The token enables rudimentary entity authentication to protect against inadvertently instantiated DHCP servers. A null token (empty string) indicates that the configuration token functionality is not enabled.

Required Privilege Level system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation • Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
retransmission-attempt

Syntax retransmission-attempt number;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet dhcp]


Description Specify the number of times the device retransmits a Dynamic Host Control Protocol (DHCP) packet if a DHCP server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

Options number—Number of retransmit attempts.
  Range: 0 through 6
  Default: 4

Required Privilege Level interface—To view this statement in the configuration.
  interface-control—To add this statement to the configuration.

Related Documentation • Configuring a DHCP Client (CLI Procedure) on page 1249
  • Example: Configuring the Device as a DHCP Client
  • interfaces
  • unit on page 2458
  • family on page 1482
retransmission-interval

Syntax   retransmission-interval seconds;

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number family inet dhcp]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify the time between successive retransmissions of the client DHCP request if a DHCP server fails to respond.

Options  seconds—Number of seconds between successive retransmissions.
           Range: 4 through 64 seconds
           Default: 4 seconds

Required Privilege Level  interface—To view this statement in the configuration.
                         interface-control—To add this statement to the configuration.

Related Documentation  • Configuring a DHCP Client (CLI Procedure) on page 1249

server (DNS and TFTP Service)

Syntax   server address <logical-system logical-system-name> <routing-instance routing-instance-name>;

Hierarchy Level  [edit forwarding-options helpers domain],
                 [edit forwarding-options helpers domain interface interface-name],
                 [edit forwarding-options helpers tftp],
                 [edit forwarding-options helpers tftp interface interface-name]

Release Information  Statement introduced before Junos OS Release 7.4.
                     Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify the DNS or TFTP server for forwarding DNS or TFTP requests. Only one server can be specified for each interface.

Options  address—Address of the server.
          logical-system logical-system-name—(Optional) Logical system of the server.
          routing-instance [ routing-instance-names ]—(Optional) Set the routing instance name or names that belong to the DNS server or TFTP server.

Required Privilege Level  interface—To view this statement in the configuration.
                         interface-control—To add this statement to the configuration.

Related Documentation  • Configuring DNS and TFTP Packet Forwarding
server-address

Syntax server-address ip-address;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family inet dhcp]

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 9.2 for SRX Series devices.

Description Specify the address of the DHCP server that the client should accept DHCP offers from.
If this option is included in the DHCP configuration, the client accepts offers only from
this server and ignores all other offers.

Default The client accepts the first offer it receives from any DHCP server.

Options ip-address—DHCP server address.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring a DHCP Client (CLI Procedure) on page 1249
- Example: Configuring the Device as a DHCP Client
- interfaces
- unit on page 2458
- family on page 1482
server-identifier

Syntax  
server-identifier address;

Hierarchy Level  
[edit system services dhcp],  
[edit system services dhcp pool],  
[edit system services dhcp static-binding]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
For J Series Services Routers and EX Series switches only. Configure a server identifier.  
The identifier can be used to identify a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).

Servers include the server identifier in DHCP OFFER messages so that clients can distinguish between multiple lease offers. Clients include the server identifier in DHCP REQUEST messages to select a lease and indicate which offer is accepted from multiple lease offers. Also, clients can use the server identifier to send unicast request messages to specific DHCP servers to renew a current lease.

This address must be a manually assigned, static IP address. The server cannot send a request and receive an IP address from itself or another DHCP server.

Default  
If no server identifier is set, the DHCP server sets the server identifier based on the primary interface address used by the server to receive a client request. For example, if the client sends a DHCP request and the server receives it on fe-0/0/0 and the primary interface address is 1.1.1.1, then the server identifier is set to 1.1.1.1.

Options  
address—IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

Required Privilege Level  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

Related Documentation  
• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers
servers

Syntax
servers server-address {
    port port-number;
}

Hierarchy Level
[edit system services service-deployment]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure an IPv4 address for the Session and Resource Control (SRC) server.

Options
server-address—The TCP port number.
Default: 3333

The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Work with SRC Software

service-deployment

Syntax
service-deployment {
    servers server-address {
        port port-number;
    };
    source-address source-address;
}

Hierarchy Level
[edit system services]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Configuring the Junos OS to Work with SRC Software
services (System Services)

Syntax

```
services {
    dhcp { /* DHCP not supported on a DCF */
        dhcp_services;
    }
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    ftp {
        connection-limit limit;
        rate-limit limit;
    }
    service-deployment {
        servers address {
            port-number port-number;
        }
        source-address address;
    }
    ssh {
        connection-limit limit;
        protocol-version [v1 v2];
        rate-limit limit;
        root-login (allow | deny | deny-password);
    }
    telnet {
        connection-limit limit;
        rate-limit limit;
    }
    web-management {
        http {
            interfaces [ names ];
            port port;
        }
        https {
            interfaces [ names ];
            local-certificate name;
            port port;
        }
        session {
            idle-timeout [ minutes ];
            session-limit [ limit ];
        }
    }
    xnm-clear-text {
        connection-limit limit;
        rate-limit limit;
    }
    xnm-ssl {
        connection-limit limit;
        local-certificate name;
        rate-limit limit;
    }
}
```
Hierarchy Level  [edit system]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, finger, rlogin, SSH, telnet, Web management, Junos XML protocol clear-text, Junos XML protocol SSL, and network utilities or enable Junos OS to work with the Session and Resource Control (SRC) software.

The remaining statements are explained separately.

Required Privilege  system—To view this statement in the configuration.
Level  system-control—To add this statement to the configuration.

Related Documentation  • Configuring clear-text or SSL Service for Junos XML Protocol Client Applications
• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers
• Configuring the Junos OS to Work with SRC Software
session (Time-out)

Syntax

```
session {
    idle-timeout minutes;
    session-limit session-limit;
}
```

Hierarchy Level [edit system services web-management]

Release Information Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions.

Options

- **idle-timeout minutes**—Configure the number of minutes a session can be idle before it times out.
  - Range: 1 through 1440
  - Default: 1440

- **session-limit session-limit**—Configure the maximum number of simultaneous J-Web user login sessions.
  - Range: 1 through 1024
  - Default: Unlimited

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- J-Web Interface User Guide
### sip-server

**Syntax**

```
sip-server [address | name];
```

**Hierarchy Level**

```
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

**Release Information**

Statement introduced in Junos OS Release 10.1 for EX Series switches.

**Description**

Configure Session Initiation Protocol (SIP) server addresses or names for DHCP servers.

**Options**

- **address**—IPv4 address of the SIP server. To configure multiple SIP servers, include multiple `address` options. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

- **name**—Fully qualified domain name of the SIP server. To configure multiple SIP servers, include multiple `name` options. This domain name must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).

**Required Privilege**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring a DHCP SIP Server (CLI Procedure) on page 1248
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250

### source-address (SRC Software)

**Syntax**

```
source-address source-address;
```

**Hierarchy Level**

```
[edit system services service-deployment]
```

**Release Information**


**Description**

Enable Junos OS to work with the Session and Resource Control (SRC) software.

**Options**

- **source-address**—Local IPv4 address to be used as source address for traffic to the SRC server. The source address restricts traffic within the out-of-band network.

**Required Privilege**

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring the Junos OS to Work with SRC Software
source-address-giaddr

**Syntax**

source-address-giaddr;

**Hierarchy Level**

[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface interface-name]

**Release Information**

Statement introduced in Junos OS Release 10.1 for EX Series switches.

**Description**

Configure the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent.

When this statement is entered in the [edit forwarding-options helpers bootp] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting all interfaces on the switch.

When this statement is entered in the [edit forwarding-options helpers bootp interface interface-name] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting the specified interface of the switch.

In Junos OS Release 10.1 for EX Series switches and later releases, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is used as the source IP address for relayed DHCP packets by default.

In Junos OS Releases 9.6 and 10.0 for EX Series switches, the gateway IP address of the switch is always used as the source IP address for relayed DHCP packets when the switch is used as the DHCP relay agent.

In Junos OS Releases 9.3 through 9.5 for EX Series switches, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is always used as the source IP address for relayed DHCP packets.

**Required Privilege Level**

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

**Related Documentation**

• DHCP/BOOTP Relay for Switches Overview
ssh

Syntax

```plaintext
ssh {
    ciphers [ cipher-1 cipher-2 cipher-3 ...];
    client-alive-count-max seconds;
    client-alive-interval seconds;
    connection-limit limit;
    hostkey-algorithm <algorithm|no-algorithm>;
    key-exchange <algorithm>;
    macs <algorithm>;
    max-sessions-per-connection <number>;
    no-tcp-forwarding;
    protocol-version [v1 v2];
    rate-limit limit;
    root-login (allow | deny | deny-password);
}
```

Hierarchy Level  [edit system services]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
`client-alive-interval` and `client-alive-max-count` statements introduced in Junos OS Release 12.2.

Description

Allow SSH requests from remote systems to the local router or switch.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Configuring SSH Service for Remote Access to the Router or Switch
static-binding

**Syntax**

    static-binding mac-address {
        client-identifier (ascii client-id | hexadecimal client-id);
        fixed-address {
            address;
        }
        host-name client-hostname;
    }

**Hierarchy Level**

[edit system services dhcp],
[edit system services dhcp]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

For J Series Services routers and EX Series switches only. Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address or client identifier.

**Options**

- **mac-address**—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.
- **fixed-address address**—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.
- **host-name client-hostname**—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the `domain-name` statement.
- **client-identifier (ascii client-id | hexadecimal client-id)**—Used by the DHCP server to index the database of address bindings. The client identifier is an ASCII string or hexadecimal number and can include a type-value pair as specified in RFC 1700, Assigned Numbers. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

**Required Privilege Level**

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers
- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
**system-generated-certificate**

**Syntax**
```
system-generated-certificate;
```

**Hierarchy Level**
```
[edit system services web-management https]
```

**Release Information**
Command introduced in Junos OS Release 11.1 for EX Series switches.

**Description**
Configure the automatically generated self-signed certificate for enabling HTTPS services.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure) on page 1253

---

**telnet**

**Syntax**
```
telnet {
    connection-limit limit;
    rate-limit limit;
}
```

**Hierarchy Level**
```
[edit system services]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Provide Telnet connections from remote systems to the local router or switch.

The remaining statements are explained separately.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Telnet Service for Remote Access to a Router or Switch
tftp

Syntax  
```plaintext
tftp {
    description text-description;
    interface interface-name {
        broadcast;
        description text-description;
        no-listen;
        server address <logical-system logical-system-name> <routing-instance routing-instance-name>;
    }
    server address <logical-system logical-system-name> <routing-instance routing-instance-name>;
}
```

Hierarchy Level  
[edit forwarding-options helpers]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Enable TFTP request packet forwarding.

The remaining statements are explained separately.

Required Privilege  
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation  
- Configuring DNS and TFTP Packet Forwarding
traceoptions (DNS and TFTP Packet Forwarding)

**Syntax**

traceoptions {
    file filename <files number> <match regular-expression> <size bytes> <world-readable | no-world-readable>;
    flag flag;
    level level;
    <no-remote-trace>;
}

**Hierarchy Level**

[edit forwarding-options helpers]

**Release Information**


**Description**

Configure tracing operations for BOOTP, DNS and TFTP packet forwarding.

**Default**

If you do not include this statement, no tracing operations are performed.

**Options**

- **file filename**—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named `fud` in the directory `/var/log`. If you include the file statement, you must specify a filename.

- **files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

  **Range**: 2 through 1000

  **Default**: 3 files

- **flag flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

  - **address**—Trace address management events
  - **all**—Trace all events
  - **bootp**—Trace BOOTP or DHCP services events
  - **config**—Trace configuration events
  - **domain**—Trace DNS service events
  - **ifdb**—Trace interface database operations
  - **io**—Trace I/O operations
  - **main**—Trace main loop events
  - **port**—Trace arbitrary protocol events
- rtsock—Trace routing socket operations
- tftp—Trace TFTP service events
- trace—Trace tracing operations
- ui—Trace user interface operations
- util—Trace miscellaneous utility operations

match regular-expression—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing globally or for a specific tracing operation.

no-world-readable—(Optional) Restrict file access to the owner.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

Syntax: \x k to specify KB, \x m to specify MB, or \x g to specify GB
Range: 0 bytes through 4,294,967,295 KB
Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation
- Tracing BOOTP, DNS, and TFTP Forwarding Operations
traceoptions

Syntax

traceoptions {
  file filename <files number> <size size>
  flag all;
  flag certificates;
  flag database;
  flag general;
  flag like;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
  level
  no-remote-trace
}

Hierarchy Level

[edit security],
[edit services ipsec-vpn]

Trace options can be configured at either the [edit security] or the [edit services ipsec-vpn] hierarchy level, but not at both levels.

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure security trace options.

To specify more than one trace option, include multiple flag statements. Trace option output is recorded in the /var/log/kmd file.

NOTE: The traceoptions statement is not supported on QFabric systems.

Options

files number—(Optional) Maximum number of trace files. When a trace file (for example, kmd) reaches its maximum size, it is renamed kmd.0, then kmd.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Range: 2 through 1000 files

Default: 0 files

size size—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, kmd) reaches this size, it is renamed, kmd.0, then kmd.1 and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Default: 1024 KB
flag flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements.

- all—Trace all security events.
- certificates—Trace certificate events.
- database—Trace database events.
- general—Trace general events.
- ike—Trace IKE module processing.
- parse—Trace configuration processing.
- policy-manager—Trace policy manager processing.
- routing-socket—Trace routing socket messages.
- timer—Trace internal timer events.

level level—(Optional) Set traceoptions level.

- all—match all levels.
- error—Match error conditions.
- info—Match informational messages.
- notice—Match conditions that should be handled specially.
- verbose—Match verbose messages.
- warning—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing

**Required Privilege**
- **Level**
  - admin—To view the configuration.
  - admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Tracing Operations for Security Services
**update-server**

**Syntax**
update-server;

**Hierarchy Level**
[edit interfaces interface-name unit logical-unit-number inet dhcp]

**Release Information**
- Statement introduced in Junos OS Release 8.5 for J Series devices.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 9.2 for SRX Series devices.

**Description**
Propagate TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch, router, or device.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring a DHCP Client (CLI Procedure) on page 1249
- Example: Configuring the Device as a DHCP Client
  - interfaces
  - unit on page 2458
  - family on page 1482
web-management

Syntax
web-management {
  http {
    interfaces [ interface-names ];
    port port;
  }
  https {
    interfaces [ interface-names ];
    local-certificate name;
    port port;
  }
}

Hierarchy Level [edit system services]


Description Configure settings for HTTP or HTTPS access. HTTP access allows management of the router or switch using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router or switch using the J-Web interface. With HTTPS access, communication between the router or switch Web server and your browser is encrypted.

The remaining statements are explained separately.

Required Privilege Level
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation
- Table 82 on page 416
- J-Web Interface User Guide
- http on page 1487
- https on page 1488
- port on page 1500
wins-server (System)

Syntax
wins-server {
    address;
}

Hierarchy Level
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
For J Series Services Routers and EX Series switches only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as 192.168.1.3) to Windows NetBIOS names (such as \Marketing). List servers in order of preference.

Options
address—IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple address options.

Required Privilege
Level
system—to view this statement in the configuration.
system-control—to add this statement to the configuration.

Related Documentation
• Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers
• Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
CHAPTER 27

Administration

- Routine Monitoring on page 1527
- Verifying and Managing DHCP Local Server Configurations on page 1531
- Verifying and Managing DHCP Relay Agent Configurations on page 1532
- DHCP Local Server Monitoring Commands on page 1533
- DHCP Relay Agent Monitoring Commands on page 1567
- Other Operational Commands on page 1621

Routine Monitoring

- Monitoring DHCP Services on page 1527

Monitoring DHCP Services

**Purpose** A switch or router can operate as a DHCP server. Use the monitoring functionality to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

**Action** To monitor the DHCP server in the J-Web interface, select *Monitor > Services > DHCP.*

To monitor the DHCP server in the CLI, enter the following CLI commands:

- `show system services dhcp binding`
- `show system services dhcp conflict`
- `show system services dhcp pool`
- `show system services dhcp statistics`
- `show system services dhcp relay-statistics`
- `show system services dhcp global`
- `show system services dhcp client`
- `clear system services dhcp binding`
- `clear system services dhcp conflict`
- `clear system services dhcp statistics`
- `clear dhcp relay-statistics`
On EX4300 switches, to monitor the DHCP server in the CLI, enter the following CLI commands:

- show dhcp server binding
- show dhcp server statistics
- show dhcp relay binding
- show dhcp relay statistics
- clear dhcp server binding
- clear dhcp server statistics
- clear dhcp relay binding
- clear dhcp relay statistics

**Meaning**

Table 178 on page 1528 summarizes the output fields in DHCP displays in the J-Web interface.

### Table 178: Summary of DHCP Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>This column displays the following information:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Boot lease length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Domain Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Name servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Server identifier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Domain search</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Gateway routers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• WINS server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Boot file</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Boot server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default lease time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Minimum lease time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Maximum lease time</td>
<td></td>
</tr>
<tr>
<td>Value</td>
<td>Displays the value for each of the parameters in the Name column.</td>
<td></td>
</tr>
</tbody>
</table>

**Bindings tab**

<table>
<thead>
<tr>
<th>Allocated Address</th>
<th>List of IP addresses the DHCP server has assigned to clients.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Corresponding media access control (MAC) address of the client.</td>
<td></td>
</tr>
</tbody>
</table>
DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding Type</td>
<td>Type of binding assigned to the client: <strong>dynamic</strong> or <strong>static</strong></td>
<td>DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Date and time the lease expires, or <strong>never</strong> for leases that do not expire.</td>
<td></td>
</tr>
<tr>
<td>Pools tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pool Name</td>
<td>Subnet on which the IP address pool is defined.</td>
<td></td>
</tr>
<tr>
<td>Low Address</td>
<td>Lowest address in the IP address pool.</td>
<td></td>
</tr>
<tr>
<td>High Address</td>
<td>Highest address in the IP address pool.</td>
<td></td>
</tr>
<tr>
<td>Excluded Addresses</td>
<td>Addresses excluded from the address pool.</td>
<td></td>
</tr>
<tr>
<td>Clients tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface Name</td>
<td>Name of the logical interface.</td>
<td></td>
</tr>
<tr>
<td>Hardware Address</td>
<td>Vendor identification.</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>State of the client binding.</td>
<td></td>
</tr>
<tr>
<td>Address Obtained</td>
<td>IP address obtained from the DHCP server.</td>
<td></td>
</tr>
<tr>
<td>Update Server</td>
<td>Indicates whether server update is enabled.</td>
<td></td>
</tr>
<tr>
<td>Lease Obtained</td>
<td>Date and time the lease was obtained.</td>
<td></td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Date and time the lease expires.</td>
<td></td>
</tr>
<tr>
<td>Renew</td>
<td>Reacquires an IP address from the server for the interface. When you click this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.</td>
<td></td>
</tr>
</tbody>
</table>
Table 178: Summary of DHCP Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicts tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection Time</td>
<td>Date and time the client detected the conflict.</td>
<td></td>
</tr>
<tr>
<td>Detection Method</td>
<td>How the conflict was detected.</td>
<td>Only client-detected conflicts are displayed.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address where the conflict occurs.</td>
<td>The addresses in the conflicts list remain excluded until you use the <code>clear system services dhcp conflict</code> command to manually clear the list.</td>
</tr>
</tbody>
</table>

DHCP Statistics

<table>
<thead>
<tr>
<th>Relay Statistics tab</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Counters</td>
<td>Displays the number of packet counters.</td>
<td></td>
</tr>
<tr>
<td>Dropped Packet Counters</td>
<td>Graphically displays the number of dropped packet counters.</td>
<td></td>
</tr>
</tbody>
</table>

Statistics tab

<table>
<thead>
<tr>
<th>Packets dropped</th>
<th>Total number of packets dropped and the number of packets dropped due to a particular condition.</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages received</td>
<td>Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, and DHCPREQUEST messages sent from DHCP clients and received by the DHCP server.</td>
<td></td>
</tr>
<tr>
<td>Messages sent</td>
<td>Number of BOOTREPLY, DHCPACK, DHCPOFFER, DHCPNAK, and DHCPFORCERENEW messages sent from the DHCP server to DHCP clients.</td>
<td></td>
</tr>
</tbody>
</table>

Table 179 on page 1530 summarizes the output fields in DHCP displays in EX4300 switches in the J-Web interface.

Table 179: Summary of DHCP Output Fields for EX4300 Switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding Information tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the DHCP client.</td>
<td></td>
</tr>
<tr>
<td>Session ID</td>
<td>Session ID of the subscriber session.</td>
<td></td>
</tr>
<tr>
<td>Hardware Address</td>
<td>Hardware address of the DHCP client.</td>
<td></td>
</tr>
</tbody>
</table>
Table 179: Summary of DHCP Output Fields for EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expires</td>
<td>Number of seconds in which the lease expires.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>State of the address binding table on the extended DHCP local server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BOUND—Client has an active IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FORCERENEW—Client has received the FORCERENEW message from the server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• INIT—Initial state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RELEASE—Client is releasing the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RENEWING—Client is sending a request to renew the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• REQUESTING—Client is requesting a DHCP server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SELECTING—Client is receiving offers from DHCP servers.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the request was received.</td>
<td></td>
</tr>
</tbody>
</table>

Table 180 on page 1531 summarizes the output fields in DHCP Statistics Information for EX4300 switches in the J-Web interface.

Table 180: Summary of the DHCP Statistics Information Output for EX4300 switches

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Counters</td>
<td>Graphically displays the number of messages sent and received.</td>
<td></td>
</tr>
<tr>
<td>Dropped packet Counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Limit</td>
<td>Graphically displays the number of dropped packet counters.</td>
<td></td>
</tr>
</tbody>
</table>

Related Documentation

- Configuring DHCP Services (J-Web Procedure) on page 1241
- Understanding DHCP Services for Switches

Verifying and Managing DHCP Local Server Configurations

- Verifying and Managing DHCP Local Server Configuration on page 1532
- Verifying and Managing DHCPv6 Local Server Configuration on page 1532
Verifying and Managing DHCP Local Server Configuration

**Purpose**  View or clear information about client address bindings and statistics for the extended DHCP local server.

**Action**  
- To display the address bindings in the client table on the extended DHCP local server:
  ```
  user@host> show dhcp server binding routing-instance customer routing instance
  ```
- To display extended DHCP local server statistics:
  ```
  user@host> show dhcp server statistics routing-instance customer routing instance
  ```
- To clear the binding state of a DHCP client from the client table on the extended DHCP local server:
  ```
  user@host> clear dhcp server binding routing-instance customer routing instance
  ```
- To clear all extended DHCP local server statistics:
  ```
  user@host> clear dhcp server statistics routing-instance customer routing instance
  ```

**Related Documentation**  
- Junos OS Operational Mode Commands

---

Verifying and Managing DHCPv6 Local Server Configuration

**Purpose**  View or clear information about client address bindings and statistics for the DHCPv6 local server.

**Action**  
- To display the address bindings in the client table on the DHCPv6 local server:
  ```
  user@host> show dhcpv6 server binding
  ```
- To display DHCPv6 local server statistics:
  ```
  user@host> show dhcpv6 server statistics
  ```
- To clear all DHCPv6 local server statistics:
  ```
  user@host> clear dhcpv6 server binding
  ```
- To clear all DHCPv6 local server statistics:
  ```
  user@host> clear dhcpv6 server statistics
  ```

**Related Documentation**  
- Junos OS Operational Mode Commands

---

Verifying and Managing DHCP Relay Agent Configurations

- Verifying and Managing DHCP Relay Configuration on page 1532
- Verifying and Managing DHCPv6 Relay Configuration on page 1533

Verifying and Managing DHCP Relay Configuration

**Purpose**  View or clear address bindings or statistics for extended DHCP relay agent clients:
### Action
- To display the address bindings for extended DHCP relay agent clients:
  ```
  user@host> show dhcp relay binding routing-instance customer routing instance
  ```
- To display extended DHCP relay agent statistics:
  ```
  user@host> show dhcp relay statistics routing-instance customer routing instance
  ```
- To clear the binding state of DHCP relay agent clients:
  ```
  user@host> clear dhcp relay binding routing-instance customer routing instance
  ```
- To clear all extended DHCP relay agent statistics:
  ```
  user@host> clear dhcp relay statistics routing-instance customer routing instance
  ```

### Related Documentation
- Junos OS Operational Mode Commands

### Verifying and Managing DHCPv6 Relay Configuration

#### Purpose
View or clear address bindings or statistics for extended DHCPv6 relay agent clients:

#### Action
- To display the address bindings for extended DHCPv6 relay agent clients:
  ```
  user@host> show dhcpv6 relay binding
  ```
- To display extended DHCPv6 relay agent statistics:
  ```
  user@host> show dhcpv6 relay statistics
  ```
- To clear the binding state of DHCPv6 relay agent clients:
  ```
  user@host> clear dhcpv6 relay binding
  ```
- To clear all extended DHCPv6 relay agent statistics:
  ```
  user@host> clear dhcpv6 relay statistics
  ```

#### Related Documentation
- Junos OS Operational Mode Commands

### DHCP Local Server Monitoring Commands
clear dhcp server binding

Syntax  
```
<address>
<all>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information  

Description  
Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the extended DHCP local server.

Options  
- **address**—(Optional) Clear the binding state for the DHCP client, using one of the following entries:
  - `ip-address`—The specified IP address.
  - `mac-address`—The specified MAC address.
  - `session-id`—The specified session ID.

- **all**—(Optional) Clear the binding state for all DHCP clients.

- **interface interface-name**—(Optional) Clear the binding state for DHCP clients on the specified interface.

  **NOTE:** This option clears all bindings whose initial login requests were received over the specified interface. Dynamic demux login requests are not received over the dynamic demux interface, but rather the underlying interface of the dynamic demux interface. To clear a specific dynamic demux interface, use the `ip-address` or `mac-address` options.

- **interfaces-vlan**—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

- **interfaces-wildcard**—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).

- **logical-system logical-system-name**—(Optional) Clear the binding state for DHCP clients on the specified logical system.

- **routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCP clients on the specified routing instance.
Required Privilege Level

Related Documentation

List of Sample Output

Output Fields

Sample Output

clear dhcp server binding <ip-address>

The following sample output displays the address bindings in the DHCP client table on the extended DHCP local server before and after the `clear dhcp server binding` command is issued.

```
user@host> show dhcp server binding
2 clients, (0 bound, 0 selecting, 0 renewing, 0 rebinding)

IP address       Hardware address   Type     Lease expires at
100.20.32.1      90:00:00:01:00:01  active   2007-01-17 11:38:47 PST
100.20.32.3      90:00:00:02:00:01  active   2007-01-17 11:38:41 PST

user@host> clear dhcp server binding 10.20.32.1
user@host> show dhcp server binding
1 clients, (0 bound, 0 selecting, 0 renewing, 0 rebinding)

IP address       Hardware address   Type     Lease expires at
100.20.32.3      90:00:00:02:00:01  active   2007-01-17 11:38:41 PST
```

clear dhcp server binding all

The following command clears all DHCP local server bindings:

```
user@host> clear dhcp server binding all
```

clear dhcp server binding interface

The following command clears DHCP local server bindings on a specific interface:

```
user@host> clear dhcp server binding interface fe-0/0/2
```
clear dhcp server binding <interfaces-vlan>
The following command uses the interfaces-vlan option to clear all DHCP local server bindings on top of the underlying interface ae0, which clears DHCP bindings on all demux VLANs on top of ae0:

    user@host> clear dhcp server binding ae0

clear dhcp server binding <interfaces-wildcard>
The following command uses the interfaces-wildcard option to clear all DHCP local server bindings over a specific interface:

    user@host> clear dhcp server binding ge-1/0/0.*
clear dhcp server statistics

**Syntax**
```
clear dhcp server statistics
<interface interface-name>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

**Release Information**
Command introduced in Junos OS Release 9.0.

**Description**
Clear all extended Dynamic Host Configuration Protocol (DHCP) local server statistics.

**Options**
- `logical-system logical-system-name`—(Optional) Clear the statistics for DHCP clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.

- `routing-instance routing-instance-name`—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

**Required Privilege**
view

**List of Sample Output**
clear dhcp server statistics on page 1537

**Output Fields**
See `show dhcp server statistics` for an explanation of output fields.

**Sample Output**
clear dhcp server statistics

The following sample output displays the extended DHCP local server statistics before and after the `clear dhcp server statistics` command is issued.

```
user@host> show dhcp server statistics
Packets dropped:  
   Total                      0

Messages received:  
   BOOTREQUEST               89163
   DHCPDECLINE                0
   DHCPDISCOVER               8110
   DHCPINFORM                 0
   DHCPRELEASE                0
   DHCPREQUEST                81053

Messages sent:  
   BOOTREPLY                 32420
   DHCPOFFER                  8110
   DHCPACK                    8110
   DHCPNAK                    8100

user@host> clear dhcp server statistics
user@host> show dhcp server statistics
```

Copyright © 2013, Juniper Networks, Inc.
Packets dropped:
  Total                      0

Messages received:
  BOOTREQUEST                0
  DHCPDECLINE                0
  DHCPDISCOVER               0
  DHCPINFORM                 0
  DHCPRELEASE                0
  DHCPREQUEST                0

Messages sent:
  BOOTREPLY                  0
  DHCPOFFER                  0
  DHCPACK                    0
  DHCPNAK                    0
clear dhcpv6 server binding

Syntax

```
clear dhcpv6 server binding
  <address>
  <all>
  <interface interface-name>
  <interfaces-vlan>
  <interfaces-wildcard>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
```

Release Information

Options `interfaces-vlan` and `interfaces-wildcard` added in Junos OS Release 12.1.

Description

Clear the binding state of a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client from the client table on the extended DHCPv6 local server.

Options

- **address**—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:
  - `CID`—The specified Client ID (CID).
  - `ipv6-prefix`—The specified IPv6 prefix.
  - `session-id`—The specified session ID.
- **all**—(Optional) Clear the binding state for all DHCPv6 clients.
- **interface interface-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
- **interfaces-vlan**—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.
- **interfaces-wildcard**—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).
- **logical-system logical-system-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.
- **routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level

`clear`

Related Documentation

- Clearing DHCP Bindings for Subscriber Access
- show dhcpv6 server binding on page 1559

List of Sample Output

- clear dhcpv6 server binding all on page 1540
- clear dhcpv6 server binding <ipv6-prefix> on page 1540
**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

clear dhcpv6 server binding all

The following command clears all DHCPv6 local server bindings:

```
user@host> clear dhcpv6 server binding all
```

clear dhcpv6 server binding <ipv6-prefix>

The following command clears DHCPv6 local server bindings for a specific IPv6 prefix:

```
user@host> clear dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
```

clear dhcpv6 server binding interface

The following command clears DHCPv6 local server bindings on a specific interface:

```
user@host> clear dhcpv6 server binding interface fe-0/0/2
```

clear dhcpv6 server binding <interfaces-vlan>

The following command uses the `interfaces-vlan` option to clear all DHCPv6 local server bindings on top of the underlying interface `ae0`, which clears DHCPv6 bindings on all demux VLANs on top of `ae0`:

```
user@host> clear dhcpv6 server binding interface ae0
```

clear dhcpv6 server binding <interfaces-wildcard>

The following command uses the `interfaces-wildcard` option to clear all DHCPv6 local server bindings over a specific interface:

```
user@host> clear dhcpv6 server binding ge-1/0/0.*
```
clear dhcpv6 server statistics

Syntax

```
clear dhcpv6 server statistics
  <interface interface-name>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
```

Release Information


Description

Clear all extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options

- `logical-system logical-system-name`—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.
- `routing-instance routing-instance-name`—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.

Required Privilege Level

clear

Related Documentation

- show dhcpv6 server statistics on page 1565

List of Sample Output

clear dhcpv6 server statistics on page 1541

Sample Output

clear dhcpv6 server statistics

```
user@host> clear dhcpv6 server statistics
```
request dhcp server reconfigure

Syntax

request dhcp server reconfigure (all | address | interface interface–name | logical-system logical-system–name | routing-instance routing-instance-name)

Release Information

Command introduced in Junos OS Release 10.0.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

Description

Initiate reconfiguration processing for the specified DHCP clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the clear dhcp server binding command.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the forcerenew message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the clear-on-abort statement to configure the client to be cleared when reconfiguration fails.

Options

all—Initiate reconfiguration for all DHCP clients.

address—Initiate reconfiguration for DHCP client with the specified IP address or MAC address.

interface interface–name—Initiate reconfiguration for all DHCP clients on this logical interface (clients whose initial login requests were received over the specified interface).

NOTE: You cannot use the interface interface–name option with the request dhcp server reconfigure command for DHCP passive clients (clients that are added as a result of DHCP snooped packets). For passive clients, the interface is not guaranteed to be the next-hop interface to the client, as is the case for active clients.

logical-system logical-system–name—Initiate reconfiguration for all DHCP clients on the specified logical system.

routing-instance routing-instance-name—Initiate reconfiguration reconfigured for all DHCP clients in the specified routing instance.

Required Privilege

view
Related Documentation

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268

List of Sample Output

- request dhcp server reconfigure on page 1543

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request dhcp server reconfigure

user@host> request dhcp server reconfigure interface fe-0/0/0.100
request dhcpv6 server reconfigure

**Syntax**

```
request dhcpv6 server reconfigure (all | address address | client-id client-id | interface interface-name interface-name |
logical-system logical-system-name logical-system-name | routing-instance routing-instance-name routing-instance-name | session-id session-id)
```

**Release Information**

Command introduced in Junos OS Release 10.4.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Initiate reconfiguration processing for the specified DHCPv6 clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the `clear dhcpv6 server binding` command.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfigure state and the local server sends a reconfigure message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the reconfigure message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the `clear-on-abort` statement to configure the client to be cleared when reconfiguration fails.

**Options**

- **all**—Initiate reconfiguration for all DHCPv6 clients.
- **address**—Initiate reconfiguration for DHCPv6 client with the specified IPv6 address.
- **client-id**—Initiate reconfiguration for DHCPv6 client with the specified client ID.
- **interface interface-name**—Initiate reconfiguration for all DHCPv6 clients on this logical interface (clients whose initial login requests were received over the specified interface).
- **logical-system logical-system-name**—Initiate reconfiguration for all DHCPv6 clients on the specified logical system.
- **routing-instance routing-instance-name**—Initiate reconfiguration reconfigured for all DHCPv6 clients in the specified routing instance.
- **session-id**—Initiate reconfiguration for DHCPv6 client with the specified session ID.

**Required Privilege Level**

`view`

**Related Documentation**

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 1268

**List of Sample Output**

`request dhcpv6 server reconfigure on page 1545`

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.
Sample Output
request dhcpv6 server reconfigure

user@host> request dhcpv6 server reconfigure 2001::2/16
**request system reboot**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>request system reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&lt;at time&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;both-routing-engines&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;in minutes&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;media (compact-flash</td>
</tr>
<tr>
<td></td>
<td>&lt;message &quot;text&quot;&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;other-routing-engine&gt;</td>
</tr>
</tbody>
</table>

**Syntax (EX Series Switches)**

- request system reboot
- <all-members>
- <at time>
- <both-routing-engines>
- <in minutes>
- <local>
- <media (external | internal)>
- <member member-id>
- <message "text">
- <other-routing-engine>
- <slice slice>

**Syntax (TX Matrix Router)**

- request system reboot
- <all-chassis | all-lcc | lcc number | scc>
- <at time>
- <both-routing-engines>
- <in minutes>
- <media (compact-flash | disk)>
- <message "text">
- <other-routing-engine>

**Syntax (TX Matrix Plus Router)**

- request system reboot
- <all-chassis | all-lcc | lcc number | sfc number>
- <at time>
- <both-routing-engines>
- <in minutes>
- <media (compact-flash | disk)>
- <message "text">
- <other-routing-engine>
- <partition (1 | 2 | alternate)>

**Syntax (MX Series Router)**

- request system reboot
- <all-members>
- <at time>
- <both-routing-engines>
- <in minutes>
- <local>
- <media (external | internal)>
- <member member-id>
- <message "text">
- <other-routing-engine>

**Release Information**
Command introduced before Junos OS Release 7.4.

**Description**
Reboot the software.

**Options**
- **none**—Reboot the software immediately.
- **all-chassis**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.
- **all-lcc**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.
- **all-members**—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.
- **at time**—(Optional) Time at which to reboot the software, specified in one of the following ways:
  - **now**—Stop or reboot the software immediately. This is the default.
  - **+minutes**—Number of minutes from now to reboot the software.
  - **yymmddhhmm**—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
  - **hh:mm**—Absolute time on the current day at which to stop the software, specified in 24-hour time.
- **both-routing-engines**—(Optional) Reboot both Routing Engines at the same time.
- **in minutes**—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at +minutes** option.
- **lcc number**—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.
  Replace **number** with the following values depending on the LCC configuration:
  - 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
  - 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
  - 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
  - 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
local—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the local Virtual Chassis member.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Boot medium for next boot. (The options removable-compact-flash and usb pertain to the J Series routers only.)

media (external | internal)—(EX Series switches and MX Series routers only) (Optional) Reboot the boot media:
  • external—Reboot the external mass storage device.
  • internal—Reboot the internal flash device.

member member-id—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace member-id with a value from 0 through 9. For an MX Series Virtual Chassis, replace member-id with a value of 0 or 1.

message "text"—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition—(TX Matrix Plus routers only) (Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:
  • 1—Reboot from partition 1.
  • 2—Reboot from partition 2.
  • alternate—Reboot from the alternate partition.

scc—(TX Matrix routers only) (Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from the re1, re1 is rebooted.

sfc number—(TX Matrix Plus routers only) (Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace number with 0.

slice slice—(EX Series switches only) (Optional) Reboot a partition on the boot media. This option has the following suboptions:
  • 1—Power off partition 1.
  • 2—Power off partition 2.
  • alternate—Reboot from the alternate partition.
Reboot requests are recorded in the system log files, which you can view with the `show log` command (see `show log`). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the `show system processes` command (see `show system processes`).

On a TX Matrix or TX Matrix Plus router, if you issue the `request system reboot` command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.

**NOTE:** Before issuing the `request system reboot` command on a TX Matrix Plus router with no options or the all-chassis, all-lcc, lcc `number`, or `sfc` options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the `request system reboot` command.

**NOTE:** To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

**Required Privilege Level** maintenance

**Related Documentation**
- clear system reboot on page 163
- request system halt on page 180
- request system reboot
- Rebooting and Halting a QFX Series Product
- Routing Matrix with a TX Matrix Plus Router Solutions Page

**List of Sample Output**
- request system reboot on page 1550
- request system reboot (at 2300) on page 1550
- request system reboot (in 2 Hours) on page 1550
- request system reboot (Immediately) on page 1550
- request system reboot (at 1:20 AM) on page 1550

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.
Sample Output

request system reboot

user@host> request system reboot
Reboot the system? [yes,no] (no)

request system reboot (at 2300)

user@host> request system reboot at 2300 message ?Maintenance time? yes
shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

user@host> request system reboot +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00

request system reboot (Immediately)

user@host> request system reboot at now

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
show dhcp server binding

Syntax
show dhcp server binding
<address>
<brie | detail | summary>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>

Release Information
Command introduced in Junos OS Release 9.0.
Options interfaces-vlan and interfaces-wildcard added in Junos OS Release 12.1.

Description
Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol (DHCP) local server.

Options
address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:
  • ip-address—The specified IP address.
  • mac-address—The specified MAC address.
  • session-id—The specified session ID.

brie | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcp server binding.

interface interface-name—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

interfaces-vlan—(Optional) Show the binding state information on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) The set of interfaces on which to show the binding state information. This option supports the use of the wildcard character (*).

logical-system logical-system-name—(Optional) Display information about active client bindings for DHCP clients on the specified logical system.

routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.

Required Privilege
view

Related Documentation
• Clearing DHCP Bindings for Subscriber Access
• Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration
• clear dhcp server binding on page 1534

Copyright © 2013, Juniper Networks, Inc.
List of Sample Output  
show dhcp server binding on page 1553  
show dhcp server binding detail on page 1553  
show dhcp server binding detail (ACI Interface Set Configured) on page 1554  
show dhcp server binding interface <vlan-id> on page 1554  
show dhcp server binding interface <svlan-id> on page 1554  
show dhcp server binding <ip-address> on page 1555  
show dhcp server binding <session-id> on page 1555  
show dhcp server binding summary on page 1555  
show dhcp server binding <interfaces-vlan> on page 1555  
show dhcp server binding <interfaces-wildcard> on page 1555

Output Fields  
Table 181 on page 1552 lists the output fields for the `show dhcp server binding` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>number clients, (number init, number bound, number selecting, number requesting, number renewing)</td>
<td>Summary counts of the total number of DHCP clients and the number of DHCP clients in each state.</td>
<td>summary</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the DHCP client.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Session Id</td>
<td>Session ID of the subscriber session.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware address of the DHCP client.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Expires</td>
<td>Number of seconds in which lease expires.</td>
<td>brief detail</td>
</tr>
<tr>
<td>State</td>
<td>State of the address binding table on the extended DHCP local server:</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td>• BOUND—Client has active IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FORCERENEW—Client has received forcerenew message from server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• INIT—Initial state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RELEASE—Client is releasing IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RENEWING—Client sending request to renew IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• REQUESTING—Client requesting a DHCP server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SELECTING—Client receiving offers from DHCP servers.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the request was received.</td>
<td>brief</td>
</tr>
</tbody>
</table>
Table 181: show dhcp server binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease Expires</td>
<td>Date and time at which the client's IP address lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Expires in</td>
<td>Number of seconds in which lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Start</td>
<td>Date and time at which the client's IP address lease started.</td>
<td>detail</td>
</tr>
<tr>
<td>Last Packet Received</td>
<td>Date and time at which the router received the last packet.</td>
<td>detail</td>
</tr>
<tr>
<td>Incoming Client Interface</td>
<td>Client's incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Interface Svlan Id</td>
<td>S-VLAN ID of the client's incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Interface Vlan Id</td>
<td>VLAN ID of the client's incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Demux Interface</td>
<td>Name of the IP demultiplexing (demux) interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Server IP Address or Server Identifier</td>
<td>IP address of DHCP server.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Interface</td>
<td>Interface of DHCP server.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Pool Name</td>
<td>Name of address pool used to assign client IP address lease.</td>
<td>detail</td>
</tr>
<tr>
<td>ACI Interface Set Name</td>
<td>Internally generated name of the dynamic agent circuit identifier (ACI) interface set.</td>
<td>detail</td>
</tr>
<tr>
<td>ACI Interface Set Index</td>
<td>Index number of the dynamic ACI interface set.</td>
<td>detail</td>
</tr>
<tr>
<td>ACI Interface Set Session ID</td>
<td>Identifier of the dynamic ACI interface set entry in the session database.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output
show dhcp server binding

```
user@host> show dhcp server binding
IP address          Session Id  Hardware address       Expires  State    Interface
100.20.20.15         6          00:10:94:00:00:01     86180    BOUND    ge-1/0/0.0
100.20.20.16         7          00:10:94:00:00:02     86180    BOUND    ge-1/0/0.0
100.20.20.17         8          00:10:94:00:00:03     86180    BOUND    ge-1/0/0.0
100.20.20.18         9          00:10:94:00:00:04     86180    BOUND    ge-1/0/0.0
100.20.20.19         10         00:10:94:00:00:05     86180    BOUND    ge-1/0/0.0
```

show dhcp server binding detail

```
user@host> show dhcp server binding detail
```
show dhcp server binding detail (ACI Interface Set Configured)

Client IP Address:  100.20.20.15
Hardware Address:   00:10:94:00:00:01
State:             BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
Lease Expires:     2009-07-21 10:10:25 PDT
Lease Expires in:  86151 seconds
Lease Start:       2009-07-20 10:10:25 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address: 100.20.20.9
Server Interface:  none
Session Id:        6
Client Pool Name:  6
Client IP Address: 100.20.20.16
Hardware Address:  00:10:94:00:00:02
State:             BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
Lease Expires:     2009-07-21 10:10:25 PDT
Lease Expires in:  86151 seconds
Lease Start:       2009-07-20 10:10:25 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address: 100.20.20.9
Server Interface:  none
Session Id:        7
Client Pool Name:  7

show dhcp server binding detail (ACI Interface Set Configured)

Client IP Address:  100.20.22.14
Hardware Address:   00:00:64:34:01:02
State:             BOUND(LOCAL_SERVER_STATE_BOUND)
Lease Expires:     2012-03-13 09:53:32 PDT
Lease Expires in:  82660 seconds
Lease Start:       2012-03-12 10:23:32 PDT
Last Packet Received: 2012-03-12 10:23:32 PDT
Incoming Client Interface: demux0.1073741827
Client Interface Svlan Id:    1802
Client Interface Vlan Id:     302
Demux Interface:              demux0.1073741832
Server Identifier:            100.20.200.202
Session Id:                   11
Client Pool Name:             poolA
Client Profile Name:           DEMUXprofile
ACI Interface Set Name:        aci-1002-demux0.1073741827
ACI Interface Set Session ID: 6

show dhcp server binding interface <vlan-id>

user@host> show dhcp server binding interface ge-1/1/0:100
IP address        Session Id  Hardware address   Expires     State      Interface
200.20.20.15      6           00:10:94:00:00:01  86124       BOUND       ge-1/1/0:100

show dhcp server binding interface <svlan-id>

user@host> show dhcp server binding interface ge-1/1/0:100
IP address        Session Id  Hardware address   Expires     State      Interface
200.20.20.16      7           00:10:94:00:00:02  86124       BOUND       ge-1/1/0:100
show dhcp server binding `<ip-address>`

```
user@host> show dhcp server binding 100.20.20.19
IP address        Session Id  Hardware address   Expires     State      Interface
100.20.20.19      10          00:10:94:00:00:05  86081       BOUND      ge-1/0/0.0
```

show dhcp server binding `<session-id>`

```
user@host> show dhcp server binding 6
IP address        Session Id  Hardware address   Expires     State      Interface
200.20.20.15      6           00:10:94:00:00:01  86124       BOUND      ge-1/0/0.0
```

show dhcp server binding summary

```
user@host> show dhcp server binding summary
3 clients, (2 init, 1 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```

show dhcp server binding `<interfaces-vlan>`

```
user@host> show dhcp server binding ge-1/0/0:100-200
IP address        Session Id  Hardware address   Expires     State      Interface
192.168.0.17      42          00:10:94:00:00:02  86346       BOUND      ge-1/0/0.1073741827
192.168.0.16      41          00:10:94:00:00:01  86346       BOUND      ge-1/0/0.1073741827
```

show dhcp server binding `<interfaces-wildcard>`

```
user@host> show dhcp server binding ge-1/3/*
IP address        Session Id  Hardware address   Expires     State      Interface
192.168.0.9       24          00:10:94:00:00:04  86361       BOUND      ge-1/3/0.110
192.168.0.8       23          00:10:94:00:00:03  86361       BOUND      ge-1/3/0.110
192.168.0.7       22          00:10:94:00:00:02  86361       BOUND      ge-1/3/0.110
```
show dhcp server statistics

Syntax

```
show dhcp server statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 9.0.

Description

Display extended Dynamic Host Configuration Protocol (DHCP) local server statistics.

Options

- **logical-system logical-system-name**—(Optional) Display information about extended DHCP local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.

- **routing-instance routing-instance-name**—(Optional) Display information about extended DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege

- **view**

Related Documentation

- clear dhcp server statistics on page 1537

List of Sample Output

- show dhcp server statistics on page 1557

Output Fields

Table 182 on page 1557 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear.
Table 182: show dhcp server statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packets dropped</strong></td>
<td>Number of packets discarded by the extended DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td>• Total</td>
<td>Total number of packets discarded by the extended DHCP local server</td>
</tr>
<tr>
<td>• Authentication</td>
<td>Number of packets discarded because they could not be authenticated</td>
</tr>
<tr>
<td>• Bad hardware address</td>
<td>Number of packets discarded because an invalid hardware address was specified</td>
</tr>
<tr>
<td>• Bad opcode</td>
<td>Number of packets discarded because an invalid operation code was specified</td>
</tr>
<tr>
<td>• Bad options</td>
<td>Number of packets discarded because invalid options were specified</td>
</tr>
<tr>
<td>• Dynamic profile</td>
<td>Number of packets discarded due to dynamic profile information</td>
</tr>
<tr>
<td>• Invalid server address</td>
<td>Number of packets discarded because an invalid server address was specified</td>
</tr>
<tr>
<td>• No available addresses</td>
<td>Number of packets discarded because there were no addresses available for assignment</td>
</tr>
<tr>
<td>• No interface match</td>
<td>Number of packets discarded because they did not belong to a configured interface</td>
</tr>
<tr>
<td>• Norouting instance match</td>
<td>Number of packets discarded because they did not belong to a configured routing instance</td>
</tr>
<tr>
<td>• No valid local address</td>
<td>Number of packets discarded because there was no valid local address</td>
</tr>
<tr>
<td>• Packet too short</td>
<td>Number of packets discarded because they were too short</td>
</tr>
<tr>
<td>• Read error</td>
<td>Number of packets discarded because of a system read error</td>
</tr>
<tr>
<td>• Send error</td>
<td>Number of packets that the extended DHCP local server could not send</td>
</tr>
<tr>
<td><strong>Messages received</strong></td>
<td>Number of DHCP messages received.</td>
</tr>
<tr>
<td>• BOOTREQUEST</td>
<td>Number of BOOTP protocol data units (PDUs) received</td>
</tr>
<tr>
<td>• DHCPDECLINE</td>
<td>Number of DHCP PDUs of type DECLINE received</td>
</tr>
<tr>
<td>• DHCPDISCOVER</td>
<td>Number of DHCP PDUs of type DISCOVER received</td>
</tr>
<tr>
<td>• DHCPINFORM</td>
<td>Number of DHCP PDUs of type INFORM received</td>
</tr>
<tr>
<td>• DHCPREQUEST</td>
<td>Number of DHCP PDUs of type REQUEST received</td>
</tr>
<tr>
<td><strong>Messages sent</strong></td>
<td>Number of DHCP messages sent.</td>
</tr>
<tr>
<td>• BOOTREPLY</td>
<td>Number of BOOTP PDUs transmitted</td>
</tr>
<tr>
<td>• DHCPOFFER</td>
<td>Number of DHCP OFFER PDUs transmitted</td>
</tr>
<tr>
<td>• DHCPACK</td>
<td>Number of DHCP ACK PDUs transmitted</td>
</tr>
<tr>
<td>• DHCPNACK</td>
<td>Number of DHCP NACK PDUs transmitted</td>
</tr>
<tr>
<td>• DHCPFORCERENEW</td>
<td>Number of DHCP FORCERENEW PDUs transmitted</td>
</tr>
</tbody>
</table>

Sample Output

show dhcp server statistics

```
user@host> show dhcp server statistics
Packets dropped:
   Total                      0
Messages received:
```

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTREQUEST</td>
<td>25</td>
</tr>
<tr>
<td>DHCPDECLINE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPDISCOVER</td>
<td>10</td>
</tr>
<tr>
<td>DHCPINFORM</td>
<td>0</td>
</tr>
<tr>
<td>DHCPRELEASE</td>
<td>4</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
<td>10</td>
</tr>
</tbody>
</table>

Messages sent:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTREPLY</td>
<td>20</td>
</tr>
<tr>
<td>DHCPOFFER</td>
<td>10</td>
</tr>
<tr>
<td>DHCPACK</td>
<td>10</td>
</tr>
<tr>
<td>DHCPNAK</td>
<td>0</td>
</tr>
<tr>
<td>DHCPFORCERENEW</td>
<td>0</td>
</tr>
</tbody>
</table>
show dhcpv6 server binding

Syntax

show dhcpv6 server binding
<address>
<brief | detail | summary>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>

Release Information

Options interfaces-vlan and interfaces-wildcard added in Junos OS Release 12.1.

Description

Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server.

Options

address—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:
- CID—The specified Client ID (CID).
- ipv6-prefix—The specified IPv6 prefix.
- session-id—The specified session ID.

brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcpv6 server binding.

interface interface-name—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

interfaces-vlan—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.

interfaces-wildcard—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).

logical-system logical-system-name—(Optional) Display information about active client bindings for DHCPv6 clients on the specified logical system.

routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.

Required Privilege

view

Related Documentation

- Clearing DHCP Bindings for Subscriber Access
- clear dhcpv6 server binding on page 1539
Output Fields  Table 183 on page 1560 lists the output fields for the `show dhcpv6 server binding` command. Output fields are listed in the approximate order in which they appear.

### Table 183: show dhcpv6 server binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>number clients, (number init, number bound, number selecting, number requesting, number renewing)</td>
<td>Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.</td>
<td>summary</td>
</tr>
<tr>
<td>Prefix</td>
<td>Client’s DHCPv6 prefix, or prefix used to support multiple address assignment.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Session Id</td>
<td>Session ID of the subscriber session.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Expires</td>
<td>Number of seconds in which lease expires.</td>
<td>brief detail</td>
</tr>
</tbody>
</table>
| State | State of the address binding table on the extended DHCPv6 local server:  
- **BOUND**—Client has active IP address lease.  
- **INIT**—Initial state.  
- **RECONFIGURE**—Server has sent reconfigure message to client.  
- **RELEASE**—Client is releasing IP address lease.  
- **RENEWING**—Client sending request to renew IP address lease.  
- **REQUESTING**—Client requesting a DHCPv6 server.  
- **SELECTING**—Client receiving offers from DHCPv6 servers. | brief detail |
| Interface | Interface on which the DHCPv6 request was received. | brief |
| Client IPv6 Address | Client’s IPv6 address. | detail |
| Client IPv6 Prefix | Client’s IPv6 prefix. | detail |
| Client DUID | Client’s DHCP Unique Identifier (DUID). | brief detail |
| Lease expires | Date and time at which the client’s IP address lease expires. | detail |
### Table 183: show dhcpv6 server binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lease expires in</strong></td>
<td>Number of seconds in which lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Preferred Lease Expires</strong></td>
<td>Date and UTC time at which the client's IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Preferred Lease Expires in</strong></td>
<td>Number of seconds at which client's IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Lease Start</strong></td>
<td>Date and time at which the client's address lease was obtained.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Incoming Client Interface</strong></td>
<td>Client's incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server IP Address</strong></td>
<td>IP address of DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server Interface</strong></td>
<td>Interface of DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Client Pool Name</strong></td>
<td>Address pool used to assign IPv6 address.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Client Prefix Pool Name</strong></td>
<td>Address pool used to assign IPv6 prefix.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Client Id length</strong></td>
<td>Length of the DHCPv6 client ID, in bytes.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Client Id</strong></td>
<td>ID of the DHCPv6 client.</td>
<td>detail</td>
</tr>
</tbody>
</table>

### Sample Output

#### show dhcpv6 server binding

```
user@host> show dhcpv6 server binding
Prefix Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 6 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64 7 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:05
2001:bd8:1111:2222::/64 11 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:06
```

#### show dhcpv6 server binding detail

```
user@host> show dhcpv6 server binding detail
Session Id: 6
Client IPv6 Prefix: 2001:bd8:1111:2222::/64
Client DUID: LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
```
State: BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
Lease Expires: 2009-07-21 10:41:15 PDT
Lease Expires in: 86308 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start: 2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address: 0.0.0.0
Server Interface: none
Client Id Length: 14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0001

Session Id: 7
Client IPv6 Address: 2002::1/128
Client IPv6 Prefix: 2001:bd8:1111:2222::/64
Client DUID: LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

State: BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
Lease Expires: 2009-07-21 10:41:15 PDT
Lease Expires in: 86136 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start: 2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address: 0.0.0.0
Client Pool Name: bos-v6-pool
Client Prefix Pool Name: bos-v6-prefix-pool
Client Id Length: 14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

show dhcpv6 server binding interface
user@host> show dhcpv6 server binding interface ge-1/0/0:10-101
Prefix  Session Id  Expires  State   Interface   Client DUID
2001:bd8:1111:2222::/64 1  86055  BOUND  ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01

show dhcpv6 server binding interface detail
user@host> show dhcpv6 server binding interface ge-1/0/0:10-101 detail
Session Id: 7
Client IPv6 Prefix: 2001:bd8:1111:2222::/64
Client DUID: LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

State: BOUND(bound)
Lease Expires: 2009-07-21 10:41:15 PDT
Lease Expires in: 86136 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start: 2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address: 0.0.0.0
Server Interface: none
Client Id Length: 14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002
show dhcpv6 server binding (IPv6 Prefix)

```
user@host> show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005

detail
Session Id: 7
  Client IPv6 Prefix: 2001:bd8:1111:2222::/64
  Client DUID: LL_TIME0x1-0x2e159c0-00:10:94:00:02

  State: BOUND(bound)
  Lease Expires: 2009-07-21 10:41:15 PDT
  Lease Expires in: 86136 seconds
  Preferred Lease Expires: 2012-07-24 00:18:14 UTC
  Preferred Lease Expires in: 600 seconds
  Lease Start: 2009-07-20 10:41:15 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address: 0.0.0.0
  Server Interface: none
  Client Id Length: 14
  Client Id: /0x00010001/0x02e159c0/0x00109400/0x0002
```

show dhcpv6 server binding (Session ID)

```
user@host> show dhcpv6 server binding 8
Prefix           Session Id  Expires  State    Interface    Client DUID
2001:DB8::/32    8           86235    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:02:03
```

show dhcpv6 server binding (Interfaces VLAN)

```
user@host> show dhcpv6 server binding ge-1/0/0:100-200
Prefix           Session Id  Expires  State    Interface           Client DUID
2001:DB8::/32     30          87583    BOUND    ge-1/0/0.100-200
LL_TIME0x1-0x2e159c0-00:10:94:00:02
2001:DB9::/32     31          87583    BOUND    ge-1/0/0.100-200
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32     32          87583    BOUND    ge-1/0/0.100-200
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 server binding (Interfaces Wildcard)

```
user@host> show dhcpv6 server binding demux0
Prefix           Session Id  Expires  State    Interface           Client DUID
2001:DB8::/32     30          79681    BOUND    demux0.100-200
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32     31          79681    BOUND    demux0.100-200
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32     32          79681    BOUND    demux0.100-200
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 server binding (Interfaces Wildcard)

```
user@host> show dhcpv6 server binding ge-1/3/*
Prefix           Session Id  Expires  State    Interface           Client DUID
2001:DB8::/32     22          79681    BOUND    ge-1/3/0.100
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32     23          79681    BOUND    ge-1/3/0.100
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32     24          79681    BOUND    ge-1/3/0.100
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

Copyright © 2013, Juniper Networks, Inc.
show dhcpv6 server binding summary

user@host> show dhcpv6 server binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
show dhcpv6 server statistics

Syntax

show dhcpv6 server statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>

Release Information

Description
Display extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options
- logical-system logical-system-name—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.
- routing-instance routing-instance-name—(Optional) Display information about extended DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.

Required Privilege
view

Related Documentation
- clear dhcpv6 server statistics on page 1541

List of Sample Output
show dhcpv6 server statistics on page 1566

Output Fields
Table 184 on page 1566 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear.
Table 184: show dhcpv6 server statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets dropped</td>
<td>Number of packets discarded by the extended DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total</strong>—Total number of packets discarded by the extended DHCPv6 local server</td>
</tr>
<tr>
<td></td>
<td>• <strong>Strict Reconfigure</strong>—Number of solicit messages discarded because the client does not support reconfiguration</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad hardware address</strong>—Number of packets discarded because an invalid hardware address was specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad opcode</strong>—Number of packets discarded because an invalid operation code was specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bad options</strong>—Number of packets discarded because invalid options were specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>Invalid server address</strong>—Number of packets discarded because an invalid server address was specified</td>
</tr>
<tr>
<td></td>
<td>• <strong>No available addresses</strong>—Number of packets discarded because there were no addresses available for assignment</td>
</tr>
<tr>
<td></td>
<td>• <strong>No interface match</strong>—Number of packets discarded because they did not belong to a configured interface</td>
</tr>
<tr>
<td></td>
<td>• <strong>Norouting instance match</strong>—Number of packets discarded because they did not belong to a configured routing instance</td>
</tr>
<tr>
<td></td>
<td>• <strong>No valid local address</strong>—Number of packets discarded because there was no valid local address</td>
</tr>
<tr>
<td></td>
<td>• <strong>Packet too short</strong>—Number of packets discarded because they were too short</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read error</strong>—Number of packets discarded because of a system read error</td>
</tr>
<tr>
<td></td>
<td>• <strong>Send error</strong>—Number of packets that the extended DHCPv6 local server could not send</td>
</tr>
<tr>
<td>Messages received</td>
<td>Number of DHCPv6 messages received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_CONFIRM</strong>—Number of DHCPv6 CONFIRM PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_DECLINE</strong>—Number of DHCPv6 DECLINE PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_INFORMATION_REQUEST</strong>—Number of DHCPv6 INFORMATION-REQUEST PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_REBIND</strong>—Number of DHCPv6 REBIND PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_RELAY_FORW</strong>—Number of DHCPv6 RELAY-FORW PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_RELAY_REPL</strong>—Number of DHCPv6 RELAY-REPL PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_RELEASE</strong>—Number of DHCPv6 RELEASE PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_RENEW</strong>—Number of DHCPv6 RENEW PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_REQUEST</strong>—Number of DHCPv6 REQUEST PDUs received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_SOLICIT</strong>—Number of DHCPv6 SOLICIT PDUs received.</td>
</tr>
<tr>
<td>Messages sent</td>
<td>Number of DHCPv6 messages sent.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_ADVERTISE</strong>—Number of DHCPv6 ADVERTISE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCPV6_REPLY</strong>—Number of DHCPv6 ADVERTISE PDUs transmitted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHC6_RECONFIGURE</strong>—Number of DHCPv6 RECONFIGURE PDUs transmitted.</td>
</tr>
</tbody>
</table>

Sample Output

show dhcpv6 server statistics

    user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
   Total               0

Messages received:
   DHCPV6_DECLINE       0
   DHCPV6_SOLICIT       9
   DHCPV6_INFORMATION_REQUEST 0
   DHCPV6_RELEASE      0
   DHCPV6_REQUEST      5
   DHCPV6_CONFIRM      0
   DHCPV6_RENEW        0
   DHCPV6_REBIND       0
   DHCPV6_RELAY_FORW   0
   DHCPV6_RELAY_REPL   0

Messages sent:
   DHCPV6_ADVERTISE     9
   DHCPV6_REPLY         5
   DHCPV6_RECONFIGURE   0

DHCP Relay Agent Monitoring Commands
clear dhcp relay binding

Syntax

```plaintext
clear dhcp relay binding
  <address>
  <all>
  <interface interface-name>
  <interfaces-vlan>
  <interfaces-wildcard>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 8.3.
Options `all` and `interface` added in Junos OS Release 8.4.
Options `interfaces-vlan` and `interfaces-wildcard` added in Junos OS Release 12.1.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description

Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.

Options

- `address`—(Optional) Clear the binding state for the DHCP client, using one of the following entries:
  - `ip-address`—The specified IP address.
  - `mac-address`—The specified MAC address.
  - `session-id`—The specified session ID.
- `all`—(Optional) Clear the binding state for all DHCP clients.
- `interface interface-name`—(Optional) Clear the binding state for DHCP clients on the specified interface.
- `interfaces-vlan`—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.
- `interfaces-wildcard`—(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).
- `logical-system logical-system-name`—(Optional) Clear the binding state for DHCP clients on the specified logical system.
- `routing-instance routing-instance-name`—(Optional) Clear the binding state for DHCP clients on the specified routing instance.

Required Privilege Level

- `view`

Related Documentation

- *Clearing DHCP Bindings for Subscriber Access*
- *show dhcp relay binding on page 1578*
List of Sample Output

- `clear dhcp relay binding on page 1569`
- `clear dhcp relay binding all on page 1569`
- `clear dhcp relay binding interface on page 1569`
- `clear dhcp relay binding <interfaces-vlan> on page 1569`
- `clear dhcp relay binding <interfaces-wildcard> on page 1569`

Output Fields

See `show dhcp relay binding` for an explanation of output fields.

Sample Output

`clear dhcp relay binding`

The following sample output displays the address bindings in the DHCP client table before and after the `clear dhcp relay binding` command is issued.

```
user@host> show dhcp relay binding
IP address       Hardware address   Type     Lease expires at
100.20.32.1      90:00:00:01:00:01  active   2007-02-08 16:41:17 EST
192.168.14.8      90:00:01:01:02:01  active   2007-02-10 10:01:06 EST

user@host> clear dhcp relay binding 100.20.32.1

user@host> show dhcp relay binding
IP address       Hardware address   Type     Lease expires at
192.168.14.8      90:00:01:01:02:01  active   2007-02-10 10:01:06 EST
```

clear dhcp relay binding all

The following command clears all DHCP relay agent bindings:

```
user@host> clear dhcp relay binding all
```

clear dhcp relay binding interface

The following command clears DHCP relay agent bindings on a specific interface:

```
user@host> clear dhcp relay binding interface fe-0/0/3
```

clear dhcp relay binding <interfaces-vlan>

The following command uses the `interfaces-vlan` option to clear all DHCP relay agent bindings on top of the underlying interface `ae0`, which clears DHCP bindings on all demux VLANs on top of `ae0`:

```
user@host> clear dhcp relay binding interface ae0
```

clear dhcp relay binding <interfaces-wildcard>

The following command uses the `interfaces-wildcard` option to clear all DHCP relay agent bindings over a specific interface:

```
user@host> clear dhcp relay binding ge-1/0/0.*
```
clear dhcp relay statistics

Syntax

```
clear dhcp relay statistics
  <logical-system logical-system-name>  
  <routing-instance routing-instance-name>
```

Syntax for EX Series switches:

```
show dhcp relay statistics
  <routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description

Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.

Options

- `logical-system logical-system-name`—(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system.

- `routing-instance routing-instance-name`—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.

Required Privilege Level

- view

Related Documentation

- show dhcp relay statistics on page 1583

List of Sample Output

- clear dhcp relay statistics on page 1571

Output Fields

Table 185 on page 1571 lists the output fields for the `clear dhcp relay statistics` command.
Table 185: clear dhcp relay statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packets dropped</strong></td>
<td>Number of packets discarded by the extended DHCP relay agent application due to errors. Only nonzero statistics appear in the <strong>Packets dropped</strong> output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of packets discarded by the extended DHCP relay agent application.</td>
</tr>
<tr>
<td>Bad hardware address</td>
<td>Number of packets discarded because an invalid hardware address was specified.</td>
</tr>
<tr>
<td>Bad opcode</td>
<td>Number of packets discarded because an invalid operation code was specified.</td>
</tr>
<tr>
<td>Bad options</td>
<td>Number of packets discarded because invalid options were specified.</td>
</tr>
<tr>
<td>Invalid server address</td>
<td>Number of packets discarded because an invalid server address was specified.</td>
</tr>
<tr>
<td>No available addresses</td>
<td>Number of packets discarded because there were no addresses available for assignment.</td>
</tr>
<tr>
<td>No interface match</td>
<td>Number of packets discarded because they did not belong to a configured interface.</td>
</tr>
<tr>
<td>Norouting instance match</td>
<td>Number of packets discarded because they did not belong to a configured routing instance.</td>
</tr>
<tr>
<td>No valid local address</td>
<td>Number of packets discarded because there was no valid local address.</td>
</tr>
<tr>
<td>Packet too short</td>
<td>Number of packets discarded because they were too short.</td>
</tr>
<tr>
<td>Read error</td>
<td>Number of packets discarded because of a system read error.</td>
</tr>
<tr>
<td>Send error</td>
<td>Number of packets that the extended DHCP relay application could not send.</td>
</tr>
<tr>
<td>Option 60</td>
<td>Number of packets discarded containing DHCP option 60 vendor-specific information.</td>
</tr>
<tr>
<td>Option 82</td>
<td>Number of packets discarded because DHCP option 82 information could not be added.</td>
</tr>
<tr>
<td><strong>Messages received</strong></td>
<td>Number of DHCP messages received.</td>
</tr>
<tr>
<td>BOOTREQUEST</td>
<td>Number of BOOTP protocol data units (PDUs) received</td>
</tr>
<tr>
<td>DHCPDECLINE</td>
<td>Number of DHCP PDUs of type DECLINE received</td>
</tr>
<tr>
<td>DHCPDISCOVER</td>
<td>Number of DHCP PDUs of type DISCOVER received</td>
</tr>
<tr>
<td>DHCPINFORM</td>
<td>Number of DHCP PDUs of type INFORM received</td>
</tr>
<tr>
<td>DHCPRELEASE</td>
<td>Number of DHCP PDUs of type RELEASE received</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
<td>Number of DHCP PDUs of type REQUEST received</td>
</tr>
<tr>
<td><strong>Messages sent</strong></td>
<td>Number of DHCP messages sent.</td>
</tr>
<tr>
<td>BOOTREPLY</td>
<td>Number of BOOTP PDUs transmitted</td>
</tr>
<tr>
<td>DHCPOFFER</td>
<td>Number of DHCP OFFER PDUs transmitted</td>
</tr>
<tr>
<td>DHCPACK</td>
<td>Number of DHCP ACK PDUs transmitted</td>
</tr>
<tr>
<td>DHCPNACK</td>
<td>Number of DHCP NACK PDUs transmitted</td>
</tr>
</tbody>
</table>

**Sample Output**

clear dhcp relay statistics

The following sample output displays the DHCP relay statistics before and after the **clear dhcp relay statistics** command is issued.

```bash
user@host> show dhcp relay statistics
```

Copyright © 2013, Juniper Networks, Inc.
Packets dropped:
  Total                0

Messages received:
  BOOTREQUEST          116
  DHCPDECLINE          0
  DHCPDISCOVER         11
  DHCPINFORM           0
  DHCPRELEASE          0
  DHCPREQUEST          105

Messages sent:
  BOOTREPLY            44
  DHCPOFFER            11
  DHCPACK              11
  DHCPNAK              11

user@host> clear dhcp relay statistics

user@host> show dhcp relay statistics
Packets dropped:
  Total                0

Messages received:
  BOOTREQUEST          0
  DHCPDECLINE          0
  DHCPDISCOVER         0
  DHCPINFORM           0
  DHCPRELEASE          0
  DHCPREQUEST          0

Messages sent:
  BOOTREPLY            0
  DHCPOFFER            0
  DHCPACK              0
  DHCPNAK              0
clear dhcpv6 relay binding

Syntax

```
clear dhcpv6 relay binding
  <address>
  <all>
  <interface interface-name>
  <interfaces-vlan>
  <interfaces-wildcard>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
```

Release Information

Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Options `interfaces-vlan` and `interfaces-wildcard` added in Junos OS Release 12.1.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description

Clear the binding state of Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients from the client table.

Options

- **address**—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:
  - `CID`—The specified Client ID (CID).
  - `ipv6-prefix`—The specified IPv6 prefix.
  - `session-id`—The specified session ID.

- **all**—(Optional) Clear the binding state for all DHCPv6 clients.

- **interfaces-vlan**—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

- **interfaces-wildcard**—(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).

- **interface interface-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.

- **logical-system logical-system-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.

- **routing-instance routing-instance-name**—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level

view

Related Documentation

- *Clearing DHCP Bindings for Subscriber Access*
- *show dhcpv6 relay binding on page 1586*
List of Sample Output

- clear dhcpv6 relay binding on page 1574
- clear dhcpv6 relay binding <prefix> on page 1574
- clear dhcpv6 relay binding all on page 1574
- clear dhcv6p relay binding interface on page 1574
- clear dhcpv6 relay binding <interfaces-vlan> on page 1575
- clear dhcpv6 relay binding <interfaces-wildcard> on page 1575

Output Fields

See show dhcpv6 relay binding for an explanation of output fields.

Sample Output

clear dhcpv6 relay binding

The following sample output displays the DHCPv6 bindings before and after the clear dhcpv6 relay binding command is issued.

```
user@host> show dhcpv6 relay binding
Prefix                   Session Id  Expires  State    Interface    Client DUID
2001:bd8:3c4d:15::/64    1           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
2001:bd8:3c4d:16::/64    2           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:bd8:3c4d:17::/64    3           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:bd8:3c4d:18::/64    4           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:bd8:3c4d:19::/64    5           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:bd8:3c4d:20::/64    6           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06
```

clear dhcpv6 relay binding <prefix>

```
user@host> clear dhcpv6 relay binding 2001:bd8:3c4d:15::/64
user@host> show dhcpv6 relay binding
Prefix                   Session Id  Expires  State    Interface    Client DUID
2001:bd8:3c4d:16::/64    2           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:bd8:3c4d:17::/64    3           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:bd8:3c4d:18::/64    4           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:bd8:3c4d:19::/64    5           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:bd8:3c4d:20::/64    6           83720    BOUND    ge-1/0/0.0  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06
```

clear dhcpv6 relay binding all

The following command clears all DHCP relay agent bindings:

```
user@host> clear dhcpv6 relay binding all
```

clear dhcv6p relay binding interface

The following command clears DHCPv6 relay agent bindings on a specific interface:
clear dhcpv6 relay binding interface fe-0/0/2

clear dhcpv6 relay binding <interfaces-vlan>

The following command uses the *interfaces-vlan* option to clear all DHCPv6 relay agent bindings on top of the underlying interface *ae0*, which clears DHCPv6 bindings on all demux VLANs on top of *ae0*:

```
user@host> clear dhcpv6 relay binding interface ae0
```

clear dhcpv6 relay binding <interfaces-wildcard>

The following command uses the *interfaces-wildcard* option to clear all DHCPv6 relay agent bindings over a specific interface:

```
user@host> clear dhcpv6 relay binding ge-1/0/0.*
```
clear dhcpv6 relay statistics

Syntax

clear dhcpv6 relay statistics
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>

Release Information
Command introduced in Junos OS Release 11.4.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description
Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.

Options
logical-system logical-system-name—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system.

routing-instance routing-instance-name—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.

Required Privilege
view

List of Sample Output

Output Fields
See show dhcpv6 relay statistics for an explanation of output fields.

Sample Output

clear dhcpv6 relay statistics

The following sample output displays the DHCPv6 relay statistics before and after the clear dhcpv6 relay statistics command is issued.

user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
  Total                      0

Messages received:
  DHCPv6_DECLINE                  0
  DHCPv6_SOLICIT                  10
  DHCPv6_INFORMATION_REQUEST      0
  DHCPv6_RELEASE                  0
  DHCPv6_REQUEST                  10
  DHCPv6_CONFIRM                   0
  DHCPv6_RENEW                     0
  DHCPv6_REBIND                    0
  DHCPv6_RELAY_REPL                 0

Messages sent:
  DHCPv6_ADVERTISE                  0
  DHCPv6_REPLY                        0
  DHCPv6_RECONFIGURE                  0
  DHCPv6_RELAY_FWD                     0
user@host> clear dhcpv6 relay statistics
user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
  Total                       0

Messages received:
  DHCPv6_DECLINE             0
  DHCPv6_SOLICIT             0
  DHCPv6_INFORMATION_REQUEST 0
  DHCPv6_RELEASE             0
  DHCPv6_REQUEST             0
  DHCPv6_CONFIRM             0
  DHCPv6_RENEW               0
  DHCPv6_REBIND              0
  DHCPv6_RELAY_REPL          0

Messages sent:
  DHCPv6_ADVERTISE           0
  DHCPv6_REPLY               0
  DHCPv6_RECONFIGURE         0
  DHCPv6_RELAY_FORW          0
show dhcp relay binding

Syntax

```
show dhcp relay binding
<address>
<brief>
<detail>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<ip-address | mac-address>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
<summary>
```

Release Information

Command introduced in Junos OS Release 8.3.
Options `interface` and `mac-address` added in Junos OS Release 8.4.
Options `interfaces-vlan` and `interfaces-wildcard` added in Junos OS Release 12.1.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description

Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options

- `address`—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:
  - `ip-address`—The specified IP address.
  - `mac-address`—The specified MAC address.
  - `session-id`—The specified session ID.

- `brief`—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as `show dhcp relay binding`.

- `detail`—(Optional) Display detailed client binding information.

- `interface interface-name`—(Optional) Perform this operation on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

- `interfaces-vlan`—(Optional) Show the binding state information on the interface VLAN ID and S-VLAN ID.

- `interfaces-wildcard`—(Optional) The set of interfaces on which to show binding state information. This option supports the use of the wildcard character (`*`).

- `logical-system logical-system-name`—(Optional) Perform this operation on the specified logical system.

- `routinig-instance routing-instance-name`—(Optional) Perform this operation on the specified routing instance.

- `summary`—(Optional) Display a summary of DHCP client information.
Required Privilege Level

- **view**

Related Documentation

- Clearing DHCP Bindings for Subscriber Access
- clear dhcp relay binding on page 1568

List of Sample Output

show dhcp relay binding on page 1580
show dhcp relay binding detail on page 1580
show dhcp relay binding interface on page 1581
show dhcp relay binding interface vlan-id on page 1581
show dhcp relay binding interface svlan-id on page 1581
show dhcp relay binding ip-address on page 1581
show dhcp relay binding mac-address on page 1581
show dhcp relay binding session-id on page 1581
show dhcp relay binding <interfaces-vlan> on page 1582
show dhcp relay binding <interfaces-wildcard> on page 1582
show dhcp relay binding summary on page 1582

Output Fields

Table 186 on page 1579 lists the output fields for the `show dhcp relay binding` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number clients, (number init, number bound, number selecting, number requesting, number renewing, number rebinding)</code></td>
<td>Summary counts of the total number of DHCP clients and the number of DHCP clients in each state.</td>
<td>summary</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of the DHCP client.</td>
<td>briefdetail</td>
</tr>
<tr>
<td>Session Id</td>
<td>Session ID of the subscriber session.</td>
<td>briefdetail</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware address of the DHCP client.</td>
<td>briefdetail</td>
</tr>
<tr>
<td>Expires</td>
<td>Number of seconds in which the lease expires.</td>
<td>briefdetail</td>
</tr>
<tr>
<td>State</td>
<td>State of the DHCP relay address binding table on the DHCP client:</td>
<td>briefdetail</td>
</tr>
<tr>
<td></td>
<td>- <strong>BOUND</strong>—Client has an active IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>INIT</strong>—Initial state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>REBINDING</strong>—Client is broadcasting a request to renew the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RELEASE</strong>—Client is releasing the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RENEWING</strong>—Client is sending a request to renew the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>REQUESTING</strong>—Client is requesting a DHCP server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>SELECTING</strong>—Client is receiving offers from DHCP servers.</td>
<td></td>
</tr>
</tbody>
</table>
Table 186: show dhcp relay binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Incoming client interface.</td>
<td>brief</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Date and time at which the client’s IP address lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Expires in</td>
<td>Number of seconds in which the lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Start</td>
<td>Date and time at which the client’s IP address lease started.</td>
<td>detail</td>
</tr>
<tr>
<td>Incoming Client Interface</td>
<td>Client’s incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Server IP Address</td>
<td>IP address of the DHCP server.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Interface</td>
<td>Interface of the DHCP server.</td>
<td>detail</td>
</tr>
<tr>
<td>Bootp Relay Address</td>
<td>IP address of BOOTP relay.</td>
<td>detail</td>
</tr>
<tr>
<td>Type</td>
<td>Type of DHCP packet processing performed on the router:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• active—Router actively processes and relays DHCP packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• passive—Router passively snoops DHCP packets passing through the router.</td>
<td></td>
</tr>
<tr>
<td>Lease expires at</td>
<td>Date and time at which the client’s IP address lease expires.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show dhcp relay binding

```
user@host> show dhcp relay binding
IP address        Session Id  Hardware address   Expires     State      Interface
100.20.32.11      41          00:10:94:00:00:01  86371       BOUND      ge-1/0/0.0
100.20.32.12      42          00:10:94:00:00:02  86371       BOUND      ge-1/0/0.0
100.20.32.13      43          00:10:94:00:00:03  86371       BOUND      ge-1/0/0.0
100.20.32.14      44          00:10:94:00:00:04  86371       BOUND      ge-1/0/0.0
100.20.32.15      45          00:10:94:00:00:05  86371       BOUND      ge-1/0/0.0
```

show dhcp relay binding detail

```
user@host> show dhcp relay binding detail
Client IP Address:  100.20.32.11
Hardware Address:  00:10:94:00:00:01
State:              BOUND(DHCP_RELAY_STATE_BOUND_ON_INTF_DELETE)
Lease Expires:      2009-07-21 11:00:06 PDT
Lease Expires in:   86361 seconds
```
Lease Start:                  2009-07-20 11:00:06 PDT
Last Packet Received:         2009–07–20 11:00:06 PDT
Incoming Client Interface:    ge-1/0/0.0
Server Ip Address:            100.20.22.2
Server Interface:             none
Bootp Relay Address:          100.20.32.2
Session Id:                   41

Client IP Address:  100.20.32.12
Hardware Address:             00:10:94:00:00:02
State:                        BOUND(DHCP_RELAY_STATE_BOUND_ON_INTF_DELETE)
Lease Expires:                2009-07-21 11:00:06 PDT
Lease Expires in:             86361 seconds
Lease Start:                  2009-07-20 11:00:06 PDT
Last Packet Received:         2009–07–20 11:00:06 PDT
Incoming Client Interface:    ge-1/0/0.0
Server Ip Address:            100.20.22.2
Server Interface:             none
Bootp Relay Address:          100.20.32.2
Session Id:                   42

<table>
<thead>
<tr>
<th>IP address</th>
<th>Hardware address</th>
<th>Type</th>
<th>Lease expires at</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.20.32.1</td>
<td>90:00:00:01:00:01</td>
<td>active</td>
<td>2007-03-27 15:06:20 EDT</td>
</tr>
</tbody>
</table>

show dhcp relay binding interface

user@host> show dhcp relay binding interface fe-0/0/2

show dhcp relay binding interface vlan-id

user@host> show dhcp relay binding interface ge-1/1/0:100

show dhcp relay binding interface svlan-id

user@host> show dhcp relay binding interface ge-1/1/0:10-100

show dhcp relay binding ip-address

user@host> show dhcp relay binding 100.20.32.13

show dhcp relay binding mac-address

user@host> show dhcp relay binding 00:10:94:00:00:05

show dhcp relay binding session-id

user@host> show dhcp relay binding 41
show dhcp relay binding <interfaces-vlan>

user@host> show dhcp relay binding ge-1/0/0:100-200

<table>
<thead>
<tr>
<th>IP address</th>
<th>Session Id</th>
<th>Hardware address</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.17</td>
<td>42</td>
<td>00:10:94:00:00:02</td>
<td>86346</td>
<td>BOUND</td>
<td>ge-1/0/0:1073741827</td>
</tr>
<tr>
<td>192.168.0.16</td>
<td>41</td>
<td>00:10:94:00:00:01</td>
<td>86346</td>
<td>BOUND</td>
<td>ge-1/0/0:1073741827</td>
</tr>
</tbody>
</table>

show dhcp relay binding <interfaces-wildcard>

user@host> show dhcp relay binding ge-1/3/*

<table>
<thead>
<tr>
<th>IP address</th>
<th>Session Id</th>
<th>Hardware address</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.9</td>
<td>24</td>
<td>00:10:94:00:00:04</td>
<td>86361</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
</tr>
<tr>
<td>192.168.0.8</td>
<td>23</td>
<td>00:10:94:00:00:03</td>
<td>86361</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
</tr>
<tr>
<td>192.168.0.7</td>
<td>22</td>
<td>00:10:94:00:00:02</td>
<td>86361</td>
<td>BOUND</td>
<td>ge-1/3/0.110</td>
</tr>
</tbody>
</table>

show dhcp relay binding summary

user@host> show dhcp relay binding summary

3 clients, (2 init, 1 bound, 0 selecting, 0 requesting, 0 renewing, 0 rebinding, 0 releasing)
**show dhcp relay statistics**

**Syntax**
```
show dhcp relay statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

**Syntax for EX Series switches:**
```
show dhcp relay statistics
<routing-instance routing-instance-name>
```

**Release Information**
Command introduced in Junos OS Release 8.3.
Command introduced in Junos OS Release 12.1 for EX Series switches.
Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

**Description**
Display Dynamic Host Configuration Protocol (DHCP) relay statistics.

**Options**
`logical-system logical-system-name`—(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.

`routing-instance routing-instance-name`—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.

**Required Privilege**
view

**Related Documentation**
- clear dhcp relay statistics on page 1570

**List of Sample Output**
show dhcp relay statistics on page 1585

**Output Fields**
Table 187 on page 1584 lists the output fields for the show dhcp relay statistics command. Output fields are listed in the approximate order in which they appear.
Table 187: show dhcp relay statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets dropped</td>
<td>Number of packets discarded by the extended DHCP relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of packets discarded by the extended DHCP relay agent application.</td>
</tr>
<tr>
<td>Bad hardware address</td>
<td>Number of packets discarded because an invalid hardware address was specified.</td>
</tr>
<tr>
<td>Bad opcode</td>
<td>Number of packets discarded because an invalid operation code was specified.</td>
</tr>
<tr>
<td>Bad options</td>
<td>Number of packets discarded because invalid options were specified.</td>
</tr>
<tr>
<td>Invalid server address</td>
<td>Number of packets discarded because an invalid server address was specified.</td>
</tr>
<tr>
<td>No available addresses</td>
<td>Number of packets discarded because there were no addresses available for assignment.</td>
</tr>
<tr>
<td>No interface match</td>
<td>Number of packets discarded because they did not belong to a configured interface.</td>
</tr>
<tr>
<td>No routing instance match</td>
<td>Number of packets discarded because they did not belong to a configured routing instance.</td>
</tr>
<tr>
<td>No valid local address</td>
<td>Number of packets discarded because there was no valid local address.</td>
</tr>
<tr>
<td>Packet too short</td>
<td>Number of packets discarded because they were too short.</td>
</tr>
<tr>
<td>Read error</td>
<td>Number of packets discarded because of a system read error.</td>
</tr>
<tr>
<td>Send error</td>
<td>Number of packets that the extended DHCP relay application could not send.</td>
</tr>
<tr>
<td>Option 60</td>
<td>Number of packets discarded containing DHCP option 60 vendor-specific information.</td>
</tr>
<tr>
<td>Option 82</td>
<td>Number of packets discarded because DHCP option 82 information could not be added.</td>
</tr>
</tbody>
</table>

Messages received

- BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received
- DHCPDECLINE—Number of DHCP PDUs of type DECLINE received
- DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received
- DHCPINFORM—Number of DHCP PDUs of type INFORM received
- DHCPREQUEST—Number of DHCP PDUs of type REQUEST received

Messages sent

- BOOTREPLY—Number of BOOTP PDUs transmitted
- DHCPOFFER—Number of DHCP OFFER PDUs transmitted
- DHCPACK—Number of DHCP ACK PDUs transmitted
- DHCPNACK—Number of DHCP NACK PDUs transmitted
- DHCPFORCERENEW—Number of DHCP FORCERENEW PDUs transmitted

Packets forwarded

- BOOTREQUEST—Number of BOOTREQUEST protocol data units (PDUs) forwarded
- BOOTREPLY—Number of BOOTREPLY protocol data units (PDUs) forwarded
### Sample Output

**show dhcp relay statistics**

```bash
user@host> show dhcp relay statistics
```

#### Packets dropped:

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>30</td>
</tr>
<tr>
<td>Bad hardware address</td>
<td>1</td>
</tr>
<tr>
<td>Bad opcode</td>
<td>1</td>
</tr>
<tr>
<td>Bad options</td>
<td>3</td>
</tr>
<tr>
<td>Invalid server address</td>
<td>5</td>
</tr>
<tr>
<td>No available addresses</td>
<td>1</td>
</tr>
<tr>
<td>No interface match</td>
<td>2</td>
</tr>
<tr>
<td>No routing instance match</td>
<td>9</td>
</tr>
<tr>
<td>No valid local address</td>
<td>4</td>
</tr>
<tr>
<td>Packet too short</td>
<td>2</td>
</tr>
<tr>
<td>Read error</td>
<td>1</td>
</tr>
<tr>
<td>Send error</td>
<td>1</td>
</tr>
<tr>
<td>Option 60</td>
<td>1</td>
</tr>
<tr>
<td>Option 82</td>
<td>2</td>
</tr>
</tbody>
</table>

#### Messages received:

<table>
<thead>
<tr>
<th>Message</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTREQUEST</td>
<td>116</td>
</tr>
<tr>
<td>DHCPDECLINE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPDISCOVER</td>
<td>11</td>
</tr>
<tr>
<td>DHCPINFORM</td>
<td>0</td>
</tr>
<tr>
<td>DHCPRELEASE</td>
<td>0</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
<td>105</td>
</tr>
</tbody>
</table>

#### Messages sent:

<table>
<thead>
<tr>
<th>Message</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTREPLY</td>
<td>0</td>
</tr>
<tr>
<td>DHCPOFFER</td>
<td>2</td>
</tr>
<tr>
<td>DHCPACK</td>
<td>1</td>
</tr>
<tr>
<td>DHCPNAK</td>
<td>0</td>
</tr>
<tr>
<td>DHCPFORCERENEW</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Packets forwarded:

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>4</td>
</tr>
<tr>
<td>BOOTREQUEST</td>
<td>2</td>
</tr>
<tr>
<td>BOOTREPLY</td>
<td>2</td>
</tr>
</tbody>
</table>
show dhcpv6 relay binding

**Syntax**

```
show dhcpv6 relay binding
<address>
<brief>
<detail>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
<summary>
```

**Release Information**

Command introduced in Junos OS Release 11.4.

*interfaces-vlan* and *interfaces-wildcard* options introduced in Junos OS Release 12.1.

**Description**

Display the DHCPv6 address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

**Options**

- **address**—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:
  - `CID`—The specified Client ID (CID).
  - `ipv6-prefix`—The specified IPv6 prefix.
  - `session-id`—The specified session ID.
- **brief**—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as `show dhcpv6 relay binding`.
- **detail**—(Optional) Display detailed client binding information.
- **interface interface-name**—(Optional) Perform this operation on the specified interface.
  You can optionally filter on VLAN ID and S-VLAN ID.
- **interfaces-vlan**—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.
- **interfaces-wildcard**—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).
- **logical-system logical-system-name**—(Optional) Perform this operation on the specified logical system.
- **routing-instance routing-instance-name**—(Optional) Perform this operation on the specified routing instance.
- **summary**—(Optional) Display a summary of DHCPv6 client information.

**Required Privilege**

*view*
### Related Documentation
- Clearing DHCP Bindings for Subscriber Access
- clear dhcpv6 relay binding on page 1573

### List of Sample Output
- show dhcpv6 relay binding on page 1588
- show dhcpv6 relay binding (Address) on page 1588
- show dhcpv6 relay binding detail (Client ID) on page 1589
- show dhcpv6 relay binding detail on page 1589
- show dhcpv6 relay binding detail (Multi-Relay Topology) on page 1589
- show dhcpv6 relay binding (Session ID) on page 1590
- show dhcpv6 relay binding (Interfaces VLAN) on page 1590
- show dhcpv6 relay binding (Interfaces Wildcard) on page 1590
- show dhcpv6 relay binding summary on page 1590

### Output Fields
Table 188 on page 1587 lists the output fields for the show dhcpv6 relay binding command. Output fields are listed in the approximate order in which they appear.

#### Table 188: show dhcpv6 relay binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>number clients, (number init, number bound, number selecting, number requesting, number renewing, number rebinding)</td>
<td>Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.</td>
<td>summary</td>
</tr>
<tr>
<td>Client IPv6 Prefix</td>
<td>Prefix of the DHCPv6 client.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Client DUID</td>
<td>DHCP for IPv6 Unique Identifier (DUID) of the client.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Session Id</td>
<td>Session ID of the subscriber (DHCP client) session.</td>
<td>brief detail</td>
</tr>
<tr>
<td>Expires</td>
<td>Number of seconds in which the lease expires.</td>
<td>brief detail</td>
</tr>
<tr>
<td>State</td>
<td>State of the DHCPv6 relay address binding table on the DHCPv6 client:</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td>- <strong>BOUND</strong>—Client has an active IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>INIT</strong>—Initial state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>REBINDING</strong>—Client is broadcasting a request to renew the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RELEASE</strong>—Client is releasing the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>RENEWING</strong>—Client is sending a request to renew the IP address lease.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>REQUESTING</strong>—Client is requesting a DHCPv6 server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>SELECTING</strong>—Client is receiving offers from DHCPv6 servers.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Incoming client interface.</td>
<td>brief</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Date and time at which the client's IP address lease expires.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 188: show dhcpv6 relay binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lease Expires in</td>
<td>Number of seconds in which the lease expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Preferred Lease Expires</td>
<td>Date and UTC time at which the client's IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Preferred Lease Expires</td>
<td>Number of seconds at which the client's IPv6 prefix expires.</td>
<td>detail</td>
</tr>
<tr>
<td>Lease Start</td>
<td>Date and time at which the client's IP address lease started.</td>
<td>detail</td>
</tr>
<tr>
<td>Incoming Client Interface</td>
<td>Client's incoming interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Address</td>
<td>IP address of the DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>Displays unknown for a DHCPv6 relay agent in a multi-relay topology that is not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>directly adjacent to the DHCPv6 server and does not detect the IP address of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server. In that case, the output instead displays the Next Hop Server Facing Relay field.</td>
<td></td>
</tr>
<tr>
<td>Next Hop Server Facing Relay</td>
<td>Next-hop address in the direction of the DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td>Server Interface</td>
<td>Interface of the DHCPv6 server.</td>
<td>detail</td>
</tr>
<tr>
<td>Relay Address</td>
<td>IP address of the relay.</td>
<td>detail</td>
</tr>
<tr>
<td>Client Pool Name</td>
<td>Address pool that granted the client lease.</td>
<td>detail</td>
</tr>
<tr>
<td>Client ID Length</td>
<td>Length of client ID.</td>
<td>All levels</td>
</tr>
<tr>
<td>Client Id</td>
<td>Client ID.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

dshow dhcpv6 relay binding

user@host> show dhcpv6 relay binding

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Session Id</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
<th>Client DUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:bd8:3c4d:15::/64</td>
<td>1</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01</td>
</tr>
<tr>
<td>2001:bd8:3c4d:16::/64</td>
<td>2</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02</td>
</tr>
<tr>
<td>2001:bd8:3c4d:17::/64</td>
<td>3</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03</td>
</tr>
<tr>
<td>2001:bd8:3c4d:18::/64</td>
<td>4</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04</td>
</tr>
<tr>
<td>2001:bd8:3c4d:19::/64</td>
<td>5</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05</td>
</tr>
<tr>
<td>2001:bd8:3c4d:20::/64</td>
<td>6</td>
<td>83720</td>
<td>BOUND</td>
<td>ge-1/0/0.0</td>
<td>LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06</td>
</tr>
</tbody>
</table>

show dhcpv6 relay binding (Address)

user@host> show dhcpv6 relay binding 2001:bd8:1111:2222::/64 detail

Session Id: 1

Client IPv6 Prefix: 2001:bd8:3c4d:15::/64
Client DUID: LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
show dhcpv6 relay binding detail (Client ID)

user@host> show dhcpv6 relay binding 14/0x00010001/0x4bfa26af/0x00109400/0x0001 detail

Session Id:  1
Client IPv6 Prefix:  2001:bd8:3c4d:15::/64
Client DUID:  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
State:  BOUND(RELAY_STATE_BOUND)
Lease Expires:  2011-05-25 07:12:09 PDT
Lease Expires in:  77115 seconds
Preferred Lease Expires:  2012-07-24 00:18:14 UTC
Preferred Lease Expires in:  600 seconds
Lease Start:  2011-05-24 07:12:09 PDT
Incoming Client Interface:  ge-1/0/0.0
Server Address:  2008:aaaa:bbbb::1
Server Interface:  none
Relay Address:  2001:bd8:1111:2222::
Client Pool Name:  pool-25
Client Id Length:  14
Client Id:  /0x00010001/0x4bfa26af/0x00109400/0x0001

show dhcpv6 relay binding detail

user@host> show dhcpv6 relay binding detail

Session Id:  1
Client IPv6 Prefix:  2001:bd8:3c4d:15::/64
Client DUID:  LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
State:  BOUND(RELAY_STATE_BOUND)
Lease Expires:  2011-05-25 07:12:09 PDT
Lease Expires in:  77115 seconds
Preferred Lease Expires:  2012-07-24 00:18:14 UTC
Preferred Lease Expires in:  600 seconds
Lease Start:  2011-05-24 07:12:09 PDT
Incoming Client Interface:  ge-1/0/0.0
Server Address:  2008:aaaa:bbbb::1
Server Interface:  none
Relay Address:  2001:bd8:1111:2222::
Client Pool Name:  pool-25
Client Id Length:  14
Client Id:  /0x00010001/0x4bfa26af/0x00109400/0x0001

show dhcpv6 relay binding detail (Multi-Relay Topology)

user@host> show dhcpv6 relay binding detail
Session Id: 13
Client IPv6 Prefix: 3000:0:0:8001::5/128
Client DUID: LL0x1-00:00:65:03:01:02
State: BOUND(DHCPV6_RELAY_STATE_BOUND)
Lease Expires: 2011-11-21 06:14:50 PST
Lease Expires in: 293 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start: 2011-11-21 06:09:50 PST
Incoming Client Interface: ge-1/0/0.0
Server Address: unknown
Next Hop Server Facing Relay: 4000::2
Server Interface: none
Client Id Length: 10
Client Id: /0x00030001/0x00006503/0x0102

show dhcpv6 relay binding (Session ID)

user@host> show dhcpv6 relay binding 41
Prefix Session Id Expires State Interface Client DUID
2001:bd8:3c4d:15::/64 41 78837 BOUND ge-1/0/0.0 LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

show dhcpv6 relay binding (Interfaces VLAN)

user@host> show dhcpv6 relay binding ge-1/0/0:100-200
Prefix Session Id Expires State Interface Client DUID
2001:DB8::/32 11 87583 BOUND ge-1/0/0.1073741827 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32 12 87583 BOUND ge-1/0/0.1073741827 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

show dhcpv6 relay binding (Interfaces Wildcard)

user@host> show dhcpv6 relay binding demux0
Prefix Session Id Expires State Interface Client DUID
2001:DB8::/32 30 79681 BOUND demux0.1073741824 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32 31 79681 BOUND demux0.1073741825 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32 32 79681 BOUND demux0.1073741826 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

show dhcpv6 relay binding (Interfaces Wildcard)

user@host> show dhcpv6 relay binding ge-1/3/*
Prefix Session Id Expires State Interface Client DUID
2001:DB8::/32 22 79681 BOUND ge-1/3/0.110 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32 33 79681 BOUND ge-1/3/0.110 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32 24 79681 BOUND ge-1/3/0.110 LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

show dhcpv6 relay binding summary

user@host> show dhcpv6 relay binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
**show dhcpv6 relay statistics**

**Syntax**
```
show dhcpv6 relay statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

**Release Information**
- Command introduced in Junos OS Release 11.4.
- Command introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

**Options**
- `logical-system logical-system-name`—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.
- `routing-instance routing-instance-name`—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.

**Required Privilege Level**
view

**Related Documentation**
- `clear dhcpv6 relay statistics` on page 1576
- `List of Sample Output` on page 1592

**Output Fields**
Table 189 on page 1591 lists the output fields for the `show dhcpv6 relay statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 189: show dhcpv6 relay statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Packets dropped</td>
<td>Number of packets discarded by the extended DHCPv6 relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</td>
</tr>
<tr>
<td></td>
<td>- Total—Total number of packets discarded by the DHCPv6 relay agent application.</td>
</tr>
<tr>
<td></td>
<td>- Bad options—Number of packets discarded because invalid options were specified.</td>
</tr>
<tr>
<td></td>
<td>- Bad send—Number of packets that the extended DHCP relay application could not send.</td>
</tr>
<tr>
<td></td>
<td>- Bad src address—Number of packets discarded because the family type was not AF_INET6.</td>
</tr>
<tr>
<td></td>
<td>- No client id—Number of packets discarded because they could not be matched to a client.</td>
</tr>
<tr>
<td></td>
<td>- No safd—Number of packets discarded because they arrived on an unconfigured interface.</td>
</tr>
<tr>
<td></td>
<td>- Short packet—Number of packets discarded because they were too short.</td>
</tr>
<tr>
<td></td>
<td>- Relay hop count—Number of packets discarded because the hop count in the packet exceeded 32.</td>
</tr>
</tbody>
</table>
Table 189: show dhcpv6 relay statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages received</td>
<td>Number of DHCPv6 messages received.</td>
</tr>
<tr>
<td>DHCPv6_DECLINE</td>
<td>Number of DHCPv6 PDU of type DECLINE received</td>
</tr>
<tr>
<td>DHCPv6_SOLICIT</td>
<td>Number of DHCPv6 PDU of type SOLICIT received</td>
</tr>
<tr>
<td>DHCPv6_INFORMATION_REQUEST</td>
<td>Number of DHCPv6 PDU of type INFORMATION-REQUEST received</td>
</tr>
<tr>
<td>DHCPv6_RELEASE</td>
<td>Number of DHCPv6 PDU of type RELEASE received</td>
</tr>
<tr>
<td>DHCPv6_REQUEST</td>
<td>Number of DHCPv6 PDU of type REQUEST received</td>
</tr>
<tr>
<td>DHCPv6_CONFIRM</td>
<td>Number of DHCPv6 PDU of type CONFIRM received</td>
</tr>
<tr>
<td>DHCPv6_RENEW</td>
<td>Number of DHCPv6 PDU of type RENEW received</td>
</tr>
<tr>
<td>DHCPv6_REBIND</td>
<td>Number of DHCPv6 PDU of type REBIND received</td>
</tr>
<tr>
<td>DHCPv6_RELAY_REPL</td>
<td>Number of DHCPv6 PDU of type RELAY-REPL received</td>
</tr>
</tbody>
</table>

| Messages sent | Number of DHCPv6 messages sent.                                                   |
| DHCPv6_ADVERTISE | Number of DHCPv6 ADVERTISE PDU transmitted                                     |
| DHCP_REPLY      | Number of DHCPv6 REPLY PDU transmitted                                             |
| DHCP_RECONFIGURE | Number of DHCPv6 RECONFIGURE PDU transmitted                                     |
| DHCP_RELAY_FORW | Number of DHCPv6 RELAY-FORW PDU transmitted                                      |

| Packets forwarded | Number of packets forwarded by the extended DHCPv6 relay agent application. |
| FWD_REQUEST       | Number of DHCPv6 REQUEST packets forwarded                                       |
| FWD_REPLY          | Number of DHCPv6 REPLY packets forwarded                                          |

Sample Output

show dhcpv6 relay statistics

```
user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
    Total                       0

Messages received:
    DHCPv6_DECLINE              0
    DHCPv6_SOLICIT              10
    DHCPv6_INFORMATION_REQUEST  0
    DHCPv6_RELEASE              0
    DHCPv6_REQUEST              10
    DHCPv6_CONFIRM              0
    DHCPv6_RENEW                0
    DHCPv6_REBIND               0
    DHCPv6_RELAY_REPL           0

Messages sent:
    DHCPv6_ADVERTISE            0
    DHCPv6_REPLY                 0
    DHCPv6_RECONFIGURE          0
    DHCPv6_RELAY_FORW            0

Packets forwarded:
    Total                       4
```
<table>
<thead>
<tr>
<th>FWD REQUEST</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>FWD REPLY</td>
<td>2</td>
</tr>
</tbody>
</table>
show route extensive

Syntax

```
show route extensive
<destination-prefix>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches)

```
show route extensive
<destination-prefix>
```

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display extensive information about the active entries in the routing tables.

Options

- `none`—Display all active entries in the routing table.
- `destination-prefix`—(Optional) Display active entries for the specified address or range of addresses.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

- view

List of Sample Output

- show route extensive on page 1600
- show route extensive (Access Route) on page 1606
- show route extensive (BGP PIC Edge) on page 1607
- show route extensive (FRR and LFA) on page 1607
- show route extensive (Route Reflector) on page 1608
- show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 1608

Output Fields

Table 190 on page 1594 describes the output fields for the `show route extensive` command. Output fields are listed in the approximate order in which they appear.

Table 190: show route extensive Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>routing-table-name</code></td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td><code>number destinations</code></td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td><code>number routes</code></td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>• active (routes that are active).</td>
</tr>
<tr>
<td></td>
<td>• holdown (routes that are in the pending state before being declared inactive).</td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy).</td>
</tr>
</tbody>
</table>
Table 190: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>route-destination</strong> (entry, announced)</td>
<td>Route destination (for example: 10.0.0.1/24). The entry value is the number of route for this destination, and the announced value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:</td>
</tr>
<tr>
<td></td>
<td>• <strong>MPLS-label</strong> (for example, 80001).</td>
</tr>
<tr>
<td></td>
<td>• <strong>interface-name</strong> (for example, ge-1/0/2).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address; control-word-status: encapsulation type; vc-id; source</strong> (Layer 2 circuit only; for example, 10.1.1.10:NoCtrlWord:1:1;Local/96).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address</strong>—Address of the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>control-word-status</strong>—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord.</td>
</tr>
<tr>
<td></td>
<td>• <strong>encapsulation type</strong>—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.</td>
</tr>
<tr>
<td></td>
<td>• <strong>vc-id</strong>—Virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td>• <strong>source</strong>—Source of the advertisement: Local or Remote.</td>
</tr>
<tr>
<td></td>
<td>Protocol header information.</td>
</tr>
<tr>
<td><strong>TSI</strong></td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>[protocol, preference]</strong></td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>• -—A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>• * —An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route.</td>
</tr>
<tr>
<td></td>
<td>In every routing metric except for the BGP LocalPref attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the LocalPref value in the Preference2 field. For example, if the LocalPref value for Route 1 is 100, the Preference2 value is -101. If the LocalPref value for Route 2 is 155, the Preference2 value is -156. Route 2 is preferred because it has a higher LocalPref value and a lower Preference2 value.</td>
</tr>
<tr>
<td><strong>Level</strong></td>
<td>(IS-IS only). In IS-IS, a single autonomous system (AS) can be divided into smaller groups called areas. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area. When the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs.</td>
</tr>
<tr>
<td><strong>Route Distinguisher</strong></td>
<td>IP subnet augmented with a 64-bit prefix.</td>
</tr>
</tbody>
</table>
## Table 190: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next-hop type</strong></td>
<td>Type of next hop. For a description of possible values for this field, see the Output Field table in the show route detail command.</td>
</tr>
<tr>
<td><strong>Next-hop reference count</strong></td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td><strong>Flood next-hop branches exceed maximum message</strong></td>
<td>Indicates that the number of flood next-hop branches exceeded the system limit of 32 branches, and only a subset of the flood next-hop branches were installed in the kernel.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>IP address of the route source.</td>
</tr>
<tr>
<td><strong>Next hop</strong></td>
<td>Network layer address of the directly reachable neighboring system.</td>
</tr>
<tr>
<td><strong>via</strong></td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word <strong>Selected</strong>. This field can also contain the following information:</td>
</tr>
<tr>
<td></td>
<td>• Weight—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.</td>
</tr>
<tr>
<td></td>
<td>• Balance—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.</td>
</tr>
<tr>
<td><strong>Label-switched-path</strong></td>
<td>Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td><strong>lsp-path-name</strong></td>
<td>Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td><strong>Label operation</strong></td>
<td>MPLS label and operation occurring at this routing device. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label).</td>
</tr>
<tr>
<td><strong>Offset</strong></td>
<td>Whether the metric has been increased or decreased by an offset value.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>(Local only) Local interface name.</td>
</tr>
<tr>
<td><strong>Protocol next hop</strong></td>
<td>Network layer address of the remote routing device that advertised the prefix. This address is used to recursively derive a forwarding next hop.</td>
</tr>
<tr>
<td><strong>label-operation</strong></td>
<td>MPLS label and operation occurring at this routing device. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label).</td>
</tr>
</tbody>
</table>
Table 190: show route extensive Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| **Indirect next hops** | When present, a list of nodes that are used to resolve the path to the next-hop destination, in the order that they are resolved.  
When BGP PIC Edge is enabled, the output lines that contain *indirect next hop: weight* follow next hops that the software can use to repair paths where a link failure occurs. The next-hop weight has one of the following values:  
• 0x1 indicates active next hops.  
• 0x4000 indicates passive next hops. |
| **State**           | State of the route (a route can be in more than one state). See the Output Field table in the `show routedetail` command. |
| **Session ID**      | The BFD session ID number that represents the protection using MPLS fast reroute (FRR) and loop-free alternate (LFA). |
| **Weight**          | Weight for the backup path. If the weight of an indirect next hop is larger than zero, the weight value is shown.  
For sample output, see `show route table`. |
Table 190: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactive reason</td>
<td>If the route is inactive, the reason for its current state is indicated. Typical reasons include:</td>
</tr>
<tr>
<td></td>
<td>• Active preferred—Currently active route was selected over this route.</td>
</tr>
<tr>
<td></td>
<td>• Always compare MED—Path with a lower multiple exit discriminator (MED) is available.</td>
</tr>
<tr>
<td></td>
<td>• AS path—Shorter AS path is available.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Non-deterministic MED selection—Cisco nondeterministic MED is enabled and a path with a lower MED is available.</td>
</tr>
<tr>
<td></td>
<td>• Cluster list length—Path with a shorter cluster list length is available.</td>
</tr>
<tr>
<td></td>
<td>• Forwarding use only—Path is only available for forwarding purposes.</td>
</tr>
<tr>
<td></td>
<td>• IGP metric—Path through the next hop with a lower IGP metric is available.</td>
</tr>
<tr>
<td></td>
<td>• IGP metric type—Path with a lower OSPF link-state advertisement type is available.</td>
</tr>
<tr>
<td></td>
<td>• Interior &gt; Exterior &gt; Exterior via Interior—Direct, static, IGP, or EBGP path is available.</td>
</tr>
<tr>
<td></td>
<td>• Local preference—Path with a higher local preference value is available.</td>
</tr>
<tr>
<td></td>
<td>• Next hop address—Path with a lower metric next hop is available.</td>
</tr>
<tr>
<td></td>
<td>• No difference—Path from a neighbor with a lower IP address is available.</td>
</tr>
<tr>
<td></td>
<td>• Not Best in its group—Occurs when multiple peers of the same external AS advertise the same prefix and are grouped together in the selection process.</td>
</tr>
<tr>
<td></td>
<td>• Number of gateways—Path with a higher number of next hops is available.</td>
</tr>
<tr>
<td></td>
<td>• Origin—Path with a lower origin code is available.</td>
</tr>
<tr>
<td></td>
<td>• OSPF version—Path does not support the indicated OSPF version.</td>
</tr>
<tr>
<td></td>
<td>• RIIB preference—Route from a higher-numbered routing table is available.</td>
</tr>
<tr>
<td></td>
<td>• Route destinguisher—64-bit prefix added to IP subnets to make them unique.</td>
</tr>
<tr>
<td></td>
<td>• Route metric or MED comparison—Route with a lower metric or MED is available.</td>
</tr>
<tr>
<td></td>
<td>• Route preference—Route with a lower preference value is available.</td>
</tr>
<tr>
<td></td>
<td>• Router ID—Path through a neighbor with a lower ID is available.</td>
</tr>
<tr>
<td></td>
<td>• Unusable path—Path is not usable because of one of the following conditions: the route is damped, the route is rejected by an import policy, or the route is unresolved.</td>
</tr>
<tr>
<td></td>
<td>• Update source—Last tiebreaker is the lowest IP address value.</td>
</tr>
<tr>
<td>Local AS</td>
<td>Autonomous system (AS) number of the local routing device.</td>
</tr>
<tr>
<td>Age</td>
<td>How long the route has been known.</td>
</tr>
<tr>
<td>AIGP</td>
<td>Accumulated interior gateway protocol (AIGP) BGP attribute.</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost value of the indicated route. For routes within an AS, the cost is determined by IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.</td>
</tr>
<tr>
<td>MED-plus-IGP</td>
<td>Metric value for BGP path selection to which the IGP cost to the next-hop destination has been added.</td>
</tr>
<tr>
<td>TTL-Action</td>
<td>For MPLS LSPs, state of the TTL propagation attribute. Can be enabled or disabled for all RSVP-signaled and LDP-signaled LSPs or for specific VRF routing instances.</td>
</tr>
<tr>
<td></td>
<td>For sample output, see show route table.</td>
</tr>
</tbody>
</table>
### Table 190: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Name of the protocol that has added the route.</td>
</tr>
<tr>
<td>Announcement bits</td>
<td>List of protocols that announce this route. <em>n-Resolve inet</em> indicates that the route is used for route resolution for next hops found in the routing table. <em>n</em> is an index used by Juniper Networks customer support only.</td>
</tr>
<tr>
<td>AS path</td>
<td>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
</tr>
<tr>
<td></td>
<td>• Recorded—The AS path is recorded by the sample process (sampled).</td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete; typically, the AS path was aggregated.</td>
</tr>
<tr>
<td></td>
<td>When AS path numbers are included in the route, the format is as follows:</td>
</tr>
<tr>
<td></td>
<td>• [ ]—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured.</td>
</tr>
<tr>
<td></td>
<td>• { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.</td>
</tr>
<tr>
<td></td>
<td>• ()—Parentheses enclose a confederation.</td>
</tr>
<tr>
<td></td>
<td>• ( [ ] )—Parentheses and brackets enclose a confederation set.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.</td>
</tr>
<tr>
<td>FECs bound to route</td>
<td>Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.</td>
</tr>
<tr>
<td>AS path: I &lt;Originator&gt;</td>
<td>(For route reflected output only) Originator ID attribute set by the route reflector.</td>
</tr>
<tr>
<td>VC Label</td>
<td>MPLS label assigned to the Layer 2 circuit virtual connection.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) of the Layer 2 circuit.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN identifier of the Layer 2 circuit.</td>
</tr>
<tr>
<td>Cluster list</td>
<td>(For route reflected output only) Cluster ID sent by the route reflector.</td>
</tr>
<tr>
<td>Originator ID</td>
<td>(For route reflected output only) Address of router that originally sent the route to the route reflector.</td>
</tr>
<tr>
<td>Prefixes bound to route</td>
<td>Forwarding equivalent class (FEC) bound to this route. Applicable only to routes installed by LDP.</td>
</tr>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See the Output Field table in the <code>show route detail</code> command for all possible values for this field.</td>
</tr>
<tr>
<td>Layer2-info: encaps</td>
<td>Layer 2 encapsulation (for example, VPLS).</td>
</tr>
</tbody>
</table>
Table 190: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>control flags</td>
<td>Control flags: none or Site Down.</td>
</tr>
<tr>
<td>mtu</td>
<td>Maximum transmission unit (MTU) information.</td>
</tr>
<tr>
<td>Label-Base, range</td>
<td>First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.</td>
</tr>
<tr>
<td>status vector</td>
<td>Layer 2 VPN and VPLS network layer reachability information (NLRI).</td>
</tr>
<tr>
<td>Localpref</td>
<td>Local preference value included in the route.</td>
</tr>
<tr>
<td>Router ID</td>
<td>BGP router ID as advertised by the neighbor in the open message.</td>
</tr>
<tr>
<td>Primary Routing Table</td>
<td>In a routing table group, the name of the primary routing table in which the route resides.</td>
</tr>
<tr>
<td>Secondary Tables</td>
<td>In a routing table group, the name of one or more secondary tables in which the route resides.</td>
</tr>
<tr>
<td>Originating RIB</td>
<td>Name of the routing table whose active route was used to determine the forwarding next-hop entry in the resolution database. For example, in the case of inet.0 resolving through inet.0 and inet.3, this field indicates which routing table, inet.0 or inet.3, provided the best path for a particular prefix.</td>
</tr>
<tr>
<td>Node path count</td>
<td>Number of nodes in the path.</td>
</tr>
<tr>
<td>Forwarding nexthops</td>
<td>Number of forwarding next hops. The forwarding next hop is the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.</td>
</tr>
</tbody>
</table>

Sample Output

```
show route extensive
inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI:
  KRT in-kernel 10.10.0.0/16 --> (192.168.71.254)
    *Static Preference: 5
    Next-hop reference count: 29
    Next hop: 192.168.71.254 via fxp0.0, selected
    State: <Active NoReadvrt Int Ext>
    Local AS: 69
    Age: 1:34:06
    Task: RT
    Announcement bits (2): 0-KRT 3-Resolve tree 2
    AS path: I

10.31.1.0/30 (2 entries, 1 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 2
  Next hop: via so-0/3/0.0, selected
  State: <Active Int>
```
Local AS: 69
Age: 1:32:40
Task: IF
Announcement bits (1): 3-Resolve tree 2
AS path: I

OSPF
Preference: 10
Next-hop reference count: 1
Next hop: via so-0/3/0.0, selected
State: <Int>
Inactive reason: Route Preference
Local AS: 69
Age: 1:32:40    Metric: 1
Area: 0.0.0.0
Task: OSPF
AS path: I

10.31.1.3/32 (1 entry, 1 announced)
  *Local
Preference: 0
Next hop type: Local
Next-hop reference count: 7
Interface: so-0/3/0.0
State: <Active NoReadvrt Int>
Local AS: 69
Age: 1:32:43
Task: IF
Announcement bits (1): 3-Resolve tree 2
AS path: I

...  

10.31.2.0/30 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.31.2.0/30 -> {10.31.1.6}
  *OSPF
Preference: 10
Next-hop reference count: 9
Next hop: via so-0/3/0.0
Next hop: 10.31.1.6 via ge-3/1/0.0, selected
State: <Active Int>
Local AS: 69
Age: 1:32:19    Metric: 2
Area: 0.0.0.0
Task: OSPF
Announcement bits (2): 0-KRT 3-Resolve tree 2
AS path: I

...  

224.0.0.2/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 224.0.0.2/32 -> {}
  *PIM
Preference: 0
Next-hop reference count: 18
State: <Active NoReadvrt Int>
Local AS: 69
Age: 1:34:08
Task: PIM Recv
Announcement bits (2): 0-KRT 3-Resolve tree 2
AS path: I

...
224.0.0.22/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 224.0.0.22/32 -> {}
*IGMP  Preference: 0
Next-hop reference count: 18
State: <Active NoReadvrt Int>
Local AS: 69
Age: 1:34:06
Task: IGMP
Announcement bits (2): 0-KRT 3-Resolve tree 2
AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.255.70.103/32 (1 entry, 1 announced)
State: <FlashAll>
*RSVP  Preference: 7
Next-hop reference count: 6
Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
Label-switched-path green-r1-r3
Label operation: Push 100096
State: <Active Int>
Local AS: 69
Age: 1:28:12  Metric: 2
Task: RSVP
Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
AS path: I

10.255.71.238/32 (1 entry, 1 announced)
State: <FlashAll>
*RSVP  Preference: 7
Next-hop reference count: 6
Next hop: via so-0/3/0.0 weight 0x1, selected
Label-switched-path green-r1-r2
State: <Active Int>
Local AS: 69
Age: 1:28:12  Metric: 1
Task: RSVP
Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

47.0005.80ff.f800.0000.0108.0001.0102.5507.1052/152 (1 entry, 0 announced)
*Direct Preference: 0
Next hop type: Interface
Next-hop reference count: 1
Next hop: via lo0.0, selected
State: <Active Int>
Local AS: 69
Age: 1:34:07
Task: IF
AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

0 (1 entry, 1 announced)
TSI:
KRT in-kernel 0 /36 -> {}
  *MPLS  Preference: 0
  Next hop type: Receive
  Next-hop reference count: 6
  State: <Active Int>
  Local AS:  69
  Age: 1:34:08  Metric: 1
  Task: MPLS
  Announcement bits (1): 0-KRT
  AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
299776 (1 entry, 1 announced)

TSI:
KRT in-kernel 299776 /52 -> {Flood}
  *RSVP  Preference: 7
  Next hop type: Flood
  Next-hop reference count: 130
  Flood nexthop branches exceed maximum
  Address: 0x8ea65d0

800010 (1 entry, 1 announced)

TSI:
KRT in-kernel 800010 /36 -> {vt-3/2/0.32769}
  *VPLS  Preference: 7
  Next-hop reference count: 2
  Next hop: via vt-3/2/0.32769, selected
  Label operation: Pop
  State: <Active Int>
  Age: 1:31:53
  Task: Common L2 VC
  Announcement bits (1): 0-KRT
  AS path: I

vt-3/2/0.32769 (1 entry, 1 announced)

TSI:
KRT in-kernel vt-3/2/0.32769.0 /16 -> {indirect(1048574)}
  *VPLS  Preference: 7
  Next-hop reference count: 2
  Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
  Label-switched-path green-r1-r3
  Label operation: Push 800012, Push 100096(top)
  Protocol next hop: 10.255.70.103
  Push 800012
  Indirect next hop: 87272e4 1048574
  State: <Active Int>
  Age: 1:31:53  Metric2: 2
  Task: Common L2 VC
  Announcement bits (2): 0-KRT 1-Common L2 VC
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS,
  control flags:, mtu: 0
  Indirect next hops: 1
    Protocol next hop: 10.255.70.103 Metric: 2
    Push 800012
    Indirect next hop: 87272e4 1048574
Indirect path forwarding next hops: 1
   Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1
10.255.70.103/32 Originating RIB: inet.3
   Metric: 2
   Node path count: 1
Forwarding nexthops: 1
   Nexthop: 10.31.1.6 via ge-3/1/0.0

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

abcd::10:255:71:52/128 (1 entry, 0 announced)
   *Direct Preference: 0
   Next hop type: Interface
   Next-hop reference count: 1
   Next hop: via lo0.0, selected
   State: <Active Int>
   Local AS: 69
   Age: 1:34:07
   Task: IF
   AS path: I

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
   *Direct Preference: 0
   Next hop type: Interface
   Next-hop reference count: 1
   Next hop: via lo0.0, selected
   State: <Active NoReadvrt Int>
   Local AS: 69
   Age: 1:34:07
   Task: IF
   AS path: I

ff02::2/128 (1 entry, 1 announced)
   TSI:
   KRT in-kernel ff02::2/128 -> {}
   *PIM
   Preference: 0
   Next-hop reference count: 18
   State: <Active NoReadvrt Int>
   Local AS: 69
   Age: 1:34:08
   Task: PIM Recv6
   Announcement bits (1): 0-KRT
   AS path: I

ff02::d/128 (1 entry, 1 announced)
   TSI:
   KRT in-kernel ff02::d/128 -> {}
   *PIM
   Preference: 0
   Next-hop reference count: 18
   State: <Active NoReadvrt Int>
   Local AS: 69
   Age: 1:34:08
   Task: PIM Recv6
   Announcement bits (1): 0-KRT
   AS path: I

ff02::16/128 (1 entry, 1 announced)
   TSI:
   KRT in-kernel ff02::16/128 -> {}
   *MLD
   Preference: 0
   Next-hop reference count: 18
   State: <Active NoReadvrt Int>
Local AS:    69
Age: 1:34:06
Task: MLD
Announcement bits (1): 0-KRT
AS path: I

private.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
  ^Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.16385, selected
  State: <Active NoReadvrt Int>
  Age: 1:34:07
  Task: IF
  AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
  ^BGP    Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Secondary Active Int Ext>
  Local AS:    69 Peer AS:    69
  Age: 1:28:12    Metric2: 1
  Task: BGP_69.10.255.70.103+179
  Announcement bits (1): 0-green-l2vpn
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS,
  control flags:, mtu: 0
  Label-base: 800008, range: 8
  Localpref: 100
  Router ID: 10.255.70.103
  Primary Routing Table bgp.l2vpn.0

10.255.71.52:1:1:1/96 (1 entry, 1 announced)
  ^L2VPN    Preference: 170/-1
  Next-hop reference count: 5
  Protocol next hop: 10.255.71.52
  Indirect next hop: 0 -
  State: <Active Int Ext>
  Age: 1:34:03    Metric2: 1
  Task: green-l2vpn
  Announcement bits (1): 1-BGP.0.0.0.0+179
  AS path: I
  Communities: Layer2-info: encaps:VPLS, control flags:Site-Down,
  mtu: 0
  Label-base: 800016, range: 8, status-vector: 0x9F

10.255.71.52:1:5:1/96 (1 entry, 1 announced)
  ^L2VPN    Preference: 170/-101
  Next-hop reference count: 5
Protocol next hop: 10.255.71.52
Indirect next hop: 0 -
State: <Active Int Ext>
Age: 1:34:03    Metric2: 1
Task: green-l2vpn
Announcement bits (1): 1-BGP.0.0.0.0+179
AS path: I
Communities: Layer2-info: encaps:VPLS, control flags:, mtu: 0
Label-base: 800008, range: 8, status-vector: 0x9F

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

TSI:

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  *L2CKT Preference: 7
  Next hop: via so-1/1/2.0 weight 1, selected
  Label-switched-path my-lsp
  Label operation: Push 100000[0]
  Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
  State: <Active Int>
  Local AS:    99
  Age: 10:21
  Task: l2 circuit
  Announcement bits (1): 0-LDP
  AS path: I
  VC Label 100000, MTU 1500, VLAN ID 512

55.0.0.0/24 (1 entry, 1 announced)
TSI:
  KRT queued (pending) add
  55.0.0.0/24 -> {Push 300112}
  *BGP Preference: 170/-101
  Next hop type: Router
  Address: 0x925c208
  Next-hop reference count: 2
  Source: 10.0.0.9
  Next hop: 10.0.0.9 via ge-1/2/0.15, selected
  Label operation: Push 300112
  Label TTL action: prop-ttl
  State: <Active Ext>
  Local AS:  7019 Peer AS: 13979
  Age: lw0d 23:06:56
  AIGP: 25
  Task: BGP_13979.10.0.0.9+56732
  Announcement bits (1): 0-KRT
  AS path: 13979 7019 I
  Accepted
  Route Label: 300112
  Localpref: 100
  Router ID: 10.9.9.1

show route extensive (Access Route)

user@host> show route 13.160.0.102 extensive
inet.0: 39256 destinations, 39258 routes (39255 active, 0 holddown, 1 hidden)
13.160.0.102/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.102/32 -> {13.160.0.2}
OSPF area: 0.0.0.0, LSA ID: 13.160.0.102, LSA type: Extern
   *Access Preference: 13
   Next-hop reference count: 78472
   Next hop: 13.160.0.2 via fe-0/0/0.0, selected
   State: <Active Int>
   Age: 12
   Task: RPD Unix Domain Server./var/run/rpd_serv.local
   Announcement bits (2): 0-KRT 1-OSPFv2
   AS path: I

show route extensive (BGP PIC Edge)

user@host> show route 1.1.1.6 extensive
ed.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
   1.1.1.6/32 (3 entries, 2 announced)
   State: <CalcForwarding>
   TSI:
   KRT in-kernel 1.1.1.6/32 -> {indirect(1048574), indirect(1048577)}
   Page 0 idx 0 Type 1 val 9219e30
   Nexthop: Self
   AS path: [2] 3 I
   Communities: target:2:1
   Path 1.1.1.6 from 1.1.1.4 Vector len 4. Val: 0
   ...#Multipath Preference: 255
   Next hop type: Indirect
   Address: 0x93f4010
   Next-hop reference count: 2
   ...
   Protocol next hop: 1.1.1.4
   Push 299824
   Indirect next hop: 944c000 1048574 INH Session ID: 0x3
   Indirect next hop: weight 0x1
   Protocol next hop: 1.1.1.5
   Push 299824
   Indirect next hop: 944c1d8 1048577 INH Session ID: 0x4
   Indirect next hop: weight 0x4000
   State: <ForwardingOnly Int Ext>
   Inactive reason: Forwarding use only
   Age: 25  Metric2: 15
   Validation State: unverified
   Task: RT
   Announcement bits (1): 0-KRT
   AS path: 3 I
   Communities: target:2:1

show route extensive (FRR and LFA)

user@host> show route 20.31.2.0 extensive
inet.0: 46 destinations, 49 routes (45 active, 0 holddown, 1 hidden)
   20.31.2.0/24 (2 entries, 1 announced)
   State: FlashAll
   TSI:
   KRT in-kernel 20.31.2.0/24 -> {Push 299776, Push 299792}
   *RSVP
   Preference: 7/1
   Next hop type: Router, Next hop index: 1048574
   Address: 0xbbbc010
   Next-hop reference count: 5
   Next hop: 10.31.1.2 via ge-2/1/8.0 weight 0x1, selected
   Label-switched-path europa-d-to-europa-e

KRT in-kernel 13.160.0.102/32 -> {13.160.0.2}
OSPF area: 0.0.0.0, LSA ID: 13.160.0.102, LSA type: Extern
   *Access Preference: 13
   Next-hop reference count: 78472
   Next hop: 13.160.0.2 via fe-0/0/0.0, selected
   State: <Active Int>
   Age: 12
   Task: RPD Unix Domain Server./var/run/rpd_serv.local
   Announcement bits (2): 0-KRT 1-OSPFv2
   AS path: I

show route extensive (BGP PIC Edge)

user@host> show route 1.1.1.6 extensive
ed.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
   1.1.1.6/32 (3 entries, 2 announced)
   State: <CalcForwarding>
   TSI:
   KRT in-kernel 1.1.1.6/32 -> {indirect(1048574), indirect(1048577)}
   Page 0 idx 0 Type 1 val 9219e30
   Nexthop: Self
   AS path: [2] 3 I
   Communities: target:2:1
   Path 1.1.1.6 from 1.1.1.4 Vector len 4. Val: 0
   ...#Multipath Preference: 255
   Next hop type: Indirect
   Address: 0x93f4010
   Next-hop reference count: 2
   ...
   Protocol next hop: 1.1.1.4
   Push 299824
   Indirect next hop: 944c000 1048574 INH Session ID: 0x3
   Indirect next hop: weight 0x1
   Protocol next hop: 1.1.1.5
   Push 299824
   Indirect next hop: 944c1d8 1048577 INH Session ID: 0x4
   Indirect next hop: weight 0x4000
   State: <ForwardingOnly Int Ext>
   Inactive reason: Forwarding use only
   Age: 25  Metric2: 15
   Validation State: unverified
   Task: RT
   Announcement bits (1): 0-KRT
   AS path: 3 I
   Communities: target:2:1

show route extensive (FRR and LFA)

user@host> show route 20.31.2.0 extensive
inet.0: 46 destinations, 49 routes (45 active, 0 holddown, 1 hidden)
   20.31.2.0/24 (2 entries, 1 announced)
   State: FlashAll
   TSI:
   KRT in-kernel 20.31.2.0/24 -> {Push 299776, Push 299792}
   *RSVP
   Preference: 7/1
   Next hop type: Router, Next hop index: 1048574
   Address: 0xbbbc010
   Next-hop reference count: 5
   Next hop: 10.31.1.2 via ge-2/1/8.0 weight 0x1, selected
   Label-switched-path europa-d-to-europa-e

Copyright © 2013, Juniper Networks, Inc.
show route extensive (Route Reflector)

user@host> show route extensive
1.0.0.0/8 (1 entry, 1 announced)

TSI:
KRT in-kernel 1.0.0.0/8 -> {indirect(40)}
  *BGP  Preference: 170/-101
  Source: 192.168.4.214
  Protocol next hop: 207.17.136.192 Indirect next hop: 84ac908 40
  State: <Active Int Ext>
  Local AS: 10458 Peer AS: 10458
  Age: 3:09  Metric: 0  Metric2: 0
  Task: BGP_10458.192.168.4.214+1033
  Announcement bits (2): 0-KRT 4-Resolve inet.0
  AS path: 3944 7777 I <Originator>
  Cluster list: 1.1.1.1
  Originator ID: 10.255.245.88
  Communities: 7777:7777
  Localpref: 100
  Router ID: 4.4.4.4
  Indirect next hops: 1
  Protocol next hop: 207.17.136.192 Metric: 0
  Indirect next hop: 84ac908 40
  Indirect path forwarding next hops: 0
  Next hop type: Discard

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show route label 299872 detail
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
  *LDP  Preference: 9
Next hop type: Flood
Next-hop reference count: 3
Address: 0x9097d90
Next hop: via vt-0/1/0.1
Next-hop index: 661
Label operation: Pop
Address: 0x9172130
Next hop: via so-0/0/3.0
Next-hop index: 654
Label operation: Swap 299872
State: **Active Int>
Local AS:  1001
Age: 8:20     Metric: 1
Task: LDP
Announcement bits (1): 0–KRT
AS path: I
FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1, src 192.168.142.2
show route protocol

Syntax

```
show route protocol protocol
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches)

```
show route protocol protocol
  <brief | detail | extensive | terse>
```

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `opsf2` and `ospf3` options introduced in Junos OS Release 9.2.
- `opsf2` and `ospf3` options introduced in Junos OS Release 9.2 for EX Series switches.
- `flow` option introduced in Junos OS Release 10.0.
- `flow` option introduced in Junos OS Release 10.0 for EX Series switches.

Description

Display the route entries in the routing table that were learned from a particular protocol.

Options

- `brief | detail | extensive | terse`—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to `brief`.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

`protocol`—Protocol from which the route was learned:

- `access`—Access route for use by DHCP application
- `access-internal`—Access-internal route for use by DHCP application
- `aggregate`—Locally generated aggregate route
- `arp`—Route learned through the Address Resolution Protocol
- `atmvpn`—Asynchronous Transfer Mode virtual private network
- `bgp`—Border Gateway Protocol
- `ccc`—Circuit cross-connect
- `direct`—Directly connected route
- `dvmrp`—Distance Vector Multicast Routing Protocol
- `esis`—End System-to-Intermediate System
- `flow`—Locally defined flow-specification route
- `frr`—Precomputed protection route or backup route used when a link goes down
- `isis`—Intermediate System-to-Intermediate System
- `ldp`—Label Distribution Protocol
- `l2circuit`—Layer 2 circuit
- `l2vpn`—Layer 2 virtual private network
- **local**—Local address
- **mpls**—Multiprotocol Label Switching
- **msdp**—Multicast Source Discovery Protocol
- **ospf**—Open Shortest Path First versions 2 and 3
- **ospf2**—Open Shortest Path First versions 2 only
- **ospf3**—Open Shortest Path First version 3 only
- **pim**—Protocol Independent Multicast
- **rip**—Routing Information Protocol
- **ripng**—Routing Information Protocol next generation
- **rsvp**—Resource Reservation Protocol
- **rtarget**—Local route target virtual private network
- **static**—Statically defined route
- **tunnel**—Dynamic tunnel
- **vpn**—Virtual private network

**NOTE:** EX Series switches run a subset of these protocols. See the switch CLI for details.

**List of Sample Output**
- show route protocol access on page 1612
- show route protocol access-internal extensive on page 1612
- show route protocol arp on page 1612
- show route protocol bgp on page 1613
- show route protocol bgp detail on page 1613
- show route protocol bgp extensive on page 1613
- show route protocol bgp terse on page 1614
- show route protocol direct on page 1614
- show route protocol frr on page 1615
- show route protocol l2circuit detail on page 1615
- show route protocol l2vpn extensive on page 1616
- show route protocol ldp on page 1617
- show route protocol ldp extensive on page 1617
- show route protocol ospf (Layer 3 VPN) on page 1618
- show route protocol ospf detail on page 1619
- show route protocol rip on page 1619
- show route protocol rip detail on page 1619
- show route protocol ripng table inet6 on page 1620
- show route protocol static detail on page 1620
Output Fields  For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output

show route protocol access

user@host> show route protocol access
inet.0: 30380 destinations, 30382 routes (30379 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
13.160.0.3/32 *[Access/13] 00:00:09
> to 13.160.0.2 via fe-0/0/0.0
13.160.0.4/32 *[Access/13] 00:00:09
> to 13.160.0.2 via fe-0/0/0.0
13.160.0.5/32 *[Access/13] 00:00:09
> to 13.160.0.2 via fe-0/0/0.0

show route protocol access-internal extensive

user@host> show route protocol access-internal 13.160.0.19 extensive
inet.0: 100020 destinations, 100022 routes (100019 active, 0 holddown, 1 hidden)
13.160.0.19/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.19/32 -> {13.160.0.2}
*Access-internal Preference: 12
Next-hop reference count: 200000
Next hop: 13.160.0.2 via fe-0/0/0.0, selected
State: <Active Int>
Age: 36
Task: RPD Unix Domain Server./var/run/rpd_serv.local
Announcement bits (1): 0-KRT
AS path: I

show route protocol arp

user@host> show route protocol arp
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)
inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
20.20.1.3/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
   Unusable
20.20.1.4/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
   Unusable
20.20.1.5/32 [ARP/4294967293] 00:04:32, from 20.20.1.1
   Unusable
20.20.1.6/32 [ARP/4294967293] 00:04:34, from 20.20.1.1
   Unusable
20.20.1.7/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
   Unusable
20.20.1.8/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
   Unusable
20.20.1.9/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
   Unusable
20.20.1.10/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
   Unusable
Unusable

20.20.1.11/32  [ARP/4294967293] 00:04:33, from 20.20.1.1
Unusable

20.20.1.12/32  [ARP/4294967293] 00:04:33, from 20.20.1.1
Unusable

20.20.1.13/32  [ARP/4294967293] 00:04:33, from 20.20.1.1
Unusable

show route protocol bgp

user@host> show route protocol bgp 192.168.64.0/21
inet.0: 335832 destinations, 335833 routes (335383 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.64.0/21  *[BGP/170] 6d 10:41:16, localpref 100, from 192.168.69.71
   AS path: 10458 14203 2914 4788 4788 I
   > to 192.168.167.254 via fxp0.0

show route protocol bgp detail

user@host> show route protocol bgp 66.117.63.0/24 detail
inet.0: 335805 destinations, 335806 routes (335356 active, 0 holddown, 450 hidden)
66.117.63.0/24  (1 entry, 1 announced)
   *BGP  Preference: 170/-101
      Next hop type: Indirect
      Next-hop reference count: 1006436
      Source: 192.168.69.71
      Next hop type: Router, Next hop index: 324
      Next hop: 192.168.167.254 via fxp0.0, selected
      Protocol next hop: 192.168.69.71
      Indirect next hop: 8e166c0 342
      State: <Active Ext>
      Local AS: 69 Peer AS: 10458
      Age: 6d 10:42:42  Metric2: 0
      Task: BGP_10458.192.168.69.71+179
      Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree
      1
         AS path: 10458 14203 2914 4788 4788 I
      Communities: 2914:410 2914:2403 2914:3400
      Accepted
      Localpref: 100
      Router ID: 207.17.136.192

show route protocol bgp extensive

user@host> show route protocol bgp 192.168.64.0/21 extensive
inet.0: 335827 destinations, 335828 routes (335378 active, 0 holddown, 450 hidden)
192.168.64.0/21  (1 entry, 1 announced)
TSI:
KRT in-kernel 1.9.0.0/16 -> {indirect(342)}
Page 0 idx 1 Type 1 val db31a80
   Nexthop: Self
   AS path: [69] 10458 14203 2914 4788 4788 I
   Communities: 2914:410 2914:2403 2914:3400
Path 1.9.0.0 from 192.168.69.71 Vector len 4.  Val: 1
   *BGP  Preference: 170/-101
      Next hop type: Indirect
      Next-hop reference count: 1006502
      Source: 192.168.69.71
      Next hop type: Router, Next hop index: 324
Next hop: 192.168.167.254 via fxp0.0, selected
Protocol next hop: 192.168.69.71
Indirect next hop: 8e166c0 342
State: <Active Ext>
Local AS: 69 Peer AS: 10458
Age: 6d 10:44:45 Metric2: 0
Task: BGP_10458.192.168.69.71
Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree
AS path: 10458 14203 2914 4788 4788 I
Communities: 2914:410 2914:2403 2914:3400
Accepted
Localpref: 100
Router ID: 207.17.136.192
Indirect next hops: 1
Protocol next hop: 192.168.69.71
Indirect next hop: 8e166c0 342
Indirect path forwarding next hops: 1
Next hop type: Router
Next hop: 192.168.167.254 via fxp0.0
192.168.0.0/16 Originating RIB: inet.0
Node path count: 1
Forwarding nexthops: 1
Nexthop: 192.168.167.254 via fxp0.0

show route protocol bgp terse

user@host> show route protocol bgp 192.168.64.0/21 terse

inet.0: 24 destinations, 32 routes (23 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination P Prf Metric1 Metric2 Next hop AS path
192.168.64.0/21 B 170 100 >100.1.3.2 10203 21 I

show route protocol direct

user@host> show route protocol direct

inet.0: 335843 destinations, 335844 routes (335394 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

8.8.8.0/24 *[Direct/0] 17w0d 10:31:49
  > via fe-1/3/1.0
10.255.165.1/32 *[Direct/0] 25w4d 04:13:18
  > via lo0.0
30.30.30.0/24 *[Direct/0] 17w0d 23:06:26
  > via fe-1/3/2.0
192.168.164.0/22 *[Direct/0] 25w4d 04:13:20
  > via fxp0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

47.0005.80ff.f800.0000.0108.0001.0102.5516.5001/152
  *[Direct/0] 25w4d 04:13:21
  > via lo0.0

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
show route protocol frr

user@host> show route protocol frr
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)
inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32  *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.3 via ge-4/1/0.0
    > to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.4/32  *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.4 via ge-4/1/0.0
    > to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.5/32  *[FRR/200] 00:05:35, from 20.20.1.1
    > to 20.20.1.5 via ge-4/1/0.0
    > to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.6/32  *[FRR/200] 00:05:37, from 20.20.1.1
    > to 20.20.1.6 via ge-4/1/0.0
    > to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.7/32  *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.7 via ge-4/1/0.0
    > to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.8/32  *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.8 via ge-4/1/0.0
    > to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.9/32  *[FRR/200] 00:05:38, from 20.20.1.1
    > to 20.20.1.9 via ge-4/1/0.0
    > to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)

show route protocol l2circuit detail

user@host> show route protocol l2circuit detail
mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
100000 (1 entry, 1 announced)
*L2CKT  Preference: 7
    Next hop: via ge-2/0/0.0, selected
    Label operation: Pop Offset: 4
    State: <Active Int>
    Local AS:    99
    Age: 9:52
    Task: Common L2 VC
    Announcement bits (1): 0-KRT
    AS path: I

ge-2/0/0.0 (1 entry, 1 announced)
*L2CKT  Preference: 7
    Next hop: via so-1/1/2.0 weight 1, selected
    Label-switched-path my-lsp
Label operation: Push 100000, Push 100000(top)[0] Offset: -4
Protocol next hop: 10.245.255.63
Push 100000 Offset: -4
Indirect next hop: 86af0c0 298
State: <Active Int>
Local AS:    99
Age: 9:52
Task: Common L2 VC
Announcement bits (2): 0-KRT 1-Common L2 VC
AS path: I

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  "L2CKT  Preference: 7
  Next hop: via so-1/1/2.0 weight 1, selected
  Label-switched-path my-lsp
  Label operation: Push 100000[0]
  Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
  State: <Active Int>
  Local AS:    99
  Age: 10:21
  Task: l2 circuit
  Announcement bits (1): 0-LDP
  AS path: I
  VC Label 100000, MTU 1500, VLAN ID 512

Show route protocol l2vpn extensive

user@host> show route protocol l2vpn extensive

inet.0: 14 destinations, 15 routes (13 active, 0 holddown, 1 hidden)
inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
800001 (1 entry, 1 announced)
TSI:
KRT in-kernel 800001 /36 -> {so-0/0/0.0}
  "L2VPN  Preference: 7
  Next hop: via so-0/0/0.0 weight 49087 balance 97%, selected
  Label operation: Pop  Offset: 4
  State: <Active Int>
  Local AS:    69
  Age: 7:48
  Task: Common L2 VC
  Announcement bits (1): 0-KRT
  AS path: I
so-0/0/0.0 (1 entry, 1 announced)
TSI:
KRT in-kernel so-0/0/0.0 /16 -> {indirect(288)}
  "L2VPN  Preference: 7
  Next hop: via so-0/0/1.0, selected
  Label operation: Push 800000 Offset: -4
  Push 800000 Offset: -4
  Indirect next hop: 85142a0 288
  State: <Active Int>
Local AS: 69
Age: 7:48
Task: Common L2 VC
Announcement bits (2): 0-KRT 1-Common L2 VC
AS path: I
Communities: target:69:1 Layer2-info: encaps:PPP,
control flags:2, mtu: 0

show route protocol ldp

user@host> show route protocol ldp
inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.16.1/32 *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Push 100000
192.168.17.1/32 *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0

private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100064 *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Pop
100064(S=0) *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Pop
100080 *[LDP/9] 1d 23:03:35, metric 1
> via t1-4/0/0.0, Swap 100000

show route protocol ldp extensive

user@host> show route protocol ldp extensive
192.168.16.1/32 (1 entry, 1 announced)
State: <FlashAll>
  *LDP Preference: 9
  Next-hop reference count: 3
  Next hop: via t1-4/0/0.0, selected
  Label operation: Push 100000
  State: <Active Int>
  Local AS: 65500
  Age: 1d 23:03:58 Metric: 1
  Task: LDP
  Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
  AS path: I

192.168.17.1/32 (1 entry, 1 announced)
State: <FlashAll>
  *LDP Preference: 9
  Next-hop reference count: 3
  Next hop: via t1-4/0/0.0, selected
  State: <Active Int>
  Local AS: 65500
  Age: 1d 23:03:58 Metric: 1
  Task: LDP
  Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
  AS path: I
private___.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)

100064 (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /36 -> \{t1-4/0/0.0\}
  *LDP  Preference: 9
  Next-hop reference count: 2
  Next hop: via t1-4/0/0.0, selected
  State: \<Active Int\>
  Local AS:  65500
  Age:  1d  23:03:58  Metric: 1
  Task: LDP
  Announcement bits (1): 0-KRT
  AS path: I
  Prefixes bound to route:  192.168.17.1/32

100064(S=0) (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /40 -> \{t1-4/0/0.0\}
  *LDP  Preference: 9
  Next-hop reference count: 2
  Next hop: via t1-4/0/0.0, selected
  Label operation: Pop
  State: \<Active Int\>
  Local AS:  65500
  Age:  1d  23:03:58  Metric: 1
  Task: LDP
  Announcement bits (1): 0-KRT
  AS path: I

100080 (1 entry, 1 announced)
TSI:
KRT in-kernel 100080 /36 -> \{t1-4/0/0.0\}
  *LDP  Preference: 9
  Next-hop reference count: 2
  Next hop: via t1-4/0/0.0, selected
  Label operation: Swap 100000
  State: \<Active Int\>
  Local AS:  65500
  Age:  1d  23:03:58  Metric: 1
  Task: LDP
  Announcement bits (1): 0-KRT
  AS path: I
  Prefixes bound to route:  192.168.16.1/32

show route protocol ospf (Layer 3 VPN)

user@host> show route protocol ospf
inet.0: 40 destinations, 40 routes (39 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.4/30  *[OSPF/10] 00:05:18, metric 4
  > via t3-3/2/0.0
10.39.1.8/30  *[OSPF/10] 00:05:18, metric 2
  > via t3-3/2/0.0
10.255.14.171/32  *[OSPF/10] 00:05:18, metric 4
  > via t3-3/2/0.0
10.255.14.179/32  *[OSPF/10] 00:05:18, metric 2
  > via t3-3/2/0.0
224.0.0.5/32 *[OSPF/10] 20:25:55, metric 1

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30 [OSPF/10] 00:05:43, metric 1
  > via so-0/2/2.0

10.255.14.173/32 *[OSPF/10] 00:05:43, metric 1
  > via so-0/2/2.0

224.0.0.5/32 *[OSPF/10] 20:26:20, metric 1

show route protocol ospf detail

user@host> show route protocol ospf detail
VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30 (2 entries, 0 announced)
  OSPF     Preference: 10
  Nexthop: via so-0/2/2.0, selected
  State: <Int>
  Inactive reason: Route Preference
  Age: 6:25   Metric: 1
  Area: 0.0.0.0
  Task: VPN-AB-OSPF
  AS path: I
  Communities: Route-Type:0.0.0.0:1:0

...
show route protocol ripng table inet6

user@host> show route protocol ripng table inet6
inet6: 4215 destinations, 4215 routes (4214 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

1111::1/128  *[RIPng/100] 02:13:33, metric 2
  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0

1111::2/128  *[RIPng/100] 02:13:33, metric 2
  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0

1111::3/128  *[RIPng/100] 02:13:33, metric 2
  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0

1111::4/128  *[RIPng/100] 02:13:33, metric 2
  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0

1111::5/128  *[RIPng/100] 02:13:33, metric 2
  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0

1111::6/128  *[RIPng/100] 02:13:33, metric 2
  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0

show route protocol static detail

user@host> show route protocol static detail
inet: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

10.5.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.13.10.0/23 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
Task: RT
Announcement bits (1): 0-KRT
AS path: I

Other Operational Commands
clear security pki local-certificate

Syntax

```
clear security pki local-certificate
<all | certificate-id certificate-id-name | system-generated>
```

Release Information

Command introduced in Junos OS Release 11.1 for EX Series switches.

Description

Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the switch.

Options

```
all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.
```

```
NOTE: This option does not delete the automatically generated self-signed certificate or its public/private key pair.
```

```
certificate-id certificate-id-name—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.
```

```
system-generated—(Optional) Delete the automatically generated self-signed certificate.
```

Required Privilege Level

Clear

Related Documentation

- Deleting Self-Signed Certificates (CLI Procedure) on page 1255

List of Sample Output

```
clear security pki local-certificate all on page 1622
```

Output Fields

This command produces no output.

Sample Output

```
clear security pki local-certificate all

user@switch> clear security pki local-certificate all
```
clear system services dhcp binding

Syntax

```
clear system services dhcp binding
<address>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(J Series routers and EX Series switches only) Remove obsolete IP address bindings on a Dynamic Host Configuration Protocol (DHCP) server and return them to the IP address pool.

Options

```
address—(Optional) Remove a specific IP address binding and return it to the address pool.
```

Required Privilege Level

view and system

Related Documentation

• show system services dhcp binding on page 1636

List of Sample Output

```
clear system services dhcp binding on page 1623
```

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp binding

```
user@host> clear system services dhcp binding
```

Copyright © 2013, Juniper Networks, Inc.
clear system services dhcp conflict

**Syntax**
```
clear system services dhcp conflict
<address>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
(J Series routers and EX Series switches only) Remove IP addresses from the Dynamic Host Configuration Protocol (DHCP) server conflict list and return them to the IP address pool.

**Options**
- `address`—(Optional) Remove a specific IP address from the conflict list and return it to the address pool.

**Required Privilege**
- view and system

**Related Documentation**
- show system services dhcp conflict on page 1639

**List of Sample Output**
clear system services dhcp conflict on page 1624

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear system services dhcp conflict
```
user@host> clear system services dhcp conflict
```
clear system services dhcp statistics

<table>
<thead>
<tr>
<th>Syntax</th>
<th>clear system services dhcp statistics</th>
</tr>
</thead>
</table>
| **Release Information** | Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches. |
| **Description** | (J Series routers and EX Series switches only) Clear Dynamic Host Configuration Protocol (DHCP) server statistics. |
| **Options** | This command has no options. |
| **Required Privilege Level** | view and system |
| **Related Documentation** | • show system services dhcp statistics on page 1644 |
| **List of Sample Output** | clear system services dhcp statistics on page 1625 |
| **Output Fields** | When you enter this command, you are provided feedback on the status of your request. |

**Sample Output**
clear system services dhcp statistics

```bash
user@host> clear system services dhcp statistics
```
request ipsec switch

Syntax  request ipsec switch (interface <es-fpc/pic/port> | security-associations <sa-name> )

Release Information  Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description  (Encryption interface on M Series, PTX Series, and T Series routers and EX Series switches only) Manually switch from the primary to the backup encryption services interface, or switch from the primary to the backup IP Security (IPsec) tunnel.

Options  interface <es-fpc/pic/port>—Switch to the backup encryption interface.
security-associations <sa-name>—Switch to the backup tunnel.

Required Privilege  view

Related Documentation  • show ipsec redundancy

List of Sample Output  request ipsec switch on page 1626

Output Fields  When you enter this command, you are provided feedback on the status of your request.

Sample Output  request ipsec switch

user@host> request ipsec switch security-associations sa-private
**request security certificate (signed)**

**Syntax**
```
request security certificate enroll filename filename subject subject alternative-subject alternative-subject certification-authority certification-authority encoding (binary | pem) key-file key-file domain-name domain-name
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
(Encryption interface on M Series and T Series routers and EX Series switches only)
Obtain a signed certificate from a certificate authority (CA). The signed certificate validates the CA and the owner of the certificate. The results are saved in a specified file to the /var/etc/ikecert directory.

**Options**
- `filename` *filename*—File that stores the certificate.
- `subject` *subject*—Distinguished name (dn), which consists of a set of components—for example, an organization (o), an organization unit (ou), a country (c), and a locality (l).
- `alternative-subject` *alternative-subject*—Tunnel source address.
- `certification-authority` *certification-authority*—Name of the certificate authority profile in the configuration.
- `encoding` *(binary | pem)*—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default format is binary.
- `key-file` *key-file*—File containing a local private key.
- `domain-name` *domain-name*—Fully qualified domain name.

**Required Privilege Level**
maintenance

**List of Sample Output**
`request security certificate (signed)` on page 1627

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
```
user@host> request security certificate enroll filename host.crt subject c=uk,o=London alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv domain-name host.juniper.net
CA name: juniper.net CA file: ca_verisign local pub/private key pair: host.prv subject: c=uk,o=London domain name: host.juniper.net alternative subject: 10.50.1.4 Encoding: binary
```
Certificate enrollment has started. To view the status of your enrollment, check the key management process (kmd) log file at /var/log/kmd.
request security certificate (unsigned)

Syntax
request security certificate enroll filename filename ca-file ca-file ca-name ca-name encoding (binary | perm) url url

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
(Encryption interface on M Series and T Series routers and EX Series switches only)
Obtain a certificate from a certificate authority (CA). The results are saved in a specified file to the /var/etc/ikecert directory.

Options
filename — File that stores the public key certificate.
ca-file — Name of the certificate authority profile in the configuration.
ca-name — Name of the certificate authority.
encoding (binary | pem) — File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default value is binary.
url — Certificate authority URL.

Required Privilege
Level maintenance

List of Sample Output
request security certificate (unsigned) on page 1629

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
request security certificate (unsigned)

user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name juniper.net url xyzcompany URL
http://<verisign ca-name xyzcompany url>/cgi-bin/pkcclient.exe CA name: juniper.net
CA file: verisign Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check the key management process (kmd) log file at /var/log/kmd. <--------------
request security key-pair

Syntax  
request security key-pair filename
<size key-size>
<type (rsa | dsa)>

Release Information  
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description  
(Encryption interface on M Series and T Series routers and EX Series switches only)
Generate a public and private key pair for a digital certificate.

Options  
filename—Name of a file in which to store the key pair.

size key-size—(Optional) Key size, in bits. The key size can be 512, 1024, or 2048. The default value is 1024.

type—(Optional) Algorithm used to encrypt the key:
  • rsa—RSA algorithm. This is the default.
  • dsa—Digital signature algorithm with Secure Hash Algorithm (SHA).

Required Privilege  
Level maintenance

List of Sample Output  
request security key-pair on page 1630

Output Fields  
When you enter this command, you are provided feedback on the status of your request.

Sample Output  
request security key-pair

user@host> request security key-pair security-key-file
**request security pki generate-key-pair**

**Syntax**
request security pki generate-key-pair certificate-id certificate-id-name
<size (512 | 1024 | 2048)><type (dsa | rsa)>

**Release Information**
Command introduced in Junos OS Release 11.1 for EX Series switches.

**Description**
Generate a public key infrastructure (PKI) public/private key pair for a local digital certificate.

**Options**
certificate-id certificate-id-name—Name of the local digital certificate and the public/private key pair.

size—(Optional) Key pair size. The key pair size can be 512, 1024, or 2048 bits. If a key pair size is not specified, the default value, 1024 bits, is applied.

type—(Optional) The algorithm to be used for encrypting the public/private key pair. The encryption algorithm can be dsa or rsa. If an encryption algorithm is not specified, the default value, rsa, is applied.

**Required Privilege Level**
maintenance

**Related Documentation**
- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 1254

**List of Sample Output**
request security pki generate-key-pair on page 1631

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
request security pki generate-key-pair

user@switch> request security pki generate-key-pair certificate-id billy size 2048
Generated key pair billy, key size 2048 bits
request security pki local-certificate generate-self-signed

Syntax
request security pki local-certificate generate-self-signed certificate-id certificate-id-name
domain-name domain-name ip-address ip-address email email-address
subject subject-distinguished-name

Release Information
Command introduced in Junos OS Release 11.1 for EX Series switches.

Description
Manually generate a self-signed certificate for the given distinguished name.

Options
- **certificate-id certificate-id-name**—Name of the local digital certificate and the public/private key pair.
- **domain-name domain-name**—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.
- **email email-address**—E-mail address of the certificate holder.
- **ip-address ip-address**—IP address of the switch.
- **subject subject-distinguished-name**—Distinguished name format that contains the common name, department, company name, state, and country:
  - **CN**—Common name
  - **OU**—Organizational unit name
  - **O**—Organization name
  - **ST**—State
  - **C**—Country

Required Privilege
- **Level**
  - maintenance
  - security

Related Documentation
- Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 1254

List of Sample Output
request security pki local-certificate generate-self-signed on page 1632

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
request security pki local-certificate generate-self-signed

user@switch> request security pki local-certificate generate-self-signed certificate-id self-cert
subject cn=abc domain-name abc.net email jdoe@abc.net
Self-signed certificate generated and loaded successfully
show security pki local-certificate

Syntax  
show security pki local-certificate  
  <brief | detail>  
  <certificate-id certificate-id-name>  
  <system-generated>

Release Information  
Command introduced in Junos OS Release 11.1 for EX Series switches.

Description  
Display information about the local digital certificates and the corresponding public keys installed in the switch.

Options  
none—(Same as brief) Display information about all local digital certificates and corresponding public keys.

brief | detail—(Optional) Display information about local digital certificates and corresponding public keys for the specified level of output.

certificate-id certificate-id-name—(Optional) Display information about only the specified local digital certificate and corresponding public keys.

system-generated—(Optional) Display information about the automatically generated self-signed certificate.

Required Privilege  
Level view

Related Documentation  
• Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 1254

List of Sample Output  
show security pki local-certificate on page 1634
show security pki local-certificate detail on page 1635

Output Fields  
Table 191 on page 1633 lists the output fields for the show security pki local-certificate command. Output fields are listed in the approximate order in which they appear.

Table 191: show security pki local-certificate Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate identifier</td>
<td>Name of the digital certificate.</td>
<td>All levels</td>
</tr>
<tr>
<td>Certificate version</td>
<td>Revision number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Serial number</td>
<td>Unique serial number of the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Issued by</td>
<td>Authority that issued the digital certificate.</td>
<td>none brief</td>
</tr>
<tr>
<td>Issued to</td>
<td>Device that was issued the digital certificate.</td>
<td>none brief</td>
</tr>
</tbody>
</table>
Table 191: show security pki local-certificate Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>Authority that issued the digital certificate, including details of the authority</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>organized using the distinguished name format. Possible subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Common name—Name of the authority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organization—Organization of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organizational unit—Department within an organization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—State of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Country—Country of origin.</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>Details of the digital certificate holder organized using the distinguished name</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>format. Possible subfields are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Common name—Name of the authority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organization—Organization of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Organizational unit—Department within an organization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—State of origin.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Country—Country of origin.</td>
<td></td>
</tr>
<tr>
<td>Alternate subject</td>
<td>Domain name or IP address of the device related to the digital certificate.</td>
<td>detail</td>
</tr>
<tr>
<td>Validity</td>
<td>Time period when the digital certificate is valid. Values are:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Not before—Start time when the digital certificate becomes valid.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Not after—End time when the digital certificate becomes invalid.</td>
<td></td>
</tr>
<tr>
<td>Public key algorithm</td>
<td>Encryption algorithm used with the private key, such as rsaEncryption (1024 bits).</td>
<td>All levels</td>
</tr>
<tr>
<td>Public key verification status</td>
<td>Public key verification status: Failed or Passed. The detail output also provides</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>the verification hash.</td>
<td></td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>Encryption algorithm that the CA used to sign the digital certificate, such as</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>sha1WithRSAEncryption.</td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>the digital certificate.</td>
<td></td>
</tr>
<tr>
<td>Distribution CRL</td>
<td>Distinguished name information and URL for the certificate revocation list (CRL)</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>server.</td>
<td></td>
</tr>
<tr>
<td>Use for key</td>
<td>Use of the public key, such as Certificate signing, CRL signing, Digital signature,</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>or Key encipherment.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

type=show

title=show security pki local-certificate

user@switch> show security pki local-certificate
Certificate identifier: local-entrust2
   Issued to: router2.juniper.net, Issued by: juniper
Validity:
Not after: 2008 Nov 21st, 23:58:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed

show security pki local-certificate detail

user@switch> show security pki local-certificate detail
Certificate identifier: local-entrust3
Certificate version: 3
Serial number: 4355 94f9
Issuer:
   Organization: juniper, Country: us
Subject:
   Organization: juniper, Country: us, Common name: switch1.juniper.net
Alternate subject: switch1.juniper.net
Validity:
   Not after: 2008 Nov 22nd, 00:03:58 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
Distribution CRL:
   C=us, O=juniper, CN=CRL1
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature
show system services dhcp binding

Syntax

show system services dhcp binding
<detail>
<address>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
(J Series routers only) Display Dynamic Host Configuration Protocol (DHCP) server client binding information.

Options
none—Display brief information about all active client bindings.
detail—(Optional) Display detailed information about all active client bindings.
address—(Optional) Display detailed client binding information for the specified IP address only.

Required Privilege
view and system

Related Documentation
• clear system services dhcp binding on page 1623

List of Sample Output
show system services dhcp binding on page 1637
show system services dhcp binding address on page 1637
show system services dhcp binding address detail on page 1637

Output Fields
Table 192 on page 1636 describes the output fields for the show system services dhcp binding command. Output fields are listed in the approximate order in which they appear.

Table 192: show system services dhcp binding Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allocated address</td>
<td>List of IP addresses the DHCP server has assigned to clients.</td>
<td>All levels</td>
</tr>
<tr>
<td>MAC address</td>
<td>Corresponding media access control (MAC) hardware address of the client.</td>
<td>All levels</td>
</tr>
<tr>
<td>Client identifier</td>
<td>(address option only) Client's unique identifier (represented by an ASCII string or hexadecimal digits). This identifier is used by the DHCP server to index its database of address bindings.</td>
<td>All levels</td>
</tr>
<tr>
<td>Binding Type</td>
<td>Type of binding assigned to the client. DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.</td>
<td>All levels</td>
</tr>
<tr>
<td>Lease Expires at</td>
<td>Time the lease expires or never for leases that do not expire.</td>
<td>All levels</td>
</tr>
<tr>
<td>Lease Obtained at</td>
<td>(address option only) Time the client obtained the lease from the DHCP server.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 192: show system services dhcp binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Status of the binding. Bindings can be active or expired.</td>
<td>detail</td>
</tr>
<tr>
<td>Pool</td>
<td>Address pool that contains the IP address assigned to the client.</td>
<td>detail</td>
</tr>
<tr>
<td>Request received on</td>
<td>Interface on which the DHCP message exchange occurs. The IP address pool is</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>configured based on the interface's IP address. If a relay agent is used, its IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address is also displayed.</td>
<td></td>
</tr>
<tr>
<td>DHCP options</td>
<td>User-defined options created for the DHCP server. If no options have been defined</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>this field is blank.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show system services dhcp binding

```
user@host> show system services dhcp binding
Allocated address    MAC address   Binding Type   Lease expires at
192.168.1.2        00:a0:12:00:12:ab  static         never
192.168.1.3        00:a0:12:00:13:02  dynamic        2004-05-03 13:01:42 PDT
```

show system services dhcp binding address

```
user@host> show system services dhcp binding 192.168.1.3
DHCP binding information:
Allocated address: 192.168.1.3
Mac address: 00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30aced-00:a0:12:00:3a 31 33 3a 30 32:13:02
Lease information:
  Binding Type dynamic
  Obtained at 2004-05-02 13:01:42 PDT
  Expires at 2004-05-03 13:01:42 PDT
```

show system services dhcp binding address detail

```
user@host> show system services dhcp binding 192.168.1.3 detail
DHCP binding information:
Allocated address 192.168.1.3
MAC address 00:a0:12:00:12:ab
Pool 192.168.1.0/24
Request received on fe-0/0/0, relayed by 192.168.4.254
Lease information:
  Type DHCP
  Obtained at 2004-05-02 13:01:42 PDT
  Expires at 2004-05-03 13:01:42 PDT
  State active
  DHCP options:
    Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
```
Name: domain-name, Value: mydomain.tld
Code: 19, Type: flag, Value: off
Code: 40, Type: string, Value: domain.tld
Code: 32, Type: ip-address, Value: 3.3.3.33
show system services dhcp conflict

Syntax

show system services dhcp conflict

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(J Series routers only and EX Series switches) Display Dynamic Host Configuration Protocol (DHCP) client-detected conflicts for IP addresses. When a conflict is detected, the DHCP server removes the address from the address pool.

Options

This command has no options.

Required Privilege Level

view and system

Related Documentation

- clear system services dhcp conflict on page 1624

List of Sample Output

show system services dhcp conflict on page 1639

Output Fields

Table 193 on page 1639 describes the output fields for the show system services dhcp conflict command. Output fields are listed in the approximate order in which they appear.

Table 193: show system services dhcp conflict Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection time</td>
<td>Date and time the client detected the conflict.</td>
</tr>
<tr>
<td>Detection method</td>
<td>How the conflict was detected.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address where the conflict occurs. The addresses in the conflicts list remain excluded from the pool until you use a clear system services dhcp conflict command to manually clear the list.</td>
</tr>
</tbody>
</table>

Sample Output

show system services dhcp conflict

user@host> show system services dhcp conflict

<table>
<thead>
<tr>
<th>Detection time</th>
<th>Detection method</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004-08-03 19:04:00 PDT</td>
<td>ARP</td>
<td>3.3.3.5</td>
</tr>
<tr>
<td>2004-08-04 04:23:12 PDT</td>
<td>Ping</td>
<td>4.4.4.8</td>
</tr>
<tr>
<td>2004-08-05 21:06:44 PDT</td>
<td>Client</td>
<td>3.3.3.10</td>
</tr>
</tbody>
</table>
show system services dhcp global

**Syntax**

```
show system services dhcp global
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) global configuration options. Global options apply to all scopes and clients served by the DHCP server. Global options are overridden if specified otherwise in scope or client options. Scope options apply to specific subnets or ranges of addresses. Client options apply to specific clients.

**Options**
This command has no options.

**Required Privilege**
view and system

**List of Sample Output**
show system services dhcp global on page 1641

**Output Fields**
Table 194 on page 1640 describes the output fields for the show system services dhcp global command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTP lease length</td>
<td>Length of lease time assigned to BOOTP clients.</td>
</tr>
<tr>
<td>Default lease time</td>
<td>Lease time assigned to clients that do not request a specific lease time.</td>
</tr>
<tr>
<td>Minimum lease time</td>
<td>Minimum time a client retains an IP address lease on the server.</td>
</tr>
<tr>
<td>Maximum lease time</td>
<td>Maximum time a client can retain an IP address lease on the server.</td>
</tr>
<tr>
<td>DHCP options</td>
<td>User-defined options created for the DHCP server. If no options have been defined, this field is blank.</td>
</tr>
</tbody>
</table>
Sample Output

show system services dhcp global

user@host> show system services dhcp global

Global settings:
  BOOTP lease length        infinite

DHCP lease times:
  Default lease time        1 hour
  Minimum lease time        2 hours
  Maximum lease time        infinite

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
  Name: domain-name, Value: mydomain.tld
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 3.3.3.33
show system services dhcp pool

Syntax

show system services dhcp pool
<detail>
<subnet-address>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server IP address pools.

Options

none—Display brief information about all IP address pools.

detail—(Optional) Display detailed information.

subnet-address—(Optional) Display information for the specified subnet address.

Required Privilege

view and system

List of Sample Output

show system services dhcp pool on page 1643
show system services dhcp pool subnet-address on page 1643
show system services dhcp pool subnet-address detail on page 1643

Output Fields

Table 195 on page 1642 describes the output fields for the show system services dhcp pool command. Output fields are listed in the approximate order in which they appear.

Table 195: show system services dhcp pool Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool name</td>
<td>Subnet on which the IP address pool is defined.</td>
<td>None specified</td>
</tr>
<tr>
<td>Low address</td>
<td>Lowest address in the IP address pool.</td>
<td>None specified</td>
</tr>
<tr>
<td>High address</td>
<td>Highest address in the IP address pool.</td>
<td>None specified</td>
</tr>
<tr>
<td>Excluded addresses</td>
<td>Addresses excluded from the address pool.</td>
<td>None specified</td>
</tr>
<tr>
<td>Subnet</td>
<td>(subnet-address option only) Subnet to which the specified address pool belongs.</td>
<td>None specified</td>
</tr>
<tr>
<td>Address range</td>
<td>(subnet-address option only) Range of IP addresses in the address pool.</td>
<td>None specified</td>
</tr>
<tr>
<td>Addresses assigned</td>
<td>Number of IP addresses in the pool that are assigned to DHCP clients and the total number of IP addresses in the pool.</td>
<td>detail</td>
</tr>
<tr>
<td>Active</td>
<td>Number of assigned IP addresses in the pool that are active.</td>
<td>detail</td>
</tr>
<tr>
<td>Excluded</td>
<td>Number of assigned IP addresses in the pool that are excluded.</td>
<td>detail</td>
</tr>
<tr>
<td>Default lease time</td>
<td>Lease time assigned to clients that do not request a specific lease time.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 195: show system services dhcp pool Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum lease time</td>
<td>Minimum time a client can retain an IP address lease on the server.</td>
<td>detail</td>
</tr>
<tr>
<td>Maximum lease time</td>
<td>Maximum time a client can retain an IP address lease on the server.</td>
<td>detail</td>
</tr>
<tr>
<td>DHCP options</td>
<td>User-defined options created for the DHCP server. If no options have been defined, this field is blank.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show system services dhcp pool

```
user@host> show system services dhcp pool

Pool name    Low address   High address   Excluded addresses
3.3.3.0/24   3.3.3.2       3.3.3.254      3.3.3.1
```

show system services dhcp pool subnet-address

```
user@host> show system services dhcp pool 3.3.3.0/24

Pool information:
  Subnet                     3.3.3.0/24
  Address range              3.3.3.2 - 3.3.3.254
  Addresses assigned         2/253
```

show system services dhcp pool subnet-address detail

```
user@host> show system services dhcp pool 3.3.3.0/24 detail

Pool information:
  Subnet                     3.3.3.0/24
  Address range              3.3.3.2 - 3.3.3.254
  Addresses assigned         2/253
  Active: 1, Excluded: 1

DHCP lease times:
  Default lease time         1 hour
  Minimum lease time         2 hours
  Maximum lease time         infinite

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
  Name: domain-name, Value: mydomain.tld
  Name: router, Value: { 3.3.3.1 }
  Name: server-identifier, Value: 3.3.3.1
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 3.3.3.333.3.3.254 3.3.3.1
```
**show system services dhcp statistics**

**Syntax**

show system services dhcp statistics

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server statistics.

**Options**

This command has no options.

**Required Privilege Level**

view and system

**Related Documentation**

- clear system services dhcp statistics on page 1625

**List of Sample Output**

show system services dhcp statistics on page 1645

**Output Fields**

Table 196 on page 1644 describes the output fields for the `show system services dhcp statistics` command. Output fields are listed in the approximate order in which they appear.

Table 196: show system services dhcp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default lease time</td>
<td>Lease time assigned to clients that do not request a specific lease time.</td>
</tr>
<tr>
<td>Minimum lease time</td>
<td>Minimum time a client can retain an IP address lease on the server.</td>
</tr>
<tr>
<td>Maximum lease time</td>
<td>Maximum time a client can retain an IP address lease on the server.</td>
</tr>
<tr>
<td>Packets dropped</td>
<td>Total number of packets dropped and number of packets dropped because of:</td>
</tr>
<tr>
<td></td>
<td>• Invalid hardware address</td>
</tr>
<tr>
<td></td>
<td>• Invalid opcode</td>
</tr>
<tr>
<td></td>
<td>• Invalid server address</td>
</tr>
<tr>
<td></td>
<td>• No available address</td>
</tr>
<tr>
<td></td>
<td>• No interface match</td>
</tr>
<tr>
<td></td>
<td>• No routing instance match</td>
</tr>
<tr>
<td></td>
<td>• No valid local addresses</td>
</tr>
<tr>
<td></td>
<td>• Packet too short</td>
</tr>
<tr>
<td></td>
<td>• Read error</td>
</tr>
<tr>
<td></td>
<td>• Send error</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Table 196: show system services dhcp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages received</td>
<td>Number of the following message types sent from DHCP clients and received by the DHCP server:</td>
</tr>
<tr>
<td></td>
<td>• BOOTREQUEST</td>
</tr>
<tr>
<td></td>
<td>• DHCPDECLINE</td>
</tr>
<tr>
<td></td>
<td>• DHCPDISCOVER</td>
</tr>
<tr>
<td></td>
<td>• DHCPINFORM</td>
</tr>
<tr>
<td></td>
<td>• DHCPRELEASE</td>
</tr>
<tr>
<td></td>
<td>• DHCPREQUEST</td>
</tr>
<tr>
<td>Messages sent</td>
<td>Number of the following message types sent from the DHCP server to DHCP clients:</td>
</tr>
<tr>
<td></td>
<td>• BOOTREPLY</td>
</tr>
<tr>
<td></td>
<td>• DHCPACK</td>
</tr>
<tr>
<td></td>
<td>• DHCPOFFER</td>
</tr>
<tr>
<td></td>
<td>• DHCPNAK</td>
</tr>
</tbody>
</table>

Sample Output
show system services dhcp statistics

user@host> show system services dhcp statistics

DHCP lease times:
  Default lease time   1 hour
  Minimum lease time   2 hours
  Maximum lease time   infinite

Packets dropped:
  Total                0
  Bad hardware address 0
  Bad opcode           0
  Invalid server address 0
  No available addresses 0
  No interface match   0
  No routing instance match 0
  No valid local address 0
  Packet too short    0
  Read error          0
  Send error          0

Messages received:
  BOOTREQUEST          0
  DHCPDECLINE          0
  DHCPDISCOVER         0
  DHCPINFORM           0
  DHCPRELEASE          0
  DHCPREQUEST          0

Messages sent:
  BOOTREPLY            0
  DHCPACK              0
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPOFFER</td>
<td>0</td>
</tr>
<tr>
<td>DHCPNAK</td>
<td>0</td>
</tr>
</tbody>
</table>
show system services service-deployment

Syntax show system services service-deployment


Description Display information about a Session and Resource Control (SRC) client.

Options This command has no options.

Required Privilege Level system view

List of Sample Output show system services service-deployment on page 1647

Output Fields Table 197 on page 1647 lists the output fields for the show system services service-deployment command. Output fields are listed in the approximate order in which they appear.

Table 197: show system services service-deployment Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDT Keepalive settings</td>
<td>Configured PDT keepalive interval, in seconds.</td>
</tr>
<tr>
<td>Keepalives sent</td>
<td>Number of keepalives sent</td>
</tr>
<tr>
<td>Notifications sent</td>
<td>Number of notifications sent</td>
</tr>
<tr>
<td>Last update from peer</td>
<td>Time at which the last update from a peer was received.</td>
</tr>
</tbody>
</table>

Sample Output show system services service-deployment

user@host> show system services service-deployment
Connected to 192.4.4.4 port 10288 since 2004-05-03 11:04:34 PDT
Keepalive settings: Interval 15 seconds
Keepalives sent: 750
Notifications sent: 0
Last update from peer: 00:00:06 ago
ssh

Syntax

ssh host
  <bypass-routing>
  <inet | inet6>
  <interface interface-name>
  <logical-system logical-system-name>
  <routing-instance routing-instance-name>
  <source address>
  <v1 | v2>

Syntax (EX Series Switch and the QFX Series)

ssh host
  <bypass-routing>
  <inet | inet6>
  <interface interface-name>
  <routing-instance routing-instance-name>
  <source address>
  <v1 | v2>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Use the SSH program to open a connection between a local router or switch and a remote system and execute commands on the remote system. You can issue the ssh command from the Junos OS CLI to log in to a remote system or from a remote system to log in to the local router or switch. When executing this command, you include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons:

ssh address 'cli-command1 ; cli-command2'

Options

host—Name or address of the remote system.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Create an IPv4 or IPv6 connection, respectively.

interface interface-name—(Optional) Interface name for the SSH session. (This option does not work when default-address-selection is configured at the [edit system] hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system logical-system-name—(Optional) Name of a particular logical system for the SSH attempt.

routing-instance routing-instance-name—(Optional) Name of the routing instance for the SSH attempt.
source address—(Optional) Source address of the SSH connection.

v1 | v2—(Optional) Use SSH version 1 or 2, respectively, when connecting to a remote host.

Additional Information
To configure an SSH (version 1) key for your user account, include the authentication ssh-rsa statement at the [edit system login user user-name] hierarchy level. To configure an SSH (version 2) key for your user account, include the authentication dsa-rsa statement at the [edit system login user user-name] hierarchy level.

You can limit the number of times a user can attempt to enter a password while logging in through SSH. To specify the number of times a user can attempt to enter a password to log in through SSH, include the retry-options statement at the [edit system login] hierarchy level. For details, see the .

Required Privilege
Level
network

Related Documentation
- Configuring SSH Host Keys for Secure Copying of Data

List of Sample Output
ssh on page 1649

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@switch> ssh cree
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes

Host ?cree' added to the list of known hosts.
boojun@cree's password:
Last login: Sun Jun 21 10:43:42 1998 from junos-router
% ...
```
telnet

Syntax

telnet host
<8bit>
<bypass-routing>
<inet | inet6>
<interface interface-name>
<logical-system logical-system-name>
<no-resolve>
<port port-number>
<routing-instance routing-instance-name>
<source source-address>

Syntax (EX Series Switches)
telnet host
<8bit>
<bypass-routing>
<inet | inet6>
<interface interface-name>
<no-resolve>
<port port-number>
<routing-instance routing-instance-name>
<source source-address>

Release Information


Description

Open a telnet session to a remote system. Type Ctrl+] to escape from the telnet session to the telnet command level, and then type quit to exit from telnet.

Options

host—Name or address of the remote system.

8bit—(Optional) Use an 8-bit data path.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Open an IPv4 or IPv6 session, respectively.

interface interface-name—(Optional) Interface name for the telnet session. (This option does not work when default-address-selection is configured at the [edit system] hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system logical-system-name—(Optional) Name of a particular logical system for the telnet attempt.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

port port-number—(Optional) Port number or service name on the remote system.
**Routing-Instance** *(Optional)* Name of the routing instance for the telnet attempt.

**Source** *(Optional)* Source address of the telnet connection.

**Additional Information**
You can limit the number of times a user can attempt to enter a password while logging in through telnet. To specify the number of times a user can attempt to enter a password to log in through telnet, include the `retry-options` statement at the `[edit system login]` hierarchy level. For details, see the *Junos OS Administration Library for Routing Devices*.

**Required Privilege Level**
- network

**List of Sample Output**
- [Telnet on page 1651](#)

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
telnet
user@host> telnet 192.154.1.254
Trying 192.154.169.254...
Connected to level5.company.net.
Escape character is '^]'.
ttyp
login:
```
PART 10

Access Control

- Overview on page 1655
- Configuration on page 1675
- Administration on page 1813
CHAPTER 28

Overview

- Access Control Overview on page 1655

Access Control Overview

- 802.1X for EX Series Switches Overview on page 1655
- Understanding Authentication on EX Series Switches on page 1658
- Understanding Guest VLANs for 802.1X on EX Series Switches on page 1664
- Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 1664
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665
- Understanding 802.1X and VoIP on EX Series Switches on page 1668
- Understanding 802.1X and VSAs on EX Series Switches on page 1670
- Understanding Dynamic VLANs for 802.1X on EX Series Switches on page 1670
- Understanding Server Fail Fallback and Authentication on EX Series Switches on page 1671
- Authentication Process Flow for EX Series Switches on page 1672
- Understanding Authentication Session Timeout on page 1673

802.1X for EX Series Switches Overview

IEEE 802.1X provides network edge security, protecting Ethernet LANs from unauthorized user access.

How 802.1X Authentication Works

802.1X authentication works by using an Authenticator Port Access Entity (the switch) to block all traffic to and from a supplicant (end device) at the port until the supplicant's credentials are presented and matched on the Authentication server (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The end device is authenticated in either single mode, single-secure mode, or multiple mode:

- single—Authenticates only the first end device. All other end devices that connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the end devices' authentication.
• **single-secure**—Allows only one end device to connect to the port. No other end device is allowed to connect until the first logs out.

• **multiple**—Allows multiple end devices to connect to the port. Each end device will be authenticated individually.

Network access can be further defined using VLANs and firewall filters, which both act as filters to separate and match groups of end devices to the areas of the LAN they require. For example, you can configure VLANs to handle different categories of authentication failures depending upon:

• Whether or not the end device is 802.1X-enabled.

• Whether or not MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected.

• Whether the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message. See “Configuring Server Fail Fallback (CLI Procedure)” on page 1752.

**802.1X Features Overview**

**NOTE:** The 802.1X features available on the switches depend upon which switch you are using. See “EX Series Switch Software Features Overview” on page 27 for a complete list of the Junos OS 802.1X features that are supported on specific switches.

802.1X features on Juniper Networks EX Series Ethernet Switches are:

• Guest VLAN—Provides limited access to a LAN, typically just to the Internet, for nonresponsive end devices that are not 802.1X-enabled when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected. Also, a guest VLAN can be used to provide limited access to a LAN for guest users. Typically, the guest VLAN provides access just to the Internet and to other guests’ end devices.

• Server-reject VLAN—Provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials.

• Server-fail VLAN—Provides limited access to a LAN, typically just to the Internet, for 802.1X end devices during a RADIUS server timeout.

• Dynamic VLAN—Enables an end device, after authentication, to be a member of a VLAN dynamically.

• Private VLAN—Enables configuration of 802.1X authentication on interfaces that are members of private VLANs (PVLANs).

• Dynamic changes to a user session—Allows the switch administrator to terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
• Support for VoIP—Supports IP telephones. If the phone is 802.1X-enabled, it is authenticated like any other supplicant. If the phone is not 802.1X-enabled, but has another 802.1X-compatible device connected to its data port, that device is authenticated, and then VoIP traffic can flow to and from the phone (providing that the interface is configured in single mode and not in single-secure mode).

NOTE: Configuring a VoIP VLAN on private VLAN (PVLAN) interfaces is not supported.

• RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription.

• Vendor Specific Attributes (VSAs)—Supports the Juniper-Switching-Filter attribute on the RADIUS authentication server that can be used further define a supplicant's access during the 802.1X authentication process. Centrally configuring VSAs on the authentication server does away with the need to configure these same attributes in the form of firewall filters on every switch in the LAN to which the supplicant may connect to the LAN. This feature is based on RLI 4583, AAA RADIUS BRAS VSA Support.

Supported Features Related to 802.1X Authentication

802.1X does not replace other security technologies. 802.1X works together with port security features, such as DHCP snooping, dynamic ARP inspection (DAI), and MAC limiting, to guard against spoofing.

Supported features related to authentication include:

• Static MAC bypass—Provides a bypass mechanism to authenticate devices that are not 802.1X-enabled (such as printers). Static MAC bypass connects these devices to 802.1X-enabled ports, bypassing 802.1X authentication.

• MAC RADIUS authentication—Provides a means to enable or disable MAC authentication independently of whether 802.1X authentication is enabled.

NOTE: You cannot configure 802.1X authentication on redundant trunk groups (RTGs).

Related Documentation

• Understanding Authentication on EX Series Switches on page 1658
• Understanding 802.1X and VoIP on EX Series Switches on page 1668
• Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665
• Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 1664
• Understanding Guest VLANs for 802.1X on EX Series Switches on page 1664
• Understanding 802.1X and VSAs on EX Series Switches on page 1670
Understanding Authentication on EX Series Switches

You can control access to your network through a Juniper Networks EX Series Ethernet Switch using several different authentication methods—802.1X, MAC RADIUS, or captive portal. Authentication prevents unauthorized devices and users from gaining access to your LAN. For 802.1X and MAC RADIUS authentication, end devices must be authenticated before they receive an IP address from a DHCP server. For captive portal authentication, the switch allows the end devices to get an IP address and allows forwarding of DHCP, DNS, and ARP packets.

You can allow end devices to access the network without authentication by including the MAC address of the end device in the static MAC bypass list or, for captive portal, by including the MAC address of the end device in the authentication whitelist.

You can configure 802.1X, MAC RADIUS, and captive portal on the same interface and in any combination, except that you cannot configure MAC RADIUS and captive portal on an interface without also configuring 802.1X. If you configure multiple authentication methods on a single interface, the switch falls back to another method if the first method is unsuccessful. For a description of the process flow when multiple authentication methods are configured on an interface, see “Authentication Process Flow for EX Series Switches” on page 1672.

This topic covers:

- Sample Basic Authentication Topology on page 1658
- 802.1X Authentication on page 1659
- MAC RADIUS Authentication on page 1661
- Captive Portal Authentication on page 1661
- Static MAC Bypass of Authentication on page 1662
- Fallback of Authentication Methods on page 1662

Sample Basic Authentication Topology

Figure 6 on page 1659 illustrates a basic deployment topology for authentication on an EX Series switch:
802.1X Authentication

802.1X is an IEEE standard for port-based network access control (PNAC). It provides an authentication mechanism to allow devices to access a LAN. The 802.1X authentication feature on an EX Series switch is based upon the IEEE 802.1D standard Port-Based Network Access Control.

The communication protocol between the end device and the switch is Extensible Authentication Protocol Over LAN (EAPoL). EAPoL is a version of EAP designed to work with Ethernet networks. The communication protocol between the authentication server and the switch is RADIUS.
During the authentication process, the switch completes multiple message exchanges between the end device and the authentication server. While 802.1X authentication is in process, only 802.1X traffic is allowed. Other traffic, such as DHCP and HTTP, is blocked at the data link layer.

**NOTE:** You can configure both the maximum number of times an EAPoL request packet is retransmitted and the timeout period between attempts. For information, see “Configuring 802.1X Interface Settings (CLI Procedure)” on page 1740.

An 802.1X authentication configuration for a LAN contains three basic components:

- **Supplicant** (also called end device)—Supplicant is the IEEE term for an end device that requests to join the network. The end device can be responsive or nonresponsive. A responsive end device is 802.1X-enabled and provides authentication credentials—specifically, a username and password for EAP MD5 or a username and client certificates for EAP-TLS, EAP-TTLS, and EAP-PEAP.

You can configure a server-reject VLAN to provide limited LAN access for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. A server-reject VLAN can provide a remedial connection, typically just to the Internet, for these devices. See “Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients” on page 1735 for additional information.

**NOTE:** If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.

A nonresponsive end device is not 802.1X-enabled, but it can be authenticated through MAC RADIUS authentication.

- **Authenticator port access entity**—The IEEE term for the authenticator. The EX Series switch is the authenticator, and it controls access by blocking all traffic to and from end devices until they are authenticated.

- **Authentication server**—The authentication server contains the backend database that makes authentication decisions. It contains credential information for each end device that is allowed to connect to the network. The authenticator forwards credentials supplied by the end device to the authentication server. If the credentials forwarded by the authenticator match the credentials in the authentication server database, access is granted. If the credentials forwarded do not match, access is denied. The EX Series switches support RADIUS authentication servers.

**NOTE:** You cannot configure 802.1X authentication on redundant trunk groups (RTGs). For more information on RTGs, see “Understanding Redundant Trunk Links on EX Series Switches” on page 2068.
MAC RADIUS Authentication

You can configure MAC RADIUS authentication on interfaces that are connected to end devices that are not 802.1X-enabled but that you want to allow to access the LAN.

The EAP method supported for MAC RADIUS authentication on EX Series switches is EAP-MD5.

If both 802.1X-enabled end devices and end devices that are not 802.1X-enabled connect to an interface, you can configure both 802.1X and MAC RADIUS authentication methods on the interface. In this case, the switch first attempts to authenticate using 802.1X, and if that method fails, it attempts to authenticate the end device using MAC RADIUS authentication.

If you know that only non-802.1X-enabled end devices connect on that interface, you can eliminate the delay that occurs while the switch determines that the end device is non-802.1X-enabled by configuring the `mac-radius restrict` option. When this option is configured, the switch does not attempt to authenticate the end device through 802.1X but instead immediately sends a request to the RADIUS server for authentication of the MAC address of the end device. If the MAC address of an end device is configured as permitted on the RADIUS server, the switch opens LAN access to the end device on the interface to which it is connected.

This option is useful when no other 802.1X authentication methods, such as guest VLAN, are needed on the interface. When you configure `mac-radius restrict` on an interface to eliminate this delay, the switch drops all 802.1X packets.

Captive Portal Authentication

Captive portal authentication (hereafter referred to as captive portal) allows you to authenticate users on EX Series switches by redirecting Web browser requests to a login page that requires users to input a username and password before they are allowed access to the network. Captive portal controls network access by requiring users to provide information that is authenticated against a RADIUS server database using EAP-MD5. You can also use captive portal to display an acceptable-use policy to users before they access your network.

Juniper Networks Junos operating system (Junos OS) for EX Series switches provides a template that allows you to easily design and modify the look of the captive portal login page. You enable specific interfaces for captive portal. The first time an end device connected to a captive portal interface attempts to access a web page, the switch presents the captive portal login page. Upon successful authentication, the user is allowed access to the network and to continue to the original page requested.

**NOTE:** If Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) is enabled, Hypertext Transfer Protocol (HTTP) requests are redirected to an HTTPS connection for the captive portal authentication process. After authentication, the end device is returned to the HTTP connection.
If there are end devices that are not HTTP-enabled connected to the captive portal interface, you can allow them to bypass captive portal authentication by adding their MAC addresses to an authentication whitelist.

When the user is authenticated by the RADIUS server, any per-user policies (attributes) associated with that user are also sent to the switch.

Captive portal on EX Series switches has the following limitations:

- The captive portal interface must be configured for `family ethernet-switching` and set to port mode `access`.

- Captive portal does not support dynamic assignment of VLANs downloaded from the RADIUS server.

- If the user is idle for more than about 5 minutes and there is no traffic passed, the user must log back in to the captive portal.

**Static MAC Bypass of Authentication**

You can allow end devices to access the LAN without authentication on a RADIUS server by including their MAC addresses in the static MAC bypass list (also known as the exclusion list).

You might choose to include a device in the bypass list to:

- Allow non-802.1X-enabled devices access to the LAN.

- Eliminate the delay that occurs while the switch determines that a connected device is a non-802.1X-enabled host.

When you configure static MAC on the switch, the MAC address of the end device is first checked in a local database (a user-configured list of MAC addresses). If a match is found, the end device is successfully authenticated and the interface is opened up for it. No further authentication is done for that end device. If a match is not found and 802.1X authentication is enabled on the switch, the switch attempts to authenticate the end device through the RADIUS server.

For each MAC address, you can also configure the VLAN to which the end device is moved or the interfaces on which the host connects.

---

**CAUTION:** When you clear the learned MAC addresses from an interface using the `clear dot1x interface` command, all MAC addresses are cleared, including those in the static MAC bypass list.

---

**Fallback of Authentication Methods**

You can configure multiple authentication methods on a single interface to enable fallback to another method if one method fails.

If an interface is configured in multiple supplicant mode, all end devices connecting through the interface must use either captive portal or a combination of 802.1X and MAC...
RADIUS, captive portal cannot be mixed with 802.1X or MAC RADIUS. Therefore, if there is already an end device on the interface that was authenticated through 802.1X or MAC RADIUS authentication, then additional end devices authenticating do not fall back to captive portal. If only 802.1X authentication or MAC RADIUS authentication is configured, some end devices can be authenticated using 802.1X and others can still be authenticated using MAC RADIUS.

Fallback of authentication methods occurs in the following order:

1. **802.1X authentication**—If 802.1X is configured on the interface, the switch sends EAPoL requests to the end device and attempts to authenticate the end device through 802.1X authentication. If the end device does not respond to the EAP requests, the switch checks whether MAC RADIUS authentication is configured on the interface.

2. **MAC RADIUS authentication**—If MAC RADIUS authentication is configured on the interface, the switch sends the MAC RADIUS address of the end device to the authentication server. If MAC RADIUS authentication is not configured, the switch checks whether captive portal is configured on the interface.

3. **Captive portal authentication**—If captive portal is configured on the interface, the switch attempts to authenticate using this method after attempting any other configured authentication methods. If an end device is authenticated on the interface using captive portal, this becomes the active authentication method on the interface. When captive portal is the active authentication method, the switch falls back to 802.1X authentication if there are no sessions in the authenticated state and if the interface receives an EAP packet.

**Related Documentation**

- [802.1X for EX Series Switches Overview on page 1655](#)
- [Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684](#)
- [Configuring 802.1X Interface Settings (CLI Procedure) on page 1740](#)
- [Configuring MAC RADIUS Authentication (CLI Procedure) on page 1754](#)
- [Configuring Captive Portal Authentication (CLI Procedure)](#)
- [Configuring Static MAC Bypass of Authentication (CLI Procedure) on page 1755](#)
- [Controlling Authentication Session Timeouts (CLI Procedure) on page 1761](#)
- [Authentication Process Flow for EX Series Switches on page 1672](#)
Understanding Guest VLANs for 802.1X on EX Series Switches

Guest VLANs can be configured on switches that are using 802.1X authentication to provide limited access—typically only to the Internet—for:

- Corporate guests
- End devices that are not 802.1X-enabled
- Nonresponsive end devices when MAC RADIUS authentication has not been configured on the switch interfaces to which the hosts are connected

A guest VLAN is not used for supplicants sending incorrect credentials. Those supplicants are directed to the server-reject VLAN instead.

For end devices that are not 802.1X-enabled, a guest VLAN can allow limited access to a server from which the non-802.1X-enabled end device can download the supplicant software and attempt authentication again.

A guest VLAN is not used when MAC RADIUS authentication has been configured on the switch interfaces to which the hosts are connected. Some end devices, such as a printer, cannot be enabled for 802.1X. The hosts for such devices should be connected to switch interfaces that are configured for MAC RADIUS authentication. See "Configuring MAC RADIUS Authentication (CLI Procedure)" on page 1754.

Understanding 802.1X and RADIUS Accounting on EX Series Switches

Juniper Networks EX Series Ethernet Switches support IETF RFC 2866, RADIUS Accounting. Configuring RADIUS accounting on an EX Series switch permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the switch, and select the type of accounting data to be collected.

The RADIUS accounting server you specify can be the same server used for RADIUS authentication, or it can be a separate RADIUS server. You can specify a list of RADIUS accounting servers. In the event that the primary server (the first one configured) is unavailable, each RADIUS server in the list is tried in the order in which they are configured in the Juniper Networks Junos operating system (Junos OS).

The RADIUS accounting process between a switch and a RADIUS server works like this:
1. A RADIUS accounting server listens for User Datagram Protocol (UDP) packets on a specific port. For example, on FreeRADIUS, the default port is 1813.

2. The switch forwards an accounting-request packet containing an event record to the accounting server. For example, a supplicant is authenticated through 802.1X authentication and connected to the LAN. The event record associated with this supplicant contains an Acct-Status-Type attribute whose value indicates the beginning of user service for this supplicant. When the supplicant’s session ends, the accounting request will contain an Acct-Status-Type attribute value indicating the end of user service. The RADIUS accounting server records this as a stop-accounting record containing session information and the length of the session.

3. The RADIUS accounting server logs these events as start-accounting or stop-accounting records. The records are in a file. On FreeRADIUS, the file name is the server's address; for example, 122.69.1.250.

4. The accounting server sends an accounting-response packet back to the switch confirming it has received the accounting request.

5. If the switch does not receive a response from the server, it continues to send accounting requests until an accounting response is returned from the accounting server.

The statistics collected through this process can be displayed from the RADIUS server; to see those statistics, the user accesses the log file configured to receive them.

**Related Documentation**

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 1675
- 802.1X for EX Series Switches Overview on page 1655
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741

**Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches**

Juniper Networks EX Series Ethernet Switches use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device information on network links. The information allows the switch to quickly identify a variety of devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighbor devices. Device information can include information such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Juniper Networks Junos operating system (Junos OS).

LLDP-MED goes one step further than LLDP, exchanging IP-telephony messages between the switch and the IP telephone.
**NOTE:** If your IP telephone is configured for voice over IP (VoIP), the switch automatically detects the configuration and assigns the telephone to the voice VLAN. The implementation of a voice VLAN on an IP telephone is vendor-specific. Consult the documentation that came with your IP telephone for instructions on configuring a voice VLAN. For example, on an Avaya phone, you can ensure that the phone gets the correct VoIP VLAN ID even in the absence of LLDP-MED by enabling DHCP option 176.

LLDP and LLDP-MED also provide PoE power management capabilities. LLDP power negotiation allows the switch to manage PoE power by negotiating with LLDP-enabled powered devices to dynamically allocate PoE power as needed. LLDP power priority allows an LLDP-enabled powered device to set the PoE power priority on the switch interface to which it connects.

The switch also uses these protocols to ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p CoS and 802.1Q tag information can be sent to the IP telephone.

EX Series switches support the following basic TLVs:

- **Chassis Identifier**—The MAC address associated with the local system.
- **Port Identifier**—The port identification for the specified port in the local system.
- **Port Description**—Interface name for the port.
- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.
- **System Description**—The system description containing information about the software and current image running on the system. This information is not configurable, but taken from the software.
- **System Capabilities**—The primary function performed by the system. The capabilities that system supports; for example, bridge or router. This information is not configurable, but based on the model of the product.
- **Management Address**—The IPv4 or IPv6 management address of the local system.

**NOTE:** The Chassis ID TLV has a subtype for Network Address Family. LLDP frames are validated only if this subtype has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the "show lldp neighbors" command, but is not assigned to the VLAN.

EX Series switches support the following 802.3 TLVs:
• **Power via MDI**—A TLV that advertises MDI power support, PSE power pair, and power class information.

• **MAC/PHY Configuration Status**—A TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is not configurable, but based on the physical interface structure.

• **Link Aggregation**—A TLV that advertises if the port is aggregated and its aggregated port ID.

• **Maximum Frame Size**—A TLV that advertises the Maximum Transmission Unit (MTU) of the interface sending LLDP frames.

• **Port VLAN**—A TLV that advertises the VLAN name configured on the interface.

EX Series switches support the following LLDP-MED TLVs:

• **LLDP MED Capabilities**—A TLV that advertises the primary function of the port. The capabilities values range 0 through 15:
  - 0—Capabilities
  - 1—Network Policy
  - 2—Location Identification
  - 3—Extended Power via MDI-PSE
  - 4—Inventory
  - 5–15—Reserved

• **LLDP-MED Device Class Values**:
  - 0—Class not defined.
  - 1—Class 1 Device.
  - 2—Class 2 Device.
  - 3—Class 3 Device.
  - 4—Network Connectivity Device
  - 5–255—Reserved.

• **Network Policy**—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and Diffserv code points.

• **Endpoint Location**—A TLV that advertises the physical location of the endpoint.

• **Extended Power via MDI**—A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

**Related Documentation**

- [Understanding Layer 2 Protocol Tunneling on EX Series Switches](#)
When you use Voice over IP (VoIP), you can connect IP telephones to the switch and configure IEEE 802.1X authentication for 802.1X-compatible IP telephones. The 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access.

VoIP is a protocol used for the transmission of voice through packet-switched networks. VoIP transmits voice calls using a network connection instead of an analog phone line.

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters to the phone.

You can configure 802.1X authentication to work with VoIP in multiple supplicant or single supplicant mode. In *multiple-suppliant* mode, the 802.1X process allows multiple supplicants to connect to the interface. Each supplicant will be authenticated individually. For an example of a VoIP multiple supplicant topology, see Figure 7 on page 1668.
If an 802.1X-compatible IP telephone does not have an 802.1X host but has another 802.1X-compatible device connected to its data port, you can connect the phone to an interface in single-supplicant mode. In single-supplicant mode, the 802.1X process authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication. For an example of a VoIP single supplicant topology, see Figure 8 on page 1669.

**Figure 8: VoIP Single Supplicant Topology**

![Figure 8: VoIP Single Supplicant Topology](image)

If an IP telephone does not support 802.1X, you can configure VoIP to bypass 802.1X and LLDP-MED and have the packets forwarded to a VoIP VLAN.

**Related Documentation**
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support
Understanding 802.1X and VSAs on EX Series Switches

Juniper Networks EX Series Ethernet Switches support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs) and are described in RFC 2138, Remote Authentication Dial In User Service (RADIUS). Through VSAs, you can configure port-filtering attributes on the RADIUS server. VSAs are clear text fields sent from the RADIUS server to the switch as a result of the 802.1X authentication success or failure. The 802.1X authentication prevents unauthorized user access by blocking a supplicant at the port until the supplicant is authenticated by the RADIUS server. The VSA attributes are interpreted by the switch during authentication, and the switch takes appropriate actions. Implementing port-filtering attributes with 802.1X authentication on the RADIUS server provides a central location for controlling LAN access for supplicants.

These port-filtering attributes specific to Juniper Networks are encapsulated in a RADIUS server VSA with the vendor ID set to the Juniper Networks ID number, 2636.

As well as configuring port-filtering attributes through VSAs, you can apply a port firewall filter that has already been configured on the switch directly to the RADIUS server. Like port-filtering attributes, the filter is applied during the 802.1X authentication process, and its actions are applied at the switch port. Adding a port firewall filter to a RADIUS server eliminates the need to add the filter to multiple ports and switches. For more information, see “Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch” on page 1719.

VSAs are only supported for 802.1X single-suppliant configurations and multiple-suppliant configurations.

Related Documentation
- Understanding Authentication on EX Series Switches on page 1658
- Example: Setting Up 802.1X for Single Suppliant or Multiple Suppliant Configurations on an EX Series Switch on page 1684
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742
- Configuring Firewall Filters (CLI Procedure) on page 4192
- VSA Match Conditions and Actions on page 1749

Understanding Dynamic VLANs for 802.1X on EX Series Switches

Dynamic VLANs, in conjunction with the 802.1X authentication process, provide secure access to the LAN for end devices belonging to different VLANs on a single port.

When this feature is configured on the RADIUS server, an end device or user authenticating on the RADIUS server is assigned to the VLAN configured for it. The end device or user becomes a member of a VLAN dynamically after successful 802.1X authentication. For information on configuring dynamic VLANs on your RADIUS server, see the documentation for your RADIUS server.

Successful authentication requires that the VLAN ID or VLAN name exist on the switch and match the VLAN ID or VLAN name sent by the RADIUS server during authentication.
If neither exists, the end device is unauthenticated. If a guest VLAN is established, the unauthenticated end device is automatically moved to the guest VLAN.

Related Documentation
- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 1713
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 1679
- Understanding Guest VLANs for 802.1X on EX Series Switches on page 1664

Understanding Server Fail Fallback and Authentication on EX Series Switches

Server fail fallback allows you to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

Juniper Networks EX Series Ethernet Switches use authentication to implement access control in an enterprise network. If 802.1X, MAC RADIUS, or captive portal authentication are configured on the interface, end devices are evaluated at the initial connection by an authentication (RADIUS) server. If the end device is configured on the authentication server, the device is granted access to the LAN and the EX Series switch opens the interface to permit access.

A RADIUS server timeout occurs if no RADIUS authentication servers are reachable when an end device logs in and attempts to access the LAN. Server fail fallback allows you to specify one of four actions to be taken toward end devices awaiting authentication when the server is timed out:

- **Permit** authentication, allowing traffic to flow from the end device through the interface as if the end device were successfully authenticated by the RADIUS server.
- **Deny** authentication, preventing traffic from flowing from the end device through the interface. This is the default.
- **Move** the end device to a specified VLAN. (The VLAN must already exist on the switch.)
- **Sustain** authenticated end devices that already have LAN access and **deny** unauthenticated end devices. If the RADIUS servers time out during reauthentication, previously authenticated end devices are reauthenticated and new users are denied LAN access.

Server fail fallback is triggered most often during reauthentication when the already configured and in-use RADIUS server becomes inaccessible. However, server fail fallback can also be triggered by an end device’s first attempt at authentication through the RADIUS server.

Server fail fallback allows you to specify that an end device be moved to a specified VLAN if the switch receives a RADIUS access-reject message. The configured VLAN name overrides any attributes sent by the server.

Related Documentation
- 802.1X for EX Series Switches Overview on page 1655
- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch on page 1707
You can control access to your network through an EX Series switch by using several different authentication methods—including 802.1X, MAC RADIUS, or captive portal.

Figure 9 on page 1672 illustrates the authentication process:

Figure 9: Authentication Process Flow for an EX Series Switch
Understanding Authentication Session Timeout

You can specify authentication session timeout values for captive portal authentication sessions and 802.1X and MAC RADIUS authentication sessions.

For captive portal authentication, the length of the session depends on the value configured for the `session-expiry` statement. The remainder of this topic pertains only to 802.1X and MAC RADIUS authentication sessions.

For 802.1X and MAC RADIUS authentication sessions, the timeout of the session depends on the value of `reauthentication-interval` for `dot1x authentication`. The authentication session might also end when the MAC table aging time expires because, unless you configure it not to, the session is removed from the authentication session table when the MAC address is removed from the Ethernet switching table.

Information about each 802.1X and MAC RADIUS authentication session—including the associated interfaces and VLANs for each MAC address that is authenticated by 802.1X authentication or MAC RADIUS authentication—is stored in the authentication session table. The authentication session table is tied to the Ethernet switching table (also called the MAC table). Each time the switch detects traffic from a MAC address, it updates the timestamp for that network node in the Ethernet switching table. A timer on the switch periodically checks the timestamp and if its value exceeds the user-configured `mac-table-aging-time` value, the switch removes the MAC address from the Ethernet switching table. When a MAC address ages out of the Ethernet switching table, the entry for that MAC address is also removed from the authentication database, with the result that the session ends.

You can control variables affecting timeout of authentication sessions in the following ways:

- Set the authentication session timeout on all interfaces or on selected interfaces using the `reauthentication` statement.

- Disassociate the authentication session table from the Ethernet switching table using the `no-mac-table-binding` statement. This setting prevents the termination of the authentication session when the associated MAC address ages out of the Ethernet switching table.
- Controlling Authentication Session Timeouts (CLI Procedure) on page 1761
- Configuring MAC Table Aging (CLI Procedure)
CHAPTER 29

Configuration

- Configuration Examples on page 1675
- Configuration Tasks on page 1739
- Configuration Statements on page 1762

**Configuration Examples**

- **Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch** on page 1675
- **Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch** on page 1679
- **Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch** on page 1684
- **Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch** on page 1690
- **Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication** on page 1698
- **Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch** on page 1704
- **Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch** on page 1707
- **Example: Configuring MAC RADIUS Authentication on an EX Series Switch** on page 1713
- **Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch** on page 1719
- **Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication** on page 1725
- **Example: Setting Up Captive Portal Authentication on an EX Series Switch** on page 1730
- **Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients** on page 1735

**Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch**

802.1X is the IEEE standard for Port-Based Network Access Control (PNAC). You use 802.1X to control network access. Only users and devices providing credentials that have been verified against a user database are allowed access to the network. You can use a
RADIUS server as the user database for 802.1X authentication, as well as for MAC RADIUS authentication.

This example describes how to connect a RADIUS server to an EX Series switch, and configure it for 802.1X:

- Requirements on page 1676
- Overview and Topology on page 1676
- Configuration on page 1678
- Verification on page 1679

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

  **NOTE:** For more about ELS, see: “Getting Started with Enhanced Layer 2 Software” on page 3

- Configured users on the RADIUS authentication server.

**Overview and Topology**

The EX Series switch acts as an authenticator Port Access Entity (PAE). It blocks all traffic and acts as a control gate until the supplicant (client) is authenticated by the server. All other users and devices are denied access.

Figure 10 on page 1677 shows one EX4200 switch that is connected to the devices listed in Table 198 on page 1677.
## Table 198: Components of the Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/7) and 16 non-PoE ports (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database with an address of 10.0.0.100 connected to the switch at port ge-0/0/10</td>
</tr>
</tbody>
</table>
In this example, connect the RADIUS server to access port ge-0/0/10 on the EX4200 switch. The switch acts as the authenticator and forwards credentials from the supplicant to the user database on the RADIUS server. You must configure connectivity between the EX4200 and the RADIUS server by specifying the address of the server and configuring the secret password. This information is configured in an access profile on the switch.

**NOTE:** For more information about authentication, authorization, and accounting (AAA) services, see the *Junos OS System Basics Configuration Guide*.

### Configuration

**CLI Quick Configuration**

To quickly connect the RADIUS server to the switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set access radius-server 10.0.0.100 secret juniper
set access radius-server 10.0.0.200 secret juniper
set access profile profile1 authentication-order radius
set access profile profile1 radius authentication-server [10.0.0.100 10.2.14.200]
```

**Step-by-Step Procedure**

To connect the RADIUS server to the switch:

1. Define the address of the servers, and configure the secret password. The secret password on the switch must match the secret password on the server:
   ```
   [edit]
   user@switch# set access radius-server 10.0.0.100 secret juniper
   user@switch# set access radius-server 10.0.0.200 secret juniper
   ```

2. Configure the authentication order, making radius the first method of authentication:
   ```
   [edit]
   user@switch# set access profile profile1 authentication-order radius
   ```

3. Configure a list of server IP addresses to be tried in order to authenticate the supplicant:
   ```
   [edit]
   user@switch# set access profile profile1 radius authentication-server [10.0.0.100 10.2.14.200]
   ```

**Results**

Display the results of the configuration:

```
user@switch> show configuration access
radius-server {  
  10.0.0.100  
  port 1812;  
  secret "$9$qPT3ApBsv69rvWLVb.P5"; ## SECRET-DATA
  }
}
profile profile1{
  authentication-order radius;
  radius {
    authentication-server 10.0.0.100 10.2.14.200;
  }
}
```
Verification

To confirm that the configuration is working properly, perform these tasks:

- Verify That the Switch and RADIUS Server are Properly Connected on page 1679

**Verify That the Switch and RADIUS Server are Properly Connected**

**Purpose**
Verify that the RADIUS server is connected to the switch on the specified port.

**Action**
Ping the RADIUS server to verify the connection between the switch and the server:

```
user@switch> ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.93.15.218: icmp_seq=0 ttl=64 time=9.734 ms
64 bytes from 10.93.15.218: icmp_seq=1 ttl=64 time=0.228 ms
```

**Meaning**
ICMP echo request packets are sent from the switch to the target server at 10.0.0.100 to test whether it is reachable across the IP network. ICMP echo responses are being returned from the server, verifying that the switch and the server are connected.

**Related Documentation**
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 1679
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742

**Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch**

802.1X on EX Series switches provides LAN access to users who do not have credentials in the RADIUS database. These users, referred to as guests, are authenticated and typically provided with access to the Internet.

This example describes how to create a guest VLAN and configure 802.1X authentication for it.

- Requirements on page 1680
- Overview and Topology on page 1680
- Configuration of a Guest VLAN That Includes 802.1X Authentication on page 1682
- Verification on page 1682
Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator interface access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure guest VLAN authentication, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure).
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

NOTE: For more about ELS, see: “Getting Started with Enhanced Layer 2 Software” on page 3

Overview and Topology

As part of IEEE 802.1X Port-Based Network Access Control (PNAC), you can provide limited network access to supplicants who do not belong to a VLAN authentication group by configuring authentication to a guest VLAN. Typically, guest VLAN access is used to provide Internet access to visitors to a corporate site. However, you can also use the guest VLAN feature to provide supplicants that fail 802.1X authentication to a corporate LAN with access to a VLAN with limited resources.

Figure 11 on page 1681 shows the conference room connected to the switch at interface ge-0/0/1.
Table 199: Components of the Guest VLAN Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 switch, 24 Gigabit Ethernet interfaces: 8 PoE interfaces (ge-0/0/0 through ge-0/0/7) and 16 non-PoE interfaces (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN names and tag IDs</td>
<td>sales, tag 100&lt;br&gt;support, tag 200&lt;br&gt;guest-vlan, tag 300</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database connected to the switch through interface ge-0/0/10</td>
</tr>
</tbody>
</table>
In this example, access interface ge-0/0/1 provides LAN connectivity in the conference room. Configure this access interface to provide LAN connectivity to visitors in the conference room who are not authenticated by the corporate VLAN.

### Configuration of a Guest VLAN That Includes 802.1X Authentication

#### CLI Quick Configuration

To quickly configure a guest VLAN, with 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans guest-vlan vlan-id 300
set protocols dot1x authenticator interface all guest-vlan guest-vlan
```

#### Step-by-Step Procedure

To configure a guest VLAN that includes 802.1X authentication on an EX Series switch:

1. Configure the VLAN ID for the guest VLAN:
   ```
   [edit]
   user@switch# set vlans guest-vlan vlan-id 300
   ```

2. Configure the guest VLAN under dot1x protocols:
   ```
   [edit]
   user@switch# set protocols dot1x authenticator interface all guest-vlan guest-vlan
   ```

#### Results

Check the results of the configuration:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        all {
          guest-vlan {
            guest-vlan;
          }
        }
      }
    }
  }
}
vlans {
  guest-vlan {
    vlan-id 300;
  }
}
```

#### Verification

To confirm that the configuration is working properly, perform these tasks:

- **Verifying That the Guest VLAN is Configured on page 1682**

**Verifying That the Guest VLAN is Configured**

Verify that the guest VLAN is created and that an interface has failed authentication and been moved to the guest VLAN.
NOTE: On switches running Junos OS for EX Series with support for the Enhanced Layer 2 Software (ELS), the output for the `show vlans` command will contain additional information. If your switch runs software that supports ELS, see `show vlans`. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

### Action
Use the operational mode commands:

```bash
user@switch> show vlans
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Tag</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td>ge-0/0/3.0*</td>
</tr>
<tr>
<td>dynamic</td>
<td>40</td>
<td>None</td>
</tr>
<tr>
<td>guest</td>
<td>30</td>
<td>None</td>
</tr>
<tr>
<td>guest-vlan</td>
<td>300</td>
<td>ge-0/0/1.0*</td>
</tr>
<tr>
<td>vlan_dyn</td>
<td></td>
<td>None</td>
</tr>
</tbody>
</table>

```bash
user@switch> show dot1x interface ge-0/0/1.0 detail
```

- Role: Authenticator
- Administrative state: Auto
- Supplicant mode: Single
- Number of retries: 3
- Quiet period: 60 seconds
- Transmit period: 30 seconds
- Mac Radius: Enabled
- Mac Radius Restrict: Disabled
- Reauthentication: Enabled
- Configured Reauthentication interval: 3600 seconds
- Supplicant timeout: 30 seconds
- Server timeout: 30 seconds
- Maximum EAPOL requests: 2
- Guest VLAN member: guest-vlan
- Number of connected supplicants: 1
  - Supplicant: user1, 00:00:00:00:13:23
  - Operational state: Authenticated
  - Authentication method: Radius
  - Authenticated VLAN: vol1
  - Dynamic Filter: match source-dot1q-tag 10 action deny
  - Session Reauth interval: 60 seconds
  - Reauthentication due in 50 seconds

### Meaning
The output from the `show vlans` command shows `guest-vlan` as the the name of the VLAN and the VLAN ID as 300.

The output from the `show dot1x interface ge-0/0/1.0 detail` command displays the **Guest VLAN membership** field, indicating that a supplicant at this interface failed 802.1X authentication and was passed through to the `guest-vlan`. 
802.1x Port-Based Network Access Control (PNAC) authentication on EX Series switches provides three types of authentication to meet the access needs of your enterprise LAN:

- Authenticate the first end device (supplicant) on an authenticator port, and allow all others also connecting to have access.
- Authenticate only one end device on an authenticator port at one time.
- Authenticate multiple end devices on an authenticator port. Multiple supplicant mode is used in VoIP configurations.

This example configures an EX4200 switch to use IEEE 802.1X to authenticate end devices that use three different administrative modes:

- Requirements on page 1684
- Overview and Topology on page 1685
- Configuration of 802.1X to Support Multiple Supplicant Modes on page 1687
- Verification on page 1688

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from end devices until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for end devices (supplicants) that have permission to connect to the network.

Before you configure the ports for 802.1X authentication, be sure you have:

- Installed your EX Series switch.
- Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure).
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a
switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see "Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch" on page 2073. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

**NOTE:** For more about ELS, see: "Getting Started with Enhanced Layer 2 Software" on page 3

- Configured users on the authentication server.

**Overview and Topology**

As shown in Figure 12 on page 1686, the topology contains an EX4200 access switch connected to the authentication server on port ge-0/0/10. Interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/11 will be configured for three different administrative modes.
To configure the administrative modes to support supplicants in different areas of the Enterprise network:
- Configure access port `ge-0/0/8` for single supplicant mode authentication.
- Configure access port `ge-0/0/9` for single secure supplicant mode authentication.
- Configure access port `ge-0/0/11` for multiple supplicant mode authentication.

Single supplicant mode authenticates only the first end device that connects to an authenticator port. All other end devices connecting to the authenticator port after the first has connected successfully, whether they are 802.1X-enabled or not, are permitted free access to the port without further authentication. If the first authenticated end device logs out, all other end devices are locked out until an end device authenticates.

Single-secure supplicant mode authenticates only one end device to connect to an authenticator port. No other end device can connect to the authenticator port until the first logs out.

Multiple supplicant mode authenticates multiple end devices individually on one authenticator port. If you configure a maximum number of devices that can be connected to a port through port security, the lesser of the configured values is used to determine the maximum number of end devices allowed per port.

**Configuration of 802.1X to Support Multiple Supplicant Modes**

**CLI Quick Configuration**

To quickly configure the ports with different 802.1X authentication modes, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/8 supplicant single
set protocols dot1x authenticator interface ge-0/0/9 supplicant single-secure
set protocols dot1x authenticator interface ge-0/0/11 supplicant multiple
```

**Step-by-Step Procedure**

Configure the administrative mode on the interfaces:

1. Configure the supplicant mode as single on interface `ge-0/0/8`:
   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/8 supplicant single
   ```
2. Configure the supplicant mode as single secure on interface `ge-0/0/9`:
   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/9 supplicant single-secure
   ```
3. Configure multiple supplicant mode on interface `ge-0/0/11`:
   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface ge-0/0/11 supplicant multiple
   ```

**Results**

Check the results of the configuration:

```
[edit]
user@access-switch> show configuration protocols {
  dot1x {
    authenticator {
      interface {
        ge-0/0/8.0 {
          supplicant single;
```
ge-0/0/9.0 {
    supplicant single-secure;
}
ge-0/0/11.0 {
    supplicant multiple;
}

Verification
To confirm that the configuration is working properly, perform these tasks:

- Verifying the 802.1X Configuration on page 1688

Verifying the 802.1X Configuration

Purpose Verify the 802.1X configuration on interfaces ge-0/0/8, ge-0/0/9, and ge-0/0/5.
**Action** Verify the 802.1X configuration with the operational mode command `show dot1x interface`:

```plaintext
user@switch> show dot1x interface ge-0/0/8.0 detail
ge-0/0/8.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>

user@switch> show dot1x interface ge-0/0/9.0 detail
ge-0/0/9.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single-Secure
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0

user@switch> show dot1x interface ge-0/0/11.0 detail
ge-0/0/11.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 0
```

**Meaning** The **Supplicant mode** output field displays the configured administrative mode for each interface. Interface `ge-0/0/8.0` displays **Single** supplicant mode. Interface `ge-0/0/9.0` displays **Single Secure** supplicant mode. Interface `ge-0/0/11.0` displays **Multiple** supplicant mode.
Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones. The Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) protocol forwards VoIP parameters from the switch to the phone. You also configure 802.1X authentication to allow the telephone access to the LAN. Authentication is done through a backend RADIUS server.

This example describes how to configure VoIP on an EX Series switch to support an Avaya IP phone, as well as the LLDP-MED protocol and 802.1X authentication:

- Requirements on page 1690
- Overview and Topology on page 1691
- Configuration on page 1693
- Verification on page 1695

Requirements

This example uses the following hardware and software components:

- Junos OS Release 13.2X50 or later for EX Series switches
- One EX4300 switch acting as an authenticator port access entity (PAE). The interfaces on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- An Avaya IP telephone that supports LLDP-MED and 802.1X

Before you configure VoIP, be sure you have:
• Installed your EX Series switch. See the installation information for your switch.

• Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure).

• Performed basic bridging and VLAN configuration on the switch. See “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073.

• Configured the RADIUS server for 802.1X authentication and set up the access profile. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.

• (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see “Configuring PoE (CLI Procedure)” on page 3942.

NOTE: If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the voip statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN’s ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview and Topology

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX4300 switch is connected to an Avaya IP telephone. Avaya phones have a built-in bridge that allows you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one interface on the switch. The EX Series switch is connected to a RADIUS server on the ge-0/0/10 interface (see Figure 13 on page 1692).
In this example, you configure VoIP parameters and specify the forwarding class **assured-forward** for voice traffic to provide the highest quality of service.

Table 201 on page 1692 describes the components used in this VoIP configuration example.

**Table 201: Components of the VoIP Configuration Topology**

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4300 switch</td>
</tr>
</tbody>
</table>
Table 201: Components of the VoIP Configuration Topology (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN names</td>
<td>data-vlan, voice-vlan</td>
</tr>
<tr>
<td>Connection to Avaya phone—with integrated hub, to connect phone</td>
<td>ge-0/0/2</td>
</tr>
<tr>
<td>and desktop PC to a single interface (requires PoE)</td>
<td></td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Provides backend database connected to the</td>
</tr>
<tr>
<td></td>
<td>switch through interface ge-0/0/10.</td>
</tr>
</tbody>
</table>

As well as configuring a VoIP for interface ge-0/0/2, you configure:

- 802.1X authentication. Authentication is set to multiple supplicant mode to support more than one supplicant's access to the LAN through interface ge-0/0/2.
- LLDP-MED protocol information. The switch uses LLDP-MED to forward VoIP parameters to the phone. Using LLDP-MED ensures that voice traffic gets tagged and prioritized with the correct values at the source itself. For example, 802.1p class of service and 802.1Q tag information can be sent to the IP telephone.

NOTE: A PoE configuration is not necessary if an IP telephone is using a power adapter.

### Configuration

**CLI Quick Configuration**

To quickly configure VoIP, LLDP-MED, and 802.1X, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-med interface ge-0/0/2
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

**Step-by-Step Procedure**

To configure VoIP with LLDP-MED and 802.1X:

1. Configure the VLANs for voice and data:

   ```
   [edit vlans]
   user@switch# set data-vlan vlan-id 77
   user@switch# set voice-vlan vlan-id 99
   ```

2. Associate the VLAN data-vlan with the interface:

   ```
   [edit vlans]
   user@switch# set data-vlan switch-options interface ge-0/0/2.0
   ```

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the data-vlan VLAN:
4. Configure VoIP on the interface and specify the **assured-forwarding** forwarding class to provide the most dependable class of service:

```
[edit switch-options]
user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding
```

5. Configure LLDP-MED protocol support:

```
[edit protocols]
user@switch# set lldp-med interface ge-0/0/2
```

6. To authenticate an IP phone and a PC connected to the IP phone on the interface, configure 802.1X authentication support and specify *multiple* supplicant mode:

```
[edit protocols]
user@switch# set dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```

**Results**

Display the results of the configuration:

```
[edit]
user@switch# show configuration
interfaces { 
  ge-0/0/2 { 
    unit 0 { 
      family ethernet-switching { 
        interface-mode access; 
        vlan { 
          members data-vlan; 
        } 
      } 
    } 
  } 
}

protocols { 
  lldp-med { 
    interface ge-0/0/2; 
  } 
  dot1x { 
    authenticator { 
      interface { 
        ge-0/0/2.0 { 
          supplicant multiple; 
        } 
      } 
    } 
  } 
}

vlans { 
  data-vlan { 

VLAN Configuration

```
  vlan-id 77;
  switch-options {
    interface ge-0/0/2.0;
  }
  voice-vlan {
    vlan-id 99;
  }
  switch-options {
    voip {
      interface ge-0/0/2.0 {
        vlan voice-vlan;
        forwarding-class assured-forwarding;
      }
    }
  }
```

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying LLDP-MED Configuration on page 1695
- Verifying 802.1X Authentication for IP Phone and Desktop PC on page 1696
- Verifying the VLAN Association with the Interface on page 1697

**Verifying LLDP-MED Configuration**

**Purpose**
Verify that LLDP-MED is enabled on the interface.
**Action**

```
user@switch> show lldp detail
```

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP</td>
<td>: Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advertisement interval</td>
<td>: 30 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmit delay</td>
<td>: 2 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hold timer</td>
<td>: 120 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification interval</td>
<td>: 0 Second(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config Trap Interval</td>
<td>: 0 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection Hold timer</td>
<td>: 300 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LLDP MED</td>
<td>: Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MED fast start count</td>
<td>: 3 Packets</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Port ID TLV subtype** : locally-assigned

<table>
<thead>
<tr>
<th>Interface Neighbor count</th>
<th>Parent Interface</th>
<th>LLDP</th>
<th>LLDP-MED</th>
<th>Power Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Vlan-id</th>
<th>Vlan-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>-</td>
<td>77</td>
<td>vlan-77</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>-</td>
<td>99</td>
<td>vlan-99</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>-</td>
<td>1</td>
<td>vlan-1</td>
</tr>
</tbody>
</table>

Basic Management TLVs supported:
End Of LLDPDU, Chassis ID, Port ID, Time To Live, Port Description, System Name,
System Description, System Capabilities, Management Address

Organizationally Specific TLVs supported:
MAC/PHY configuration/status, Power via MDI, Link aggregation, Maximum Frame Size,
Port VLAN tag, Port VLAN name.

**Meaning**

The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the ge-0/0/2 interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.

**Verifying 802.1X Authentication for IP Phone and Desktop PC**

**Purpose**

Display the 802.1X configuration to confirm that the VoIP interface has access to the LAN.
**Action**

```
user@switch> show dot1x interface ge/0/0/2.0 detail
ge-0/0/2.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Disabled
  Mac Radius Restrict: Disabled
  Reauthentication: Enabled
  Configured Reauthentication interval: 3600 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 2
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
  Supplicant: user101, 00:04:0f:fd:ac:fe
    Operational state: Authenticated
    Authentication method: Radius
    Authenticated VLAN: vo11
    Dynamic Filter: match source-dot1q-tag 10 action deny
    Session Reauth interval: 60 seconds
    Reauthentication due in 50 seconds
```

**Meaning**
The field **Role** shows that the ge-0/0/2.0 interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

**Verifying the VLAN Association with the Interface**

**Purpose**
Display the interface's VLAN membership.

**Action**

```
user@switch> show ethernet-switching interface ge-0/0/2.0
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,  
  LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
gre-0/0/2.0                    65535                                 untagged
  voice-vlan 99
      65535    Discarding
  data-vlan  77
      65535    Discarding
```

**Meaning**
The field **VLAN members** shows that the ge-0/0/2.0 interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN.

**Related Documentation**
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 1675
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927
You can configure voice over IP (VoIP) on an EX Series switch to support IP telephones.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, you must either add the MAC address of the phone to the static MAC bypass list or enable MAC RADIUS authentication on the switch.

This example describes how to configure VoIP on an EX Series switch without 802.1X authentication by using static MAC bypass of authentication:

**Requirements**

This example uses the following hardware and software components:

- One EX4300 switch.
- Junos OS Release 13.2 or later for EX Series switches
- An Avaya IP telephone

Before you configure VoIP, be sure you have:

- Installed your EX Series switch. See the installation information for your switch.
- Performed the initial switch configuration. See *Connecting and Configuring an EX Series Switch (CLI Procedure)*.
- Performed basic bridging and VLAN configuration on the switch. See “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073.
• Configured the RADIUS server for 802.1X authentication and set up the access profile. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 1675.

• (Optional) Configured the interface ge-0/0/2 for Power over Ethernet (PoE). The PoE configuration is not necessary if the VoIP supplicant is using a power adapter. For information about configuring PoE, see "Configuring PoE (CLI Procedure)" on page 3942.

NOTE: If the IP address is not configured on the Avaya IP phone, the phone exchanges LLDP-MED information to get the VLAN ID for the voice VLAN. You must configure the voip statement on the interface to designate the interface as a VoIP interface and allow the switch to forward the VLAN name and VLAN ID for the voice VLAN to the IP telephone. The IP telephone then uses the voice VLAN (that is, it references the voice VLAN's ID) to send a DHCP discover request and exchange information with the DHCP server (voice gateway).

Overview

Instead of using a regular telephone, you connect an IP telephone directly to the switch. An IP phone has all the hardware and software needed to handle VoIP. You also can power an IP telephone by connecting it to one of the Power over Ethernet (PoE) interfaces on the switch.

In this example, the access interface ge-0/0/2 on the EX4300 switch is connected to a non-802.1X IP phone.

To configure VoIP on an EX Series switch to support an IP phone that does not support 802.1X authentication, add the MAC address of the phone as a static entry in the authenticator database and set the supplicant mode to multiple.

Configuration

To quickly configure VoIP without using 802.1X authentication, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set vlans data-vlan vlan-id 77
set vlans voice-vlan vlan-id 99
set vlans data-vlan switch-options interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family ethernet-switching interface-mode access
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan
set switch-options voip interface ge-0/0/2.0 vlan voice-vlan
set switch-options voip interface ge-0/0/2.0 forwarding-class assured-forwarding
set protocols lldp-medi interface ge-0/0/2
set protocols dot1x authenticator authentication-profile-name auth-profile
set protocols dot1x authenticator static 00:04:f2:11:aa:a7
set protocols dot1x authenticator interface ge-0/0/2.0 supplicant multiple
```
Step-by-Step Procedure

To configure VoIP without 802.1X authentication:

1. Configure the VLANs for voice and data:

   [edit vlans]
   user@switch# set data-vlan vlan-id 77
   user@switch# set voice-vlan vlan-id 99

2. Associate the VLAN data-vlan with the interface:

   [edit vlans]
   user@switch# set data-vlan switch-options interface ge-0/0/2.0

3. Configure the interface as an access interface, configure support for Ethernet switching, and add the data-vlan VLAN:

   [edit interfaces]
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching interface-mode access
   user@switch# set ge-0/0/2 unit 0 family ethernet-switching vlan members data-vlan

4. Configure VoIP on the interface and specify the assured-forwarding forwarding class to provide the most dependable class of service:

   [edit switch-options]
   user@switch# set voip interface ge-0/0/2.0 vlan voice-vlan
   user@switch# set voip interface ge-0/0/2.0 forwarding-class assured-forwarding

5. Configure LLDP-MED protocol support:

   [edit protocols]
   user@switch# set lldp-med interface ge-0/0/2

6. Set the authentication profile (see “Configuring 802.1X Interface Settings (CLI Procedure)” on page 1740 and “Configuring 802.1X RADIUS Accounting (CLI Procedure)” on page 1741):

   [edit protocols]
   set dot1x authenticator authentication-profile-name auth-profile

7. Add the MAC address of the phone to the static MAC bypass list:

   [edit protocols]
   set dot1x authenticator static 00:04:f2:11:aa:a7

8. Set the supplicant mode to multiple:

   [edit protocols]
   set dot1x authenticator interface ge-0/0/2.0 supplicant multiple

Results

Display the results of the configuration:

   [edit]
   user@switch# show configuration interfaces { 
   ge-0/0/2 { 
   unit 0 [ 
   family ethernet-switching [ 
   interface-mode access; 
   vlan { 
   members data-vlan; 
   } 
   ] 
   ] 
   } 
   } 
   } 
   } 
   protocols {
lldp-med {
    interface ge-0/0/2;
}
dot1x {
    authenticator {
        authentication-profile-name auth-profile;
        static {
            00:04:f2:11:aa:a7;
        }
    }
    interface {
        ge-0/0/2.0 {
            supplicant multiple;
        }
    }
}
vlans {
    data-vlan {
        vlan-id 77;
        switch-options {
            interface ge-0/0/2.0;
        }
    }
    voice-vlan {
        vlan-id 99;
    }
}
switch-options {
    voip {
        interface ge-0/0/2.0 {
            vlan voice-vlan;
            forwarding-class assured-forwarding;
        }
    }
}

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying LLDP-MED Configuration on page 1701
- Verifying Authentication for the Desktop PC on page 1702
- Verifying the VLAN Association with the Interface on page 1703

Verifying LLDP-MED Configuration

Purpose  Verify that LLDP-MED is enabled on the interface.
**Action**

```
user@switch>  show lldp detail
```

<table>
<thead>
<tr>
<th>LLDP</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisement interval</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Transmit delay</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Hold timer</td>
<td>120 seconds</td>
</tr>
<tr>
<td>Notification interval</td>
<td>0 Second(s)</td>
</tr>
<tr>
<td>Config Trap Interval</td>
<td>0 seconds</td>
</tr>
<tr>
<td>Connection Hold timer</td>
<td>300 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LLDP MED</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>MED fast start count</td>
<td>3 Packets</td>
</tr>
</tbody>
</table>

**Port ID TLV subtype**: locally-assigned

**Interface** | **Parent Interface** | **Vlan-id** | **Vlan-name**
---|---------------------|------------|------------
**ge-0/0/0** | -                   | 1          | vlan-1     |
**ge-0/0/1** | -                   | 1          | vlan-1     |
**ge-0/0/2** | -                   | 77         | vlan-77    |
**ge-0/0/3** | -                   | 99         | vlan-99    |
**ge-0/0/4** | -                   | 1          | vlan-1     |
**ge-0/0/5** | -                   | 1          | vlan-1     |
**ge-0/0/6** | -                   | 1          | vlan-1     |
**ge-0/0/7** | -                   | 1          | vlan-1     |
**ge-0/0/8** | -                   | 1          | vlan-1     |
**ge-0/0/9** | -                   | 1          | vlan-1     |
**ge-0/0/10**| -                   | 1          | vlan-1     |

**Meaning**

The `show lldp detail` output shows that both LLDP and LLDP-MED are configured on the `ge-0/0/2` interface. The end of the output shows the list of supported LLDP basic management TLVs and organizationally specific TLVs that are supported.

**Verifying Authentication for the Desktop PC**

**Purpose**

Display the 802.1X configuration for the desktop PC connected to the VoIP interface through the IP phone.
**Action**

```
user@switch> show dot1x interface ge/0/0/2.0 detail
```

- **Role:** Authenticator
- **Administrative state:** Auto
- **Supplicant mode:** Multiple
- **Number of retries:** 3
- **Quiet period:** 60 seconds
- **Transmit period:** 30 seconds
- **Mac Radius:** Disabled
- **Mac Radius Restrict:** Disabled
- **Reauthentication:** Enabled
- **Configured Reauthentication interval:** 3600 seconds
- **Supplicant timeout:** 30 seconds
- **Server timeout:** 30 seconds
- **Maximum EAPOL requests:** 2
- **Guest VLAN member:** <not configured>
- **Number of connected supplicants:** 1
  - **Supplicant:** user101, 00:04:0f:fd:ac:fe
  - **Operational state:** Authenticated
  - **Authentication method:** Radius
  - **Authenticated VLAN:** vo11
  - **Dynamic Filter:** match source-dot1q-tag 10 action deny
  - **Session Reauth interval:** 60 seconds
  - **Reauthentication due in 50 seconds**

**Meaning**
The field **Role** shows that the ge-0/0/2.0 interface is in the authenticator state. The **Supplicant** field shows that the interface is configured in multiple supplicant mode, permitting multiple supplicants to be authenticated on this interface. The MAC addresses of the supplicants currently connected are displayed at the bottom of the output.

**Verifying the VLAN Association with the Interface**

**Purpose**
Display the interface's VLAN membership.

**Action**

```
user@switch> show ethernet-switching interface ge-0/0/2.0
```

```
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down )

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Vlan members</th>
<th>TAG</th>
<th>MAC limit</th>
<th>STP state</th>
<th>Logical interface flags</th>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/2.0</td>
<td></td>
<td>65535</td>
<td></td>
<td></td>
<td>untagged</td>
<td></td>
</tr>
<tr>
<td>voice-vlan 99</td>
<td></td>
<td>65535</td>
<td>Discarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data-vlan 77</td>
<td></td>
<td>65535</td>
<td>Discarding</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Meaning**
The field **VLAN members** shows that the ge-0/0/2.0 interface supports both the **data-vlan** VLAN and **voice-vlan** VLAN.

**Related Documentation**
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 1690
- Understanding 802.1X and VoIP on EX Series Switches on page 1668
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665
**Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch**

To allow devices to access your LAN through 802.1X-configured interfaces without authentication, you can configure a static MAC bypass list on the EX Series switch. The static MAC bypass list, also known as the *exclusion list*, specifies MAC addresses that are allowed on the switch without a request to an authentication server.

You can use static MAC bypass of authentication to allow connection for devices that are not 802.1X-enabled, such as printers. If a host's MAC address is compared and matched against the static MAC address list, the nonresponsive host is authenticated and an interface opened for it.

This example describes how to configure static MAC bypass of authentication for two printers:

- **Requirements on page 1704**
- **Overview and Topology on page 1704**
- **Configuration on page 1706**
- **Verification on page 1707**

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.

Before you configure static MAC authentication, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see "Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch" on page 2073. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

  For more about ELS, see: "Getting Started with Enhanced Layer 2 Software" on page 3

- Specified the RADIUS server connections and configured an access profile on the switch. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 1675.

### Overview and Topology

To permit printers access to the LAN, add them to the static MAC bypass list. The MAC addresses on this list are permitted access without authentication from the RADIUS server.

*Figure 14 on page 1705* shows the two printers connected to the EX4200.
The interfaces shown in Table 202 on page 1705 will be configured for static MAC authentication.

Table 202: Components of the Static MAC Authentication Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200, 24 Gigabit Ethernet ports: 8 PoE ports (ge-0/0/0 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
</tbody>
</table>
| Connections to integrated printer/fax/copier machines (no PoE required) | ge-0/0/19, MAC address 00:04:0f:fd:ac:fe  
  ge-0/0/20, MAC address 00:04:ae:cd:23:5f |
The printer with the MAC address 00:04:0f:fd:ac:fe is connected to access interface ge-0/0/19. A second printer with the MAC address 00:04:ae:cd:23:5f is connected to access interface ge-0/0/20. Both printers will be added to the static list and bypass 802.1X authentication.

### Configuration

#### CLI Quick Configuration

To quickly configure static MAC authentication, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator authentication-profile-name profile1
set protocols dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
set protocols dot1x authenticator interface all supplicant multiple
```

#### Step-by-Step Procedure

Configure static MAC authentication:

1. Configure the authentication profile name (access profile name) to use for authentication:
   
   ```
   [edit protocols]
   user@switch# set dot1x authenticator authentication-profile-name profile1
   ```

2. Configure MAC addresses 00:04:0f:fd:ac:fe and 00:04:ae:cd:23:5f as static MAC addresses:
   
   ```
   [edit protocols]
   user@switch# set dot1x authenticator static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f]
   ```

3. Configure the 802.1X authentication method:
   
   ```
   [edit protocols]
   user@switch# set dot1x authenticator interface all supplicant multiple
   ```

#### Results

Display the results of the configuration:

```
user@switch> show
interfaces {
  ge-0/0/19 {
    unit 0 {
      family ethernet-switching {
        vlan members default;
      }
    }
  }
  ge-0/0/20 {
    unit 0 {
      family ethernet-switching {
        vlan members default;
      }
    }
  }
}
protocols {
  dot1x {
    authenticator {
      authentication-profile-name profile1
    static [00:04:0f:fd:ac:fe 00:04:ae:cd:23:5f];
    interface {
      all {
      ```
To confirm that the configuration is working properly, perform these tasks:

- Verifying Static MAC Bypass of Authentication on page 1707

**Verifying Static MAC Bypass of Authentication**

**Purpose**
Verify that the MAC address for both printers is configured and associated with the correct interfaces.

**Action**
Use the operational mode command:

```
user@switch> show dot1x static-mac-address
```

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN-Assignment</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:0f:fd:ac:fe</td>
<td>default</td>
<td>ge-0/0/19.0</td>
</tr>
<tr>
<td>00:04:ae:cd:23:5f</td>
<td>default</td>
<td>ge-0/0/20.0</td>
</tr>
</tbody>
</table>

**Meaning**
The output field *MAC address* shows the MAC addresses of the two printers.

The output field *Interface* shows that the MAC address 00:04:0f:fd:ac:fe can connect to the LAN through interface ge-0/0/19.0 and that the MAC address 00:04:ae:cd:23:5f can connect to the LAN through interface ge-0/0/20.0.

**Related Documentation**
- Configuring 802.1X Authentication (*J-Web Procedure*)
- Configuring Static MAC Bypass of Authentication (CLI Procedure) on page 1755
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Understanding Authentication on EX Series Switches on page 1658

**Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch**

Server failback allows you to specify how 802.1X supplicants connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

You use 802.1X to control network access. Only users and devices (supplicants) providing credentials that have been verified against a user database are allowed access to the network. You use a RADIUS server as the user database.
This example describes how to configure an interface to move a supplicant to a VLAN in the event of a RADIUS server timeout:

- Requirements on page 1708
- Overview and Topology on page 1708
- Configuration on page 1710
- Verification on page 1711

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

  NOTE: For more about ELS, see: “Getting Started with Enhanced Layer 2 Software” on page 3

- Set up a connection between the switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.

- Disable firewall filters on the interface. Firewall filters interfere with server fail fallback operation.

- Configured users on the authentication server.

Overview and Topology

A RADIUS server timeout occurs if no authentication RADIUS servers are reachable when a supplicant logs in and attempts to access the LAN. Using server fail fallback, configure alternative options for supplicants attempting LAN access. You can configure the switch to accept or deny access to supplicants or to maintain the access already granted towards supplicants before the RADIUS server timeout. Additionally, you can configure the switch to move supplicants to a specific VLAN if a RADIUS timeout occurs or if the RADIUS server sends an EAP Access-Reject message. Figure 15 on page 1709 shows the topology...
used for this example. The RADIUS server is connected to the EX4200 switch on access port ge-0/0/10. The switch acts as the authenticator Port Access Entity (PAE) and forwards credentials from the supplicant to the user database on the RADIUS server. The switch blocks all traffic and acts as a control gate until the supplicant is authenticated by the authentication server. A supplicant is connected to the switch through interface ge-0/0/1.

Figure 15: Topology for Configuration

Table 203 on page 1709 describes the components in this topology.

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 access switch, 24 Gigabit Ethernet ports: 8 PoE ports.</td>
</tr>
<tr>
<td>VLAN names</td>
<td>default VLAN</td>
</tr>
<tr>
<td></td>
<td>vlan-sf VLAN</td>
</tr>
<tr>
<td>Supplicant</td>
<td>Suppliant attempting access on interface ge-0/0/1</td>
</tr>
</tbody>
</table>
Table 203: Components of the Topology (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>One RADIUS server</td>
<td>Backend database with an address of 10.0.0.100 connected to the switch at port ge-0/0/10</td>
</tr>
</tbody>
</table>

In this example, configure interface ge-0/0/1 to move a supplicant attempting access to the LAN during a RADIUS timeout to another VLAN. A RADIUS timeout prevents the normal exchange of EAP messages that carry information from the RADIUS server to the switch and permit the authentication of a supplicant. The default VLAN is configured on interface ge-0/0/1. When a RADIUS timeout occurs, supplicants on the interface will be moved from the default VLAN to the VLAN named vlan-sf.

NOTE: For more information about authentication, authorization, and accounting (AAA) services, see Junos OS System Basics Configuration Guide.

Configuration

### CLI Quick Configuration

To quickly configure server fail fallback on the switch, copy the following commands and paste them into the switch terminal window:

```
[edit protocols dot1x authenticator]
set interface ge-0/0/1 server-fail vlan-name vlan-sf
```

### Step-by-Step Procedure

To configure an interface to divert supplicants to a specific VLAN when a RADIUS timeout occurs (here, the VLAN is vlan-sf):

1. Define the VLAN to which supplicants are diverted:

   ```
   [edit protocols dot1x authenticator]
   user@switch# set interface ge-0/0/1 server-fail vlan-name vlan-sf
   ```

### Results

Display the results of the configuration:

```
user@switch> show configuration
interfaces {
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members default;
        }
      }
    }
  }
}
protocols {
  dot1x {
    authenticator {
      authentication-profile-name profile52;
      interface {
        ge-0/0/1.0 {
          server-fail vlan-name vlan-sf;
        }
      }
    }
  }
```
Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout on page 1711

Verifying That the Supplicants Are Moved to an Alternative VLAN During a RADIUS Timeout

Purpose

Verify that the interface moves supplicants to an alternative VLAN during a RADIUS timeout.

NOTE: On switches running Junos OS for EX Series with support for the Enhanced Layer 2 Software (ELS), the output for the show vlans command will contain additional information. If your switch runs software that supports ELS, see show vlans. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.
**Action**  
Display the VLANs configured on the switch; the interface ge-0/0/1.0 is a member of the default VLAN:

```
user@switch> show vlans
Name      Tag     Interfaces
default   -       ge-0/0/0.0, ge-0/0/1.0*, ge-0/0/5.0*, ge-0/0/10.0,
           -       ge-0/0/12.0*, ge-0/0/14.0*, ge-0/0/15.0, ge-0/0/20.0
v2        77      None
vlansf    50      None
mgmt      -       me0.0*
```

Display 802.1X protocol information on the switch to view supplicants that are authenticated on interface ge-0/0/1.0:

```
user@switch> show dot1x interface brief
802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1.0    Authenticator  Authenticated   00:00:00:00:00:01    abc
ge-0/0/10.0   Authenticator  Initialize     -                   
ge-0/0/14.0   Authenticator  Connecting     -                   
ge-0/0/15.0   Authenticator  Initialize     -                   
ge-0/0/20.0   Authenticator  Initialize     -                   
```

A RADIUS server timeout occurs. Display the Ethernet switching table to show that the supplicant with the MAC address 00:00:00:00:00:01 previously accessing the LAN through the default VLAN is now being learned on the VLAN named vlan-sf:

```
user@switch> show ethernet-switching table
Ethernet-switching table: 3 entries, 1 learned
VLAN      MAC address       Type         Age Interfaces
v1        *                 Flood          - All-members
vlansf    00:00:00:00:00:01 Learn       1:07 ge-0/0/1.0
default   *                 Flood          - All-members
```

Display 802.1X protocol information to show that interface ge-0/0/1.0 is connecting and will open LAN access to supplicants:

```
user@switch> show dot1x interface brief
802.1X Information:
Interface     Role           State           MAC address          User
ge-0/0/1.0    Authenticator  Connecting     -                   
ge-0/0/10.0   Authenticator  Initialize     -                   
ge-0/0/14.0   Authenticator  Connecting     -                   
ge-0/0/15.0   Authenticator  Initialize     -                   
ge-0/0/20.0   Authenticator  Initialize     -                   
```

**Meaning**  
The command `show vlans` displays interface ge-0/0/1.0 as a member of the default VLAN. The command `show dot1x interface brief` shows that a supplicant (abc) is authenticated on interface ge-0/0/1.0 and has the MAC address 00:00:00:00:00:01. A RADIUS server timeout occurs, and the authentication server cannot be reached by the
switch. The command **show-ethernet-switching table** shows that MAC address 00:00:00:00:00:01 is learned on VLAN vlan-sf. The supplicant has been moved from the default VLAN to the vlan-sf VLAN. The supplicant is then connected to the LAN through the VLAN named vlan-sf.

### Related Documentation
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
- Configuring Server Fail Fallback (CLI Procedure) on page 1752
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742
- Understanding Server Fail Fallback and Authentication on EX Series Switches on page 1671

### Example: Configuring MAC RADIUS Authentication on an EX Series Switch

To permit hosts that are not 802.1X-enabled to access the LAN, you can configure MAC RADIUS authentication on the switch interfaces to which the non-802.1X-enabled hosts are connected. When MAC RADIUS authentication is configured, the switch will attempt to authenticate the host with the RADIUS server using the host’s MAC address.

This example describes how to configure MAC RADIUS authentication for two non-802.1X-enabled hosts:

- Requirements on page 1713
- Overview and Topology on page 1714
- Configuration on page 1716
- Verification on page 1717

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.3 or later for EX Series switches.
- An EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- A RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the EX Series switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.
- Performed basic bridging and VLAN configuration on the switch. See the documentation that describes setting up basic bridging and a VLAN for your switch. If you are using a
switch that supports the Enhanced Layer 2 Software (ELS) configuration style, see “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073. For all other switches, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.

NOTE: For more about ELS, see: “Getting Started with Enhanced Layer 2 Software” on page 3

• Performed basic 802.1X configuration. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 1740.

Overview and Topology

IEEE 802.1X Port-Based Network Access Control (PNAC) authenticates and permits devices access to a LAN if the devices can communicate with the switch using the 802.1X protocol (are 802.1X-enabled). To permit non-802.1X-enabled end devices to access the LAN, you can configure MAC RADIUS authentication on the interfaces to which the end devices are connected. When the MAC address of the end device appears on the interface, the switch consults the RADIUS server to check whether it is a permitted MAC address. If the MAC address of the end device is configured as permitted on the RADIUS server, the switch opens LAN access to the end device.

You can configure both MAC RADIUS authentication and 802.1X authentication methods on an interface configured for multiple supplicants. Additionally, if an interface is only connected to a non-802.1X-enabled host, you can enable MAC RADIUS and not enable 802.1X authentication using the mac-radius restrict option, and thus avoid the delay that occurs while the switch determines that the device is does not respond to EAP messages.

Figure 16 on page 1715 shows the two printers connected to the switch.
The diagram illustrates the topology for MAC RADIUS Authentication Configuration.

Table 204 on page 1715 shows the components in the example for MAC RADIUS authentication.

### Table 204: Components of the MAC RADIUS Authentication Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 ports (ge-0/0/0 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>sales</td>
</tr>
<tr>
<td>Connections to printers</td>
<td>ge-0/0/19, MAC address 00040ffdacfe</td>
</tr>
<tr>
<td>(no PoE required)</td>
<td>ge-0/0/20, MAC address 0004aecd235f</td>
</tr>
<tr>
<td>RADIUS server</td>
<td>Connected to the switch on interface ge-0/0/10</td>
</tr>
</tbody>
</table>
The printer with the MAC address 00040ffdacfe is connected to access interface ge-0/0/19. A second printer with the MAC address 0004aecd235f is connected to access interface ge-0/0/20. In this example, both interfaces are configured for MAC RADIUS authentication on the switch, and the MAC addresses (without colons) of both printers are configured on the RADIUS server. Interface ge-0/0/20 is configured to eliminate the normal delay while the switch attempts 802.1X authentication; MAC RADIUS authentication is enabled and 802.1X authentication is disabled using the `mac radius restrict` option.

### Configuration

**CLI Quick Configuration**

To quickly configure MAC RADIUS authentication, copy the following commands and paste them into the switch terminal window:

```conf
[edit]
set protocols dot1x authenticator interface ge-0/0/19 mac-radius
set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
```

**NOTE:** You must also configure the two MAC addresses as usernames and passwords on the RADIUS server, as is done in step 2 of the Step-by-Step Procedure.

### Step-by-Step Procedure

Configure MAC RADIUS authentication on the switch and on the RADIUS server:

1. On the switch, configure the interfaces to which the printers are attached for MAC RADIUS authentication, and configure the `restrict` option on interface `ge-0/0/20`, so that only MAC RADIUS authentication is used:

   ```conf
   [edit]
   user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-radius
   user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
   ```

2. On the RADIUS server, configure the MAC addresses 00040ffdacfe and 0004aecd235f as usernames and passwords:

   ```sh
   [root@freeradius#]
   edit /etc/raddb
   vi users
   00040ffdacfe Auth-type:=EAP,User-Password = "00040ffdacfe"
   0004aecd235f Auth-type:=EAP,User-Password = "0004aecd235f"
   ```

### Results

Display the results of the configuration on the switch:

```text
user@switch> show configuration
protocols {  
dot1x {  
authenticator {  
authentication-profile-name profile52;  
interface {  
ge-0/0/19.0 {  
   mac-radius;
  }
ge-0/0/20.0 {
   mac-radius
  }
  
```
Verification

Verify that the supplicants are authenticated:

- Verifying That the Supplicants Are Authenticated on page 1717

Verifying That the Supplicants Are Authenticated

Purpose

After supplicants are configured for MAC RADIUS authentication on the switch and on the RADIUS server, verify that they are authenticated and display the method of authentication:
Action

Display information about 802.1X-configured interfaces ge-0/0/19 and ge-0/0/20:

user@switch> show dot1x interface ge-0/0/19.0 detail
ge-0/0/19.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 1
Supplicant: user101, 00:04:0f:fd:ac:fe
   Operational state: Authenticated
   Authentication method: Radius
   Authenticated VLAN: vo11
   Dynamic Filter: match source-dot1q-tag 10 action deny
   Session Reauth interval: 60 seconds
   Reauthentication due in 50 seconds

user@switch> show dot1x interface ge-0/0/20.0 detail
ge-0/0/20.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Restrict: Enabled
Reauthentication: Enabled
Configured Reauthentication interval: 3600 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 2
Guest VLAN member: <not configured>
Number of connected supplicants: 1
Supplicant: user102, 00:04:ae:cd:23:5f
   Operational state: Authenticated
   Authentication method: Radius
   Authenticated VLAN: vo11
   Dynamic Filter: match source-dot1q-tag 10 action deny
   Session Reauth interval: 60 seconds
   Reauthentication due in 50 seconds

Meaning

The sample output from the `show dot1x interface detail` command displays the MAC address of the connected end device in the Supplicant field. On interface ge-0/0/19, the MAC address is 00:04:0f:fd:ac:fe, which is the MAC address of the first printer configured for MAC RADIUS authentication. The Authentication method field displays the authentication method as MAC Radius. On interface ge-0/0/20, the MAC address is 00:04:ae:cd:23:5f, which is the MAC address of the second printer configured for MAC Radius.
RADIUS authentication. The **Authentication method** field displays the authentication method as **MAC Radius**.

**Related Documentation**
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 1754
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Configuring 802.1X Authentication (J-Web Procedure)
- Understanding Authentication on EX Series Switches on page 1658

**Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch**

You can use RADIUS server attributes and a port firewall filter to centrally apply terms to multiple supplicants (end devices) connected to an EX Series switch in your enterprise. Terms are applied after a device is successfully authenticated through 802.1X. If the firewall filter configuration is modified after end devices are authenticated using the 802.1X authentication, then the established 802.1X authentication session must be terminated and re-established for the firewall filter changes to take effect.

EX Series switches support port firewall filters. Port firewall filters are configured on a single EX Series switch, but in order for them to operate throughout an enterprise, they have to be configured on multiple switches. To reduce the need to configure the same port firewall filter on multiple switches, you can instead apply the filter centrally on the RADIUS server using RADIUS server attributes.

The following example uses FreeRADIUS to apply a port firewall filter on a RADIUS server. For specifics on configuring your server, consult the documentation that was included with your RADIUS server.

This example describes how to configure a port firewall filter with terms, create counters to count packets for the supplicants, apply the filter to user profiles on the RADIUS server, and display the counters to verify the configuration:

- **Requirements** on page 1719
- **Overview and Topology** on page 1720
- **Configuring the Port Firewall Filter and Counters** on page 1722
- **Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server** on page 1724
- **Verification** on page 1724

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 9.3 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you connect the server to the switch, be sure you have:

- Set up a connection between the switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.
- Configured 802.1X authentication on the switch, with the authentication mode for interface ge-0/0/2 set to multiple. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 1740 and “Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch” on page 1684.
- Configured users on the RADIUS authentication server (in this example, the user profiles for Supplicant 1 and Supplicant 2 in the topology are modified on the RADIUS server).

**Overview and Topology**

When the 802.1X configuration on an interface is set to multiple supplicant mode, you can apply a single port firewall filter configured through the Junos OS CLI on the EX Series switch to any number of end devices (supplicants) on one interface by adding the filter centrally to the RADIUS server. Only a single filter can be applied to an interface; however, the filter can contain multiple terms for separate end devices.

For more information about firewall filters, see “Firewall Filters for EX Series Switches Overview” on page 4088.

RADIUS server attributes are applied to end devices after the devices are successfully authenticated using 802.1X. To authenticate an end device, the switch forwards the end device's credentials to the RADIUS server. The RADIUS server matches the credentials against preconfigured information about the supplicant located in the supplicant’s user profile on the RADIUS server. If a match is found, the RADIUS server instructs the switch to open an interface to the end device. Traffic then flows from and to the end device on the LAN. Further instructions configured in the port firewall filter and added to the end device’s user profile using a RADIUS server attribute further define the access that the end device is granted. Filtering terms configured in the port firewall filter are applied to the end device after 802.1X authentication is complete.

**NOTE:** If you modify the port firewall filter after an end device is successfully authenticated using 802.1X, you must terminate and re-establish the 802.1X authentication session for the firewall filter configuration changes to be effective.

Figure 17 on page 1721 shows the topology used for this example. The RADIUS server is connected to an EX4200 switch on access port ge-0/0/10. Two end devices (supplicants) are accessing the LAN on interface ge-0/0/2. Supplicant 1 has the MAC address 00:50:8b:6f:60:3a. Supplicant 2 has the MAC address 00:50:8b:6f:60:3b.
Table 205 on page 1721 describes the components in this topology.

Table 205: Components of the Firewall Filter and RADIUS Server Attributes Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4200 access switch, 24 Gigabit Ethernet ports, 8 PoE ports.</td>
</tr>
<tr>
<td>One RADIUS server</td>
<td>Backend database with the address 10.0.0.100 connected to the switch at port ge-0/0/10.</td>
</tr>
</tbody>
</table>
| 802.1X supplicants connected to the switch on interface ge-0/0/2 | - Supplicant 1 has MAC address 00:50:8b:6f:60:3a.  
- Supplicant 2 has MAC address 00:50:8b:6f:60:3b. |
Table 205: Components of the Firewall Filter and RADIUS Server Attributes Topology (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port firewall filter to be applied on the RADIUS server</td>
<td>filter1</td>
</tr>
<tr>
<td>Counters</td>
<td>counter1 counts packets from Supplicant 1, and counter2 counts packets from Supplicant 2.</td>
</tr>
<tr>
<td>Policer</td>
<td>policer p1</td>
</tr>
</tbody>
</table>
| User profiles on the RADIUS server | • Supplicant 1 has the user profile supplicant1.  
• Supplicant 2 has the user profile supplicant2. |

In this example, you configure a port firewall filter named filter1. The filter contains terms that will be applied to the end devices based on the MAC addresses of the end devices. When you configure the filter, you also configure the counters counter1 and counter2. Packets from each end device are counted, which helps you verify that the configuration is working. Policer policer p1 limits the traffic rate based on the values for exceeding and discard parameters. Then, you check to see that the RADIUS server attribute is available on the RADIUS server and apply the filter to the user profiles of each end device on the RADIUS server. Finally, you verify the configuration by displaying output for the two counters.

NOTE: For more information about authentication, authorization, and accounting (AAA) services, see the Junos OS System Basics Configuration Guide.

Configuring the Port Firewall Filter and Counters

**CLI Quick Configuration**

To quickly configure a port firewall filter with terms for Supplicant 1 and Supplicant 2 and create parallel counters for each supplicant, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
set firewall family ethernet-switching filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard
set firewall family ethernet-switching-filter filter filter1 term supplicant1 then count counter1
set firewall family ethernet-switching-filter filter filter1 term supplicant2 then count counter2
```

**Step-by-Step Procedure**

1. Configure a port firewall filter (here, filter1) with terms for each end device based upon the MAC address of each end device:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term supplicant1 from source-mac-address 00:50:8b:6f:60:3a
user@switch# set filter filter1 term supplicant2 from source-mac-address 00:50:8b:6f:60:3b
```
2. Set policer definition:

user@switch# show policer p1 | display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall policer p1 then discard

3. Create two counters that will count packets for each end device and a policer which limits the traffic rate:

   [edit firewall family ethernet-switching]
   user@switch# set filter filter1 term supplicant1 then count counter1
   user@switch# set filter filter1 term supplicant1 then policer p1
   user@switch# set filter filter1 term supplicant2 then count counter2

Results

Display the results of the configuration:

user@switch> show configuration
firewall {
    family ethernet-switching {
        filter filter1 {
            term supplicant1 {
                from {
                    source-mac-address {
                        00:50:8b:6f:60:3a;
                    }
                }
                then count counter1;
                then policer p1;
            }
            term supplicant2 {
                from {
                    source-mac-address {
                        00:50:8b:6f:60:3b;
                    }
                }
                then count counter2;
            }
        }
    }
    policer p1 {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 1k;
        }
        then discard;
    }
}
Applying the Port Firewall Filter to the Supplicant User Profiles on the RADIUS Server

Step-by-Step Procedure

To verify that the RADIUS server attribute Filter-ID is on the RADIUS server and to apply the filter to the user profiles:

1. Display the dictionary dictionary.rfc2865 on the RADIUS server, and verify that the attribute Filter-ID is in the dictionary:

   [root@freeradius]# cd/usr/share/freeradius/dictionary.rfc2865

2. Close the dictionary file.

3. Display the local user profiles of the end devices to which you want to apply the filter (here, the user profiles are called supplicant1 and supplicant2):

   [root@freeradius]# cat /usr/local/etc/raddb/users

   The output shows:

   supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-Id = "1005"

   supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-Id = "1005"

4. Apply the filter to both user profiles by adding the line Filter-Id = "filter1" to each profile, and then close the file:

   [root@freeradius]# cat /usr/local/etc/raddb/users

   After you paste the line into the files, the files look like this:

   supplicant1 Auth-Type := EAP, User-Password == "supplicant1"
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-Id = "1005",
   Filter-Id = "filter1"

   supplicant2 Auth-Type := EAP, User-Password == "supplicant2"
   Tunnel-Type = VLAN,
   Tunnel-Medium-Type = IEEE-802,
   Tunnel-Private-Group-Id = "1005",
   Filter-Id = "filter1"

Verification

Verifying That the Filter Has Been Applied to the Supplicants

Purpose

After the end devices are authenticated, verify that the filter has been configured on the switch and added to each end device’s user profile on the RADIUS server:
**Action**

Display information about firewall filter `filter1`:

```plaintext
user@switch> show firewall filter filter1
Filter: filter1
Counters:
Name       Bytes  Packets
counter1   128     2
counter2   64      1
```

**Meaning**

The output of the command `show firewall filter filter1` displays `counter1` and `counter2`. Packets from Supplicant 1 are counted using `counter1`, and packets from Supplicant 2 are counted using `counter2`. The output displays packets incrementing for both counters. The filter has been applied to both end devices.

**Related Documentation**

- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741
- Understanding Authentication on EX Series Switches on page 1658
- Understanding 802.1X and VSAs on EX Series Switches on page 1670

**Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication**

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see “Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication” on page 4186. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.
This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

- **Requirements** on page 1726
- **Overview and Topology** on page 1726
- **Configuration** on page 1728
- **Verification** on page 1730

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 13.2 or later for EX Series switches
- One EX4300 switch
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.
- Configured 802.1X authentication on the switch, with the authentication mode for the interface ge-0/0/2 set to **multiple**. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 1740 and “Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch” on page 1684.
- Configured users on the RADIUS authentication server.

**Overview and Topology**

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines the interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 18 on page 1727, when User 1 is authenticated by the EX Series switch, the system creates the firewall filter **dynamic-filter-example**. When User 2 is authenticated, another term is added to the firewall filter, and so on.
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

**NOTE:** If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface ge-0/0/2 to the file server, which is located on subnet 192.0.2.16/28, and set policer definitions to rate-limit the traffic. Figure 19 on page 1728 shows the network topology for this example.
Figure 19: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server

**Configuration**

**Configuring Firewall Filters on Interfaces with Multiple Supplicants**

**CLI Quick Configuration**
To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter filter1 term term1 from ip-destination-address 192.0.2.16/28
set firewall family ethernet-switching filter filter1 term term2 from ip-destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

**Step-by-Step Procedure**
To configure firewall filters on an interface enabled for multiple supplicants:

1. Set the policer definition:

```
user@switch# show policer p1 | display set
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1500
set firewall policer p1 then discard
```
2. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term2 from ip-destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

### Results

Check the results of the configuration:

```
user@switch> show configuration

firewall {
    family ethernet-switching {
        filter filter1 {
            term term1 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
                then count counter1;
            }
            term term2 {
                from {
                    ip-destination-address {
                        192.0.2.16/28;
                    }
                }
                then policer p1;
            }
        }
        policer p1 {
            if-exceeding {
                bandwidth-limit 1m;
                burst-size-limit 1500;
            }
            then discard;
        }
    }
    protocols {
        dot1x {
            authenticator
            interface ge-0/0/2 {
                supplicant multiple;
            }
        }
    }
}
```
Verification

**Verifying Firewall Filters on Interfaces with Multiple Supplicants**

**Purpose**
Verify that firewall filters are functioning on the interface with multiple supplicants.

**Action**
1. Check the results with one user authenticated on the interface. In this case, User 1 is authenticated on ge-0/0/2:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x_ge-0/0/2
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   ```

2. When a second user, User 2, is authenticated on the same interface, ge-0/0/2, you can verify that the filter includes the results for both of the users authenticated on the interface:

   ```
   user@switch> show dot1x firewall
   Filter: dot1x-filter-ge-0/0/0
   Counters
   counter1_dot1x_ge-0/0/2_user1 100
   counter1_dot1x_ge-0/0/2_user2 400
   ```

**Meaning**
The results displayed by the `show dot1x firewall` command output reflect the dynamic filter created with the authentication of each new user. User 1 accessed the file server located at the specified destination address 100 times, while User 2 accessed the same file server 400 times.

**Related Documentation**
- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch on page 1719
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742

**Example: Setting Up Captive Portal Authentication on an EX Series Switch**

**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Setting Up Captive Portal Authentication on an EX Series Switch. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

You can set up captive portal authentication (hereafter referred to as captive portal) on a switch to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.
This example describes how to set up captive portal on an EX4300 switch:

- Requirements on page 1731
- Overview and Topology on page 1731
- Configuration on page 1731
- Verification on page 1733
- Troubleshooting on page 1734

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 13.2X50 or later for EX Series switches
- An EX4300 Series switch

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073.
- Generated an SSL certificate and installed it on the switch. See “Generating SSL Certificates to Be Used for Secure Web Access” on page 418.
- Configured basic access between the EX Series switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.
- Designed your captive portal login page. See “Designing a Captive Portal Authentication Login Page on an EX Series Switch” on page 1759.

**Overview and Topology**

This example shows the configuration required on the switch to enable captive portal on an interface. To permit a printer connected to the captive portal interface to access the LAN, add its MAC address to the authentication whitelist and assign to a VLAN, vlan1. The MAC addresses on this list are permitted access on the interface without captive portal authentication.

The topology for this example consists of one EX4300 switch connected to a RADIUS authentication server. One interface on the switch is configured for captive portal. In this example, the interface is configured in multiple supplicant mode.

**Configuration**

To configure captive portal on your switch:

To quickly configure captive portal on the switch after completing the tasks in the Requirements section, copy the following commands and paste them into the switch terminal window:

```
[edit]
set system services web-management https local-certificate my-signed-cert
set services captive-portal secure-authentication https
set services captive-portal interface ge-0/0/10.0 supplicant multiple
set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
```
To configure captive portal on the switch:

1. To create a secure channel for Web access to the switch, configure captive portal for HTTPS:
   a. Associate the security certificate with the Web server and enable HTTPS on the switch:

   ```
   [edit]
   user@switch# set system services web-management https local-certificate my-signed-cert
   ```

   **NOTE:** You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

   b. Configure captive portal to use HTTPS:

   ```
   [edit]
   user@switch# set services captive-portal secure-authentication https
   ```

2. Enable an interface for captive portal:

   ```
   [edit]
   user@switch# set services captive-portal interface ge-0/0/10 supplicant multiple
   ```

3. (Optional) Allow specific clients to bypass captive portal authentication:

   ```
   [edit]
   user@switch# set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
   ```

   **NOTE:** If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the clear captive-portal mac-address mac-address command after adding its MAC address to the whitelist. Otherwise, the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

   ```
   [edit]
   user@switch# set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1
   ```

   **NOTE:** Optionally, you can use set switch-options authentication-whitelist 00:10:12:e0:28:22 vlan-assignment vlan1 interface ge-0/0/10.0 to limit the scope to the interface.

4. (Optional) To redirect clients to a specified page rather than the page they originally requested, configure the post-authentication URL:

   ```
   [edit services captive-portal]
   user@switch# set custom-options post-authentication-url http://www.my-home-page.com
   ```

**Results** Display the results of the configuration:
[edit]
user@switch# show
system {
    services {
        web-management {
            https {
                local-certificate my-signed-cert;
            }
        }
    }
}
security {
    certificates {
        local {
            my-signed-cert {
                "-----BEGIN RSA PRIVATE KEY-----
                MIIICXwIBAAKBgQDk8sUggnXdDUmr7TvL63yJq/\nRfDASfDZI3z9ZDe1Kfk5C9\n
Pt5YmvWDoGo0mSjoE/iH0BqYdh9YGqV3T2IEUflSTQQHEOShS0ogWDHF\nonyOb1Q/vQtjK2X9NVQgJHBwidssY9eRp\n
-----END CERTIFICATE-----
";
            ##SECRET-DATA
        }
    }
}
services {
    captive-portal {
        interface {
            ge-0/0/10.0 {
                supplicant multiple;
            }
        }
        secure-authentication https;
        custom-options {
            post-authentication-url http://www.my-home-page.com;
        }
    }
}
switch-options {
    authentication-whitelist {
        00:10:12:e0:28:22/48 {
            vlan-assignment vlan1;
        }
    }
}

**Verification**

To confirm that captive portal authentication is configured and working properly, perform these tasks:

- [Verifying That Captive Portal Is Enabled on the Interface on page 1734](#)
- [Verify That Captive Portal Is Working Correctly on page 1734](#)
Verifying That Captive Portal Is Enabled on the Interface

Purpose
Verify that captive portal is configured on the interface ge-0/0/10.

Action
Use the operational mode command show captive-portal interface interface-name detail:

```
user@switch> show captive-portal interface ge-0/0/10.0 detail
ge-0/0/10.0
  Supplicant mode: Multiple
  Number of retries: 3
  Quiet period: 60 seconds
  Configured CP session timeout: 3600 seconds
  Server timeout: 15 seconds
```

Meaning
The output confirms that captive portal is configured on the interface ge-0/0/10, with the default settings for number of retries, quiet period, CP session timeout, and server timeout.

Verify That Captive Portal Is Working Correctly

Purpose
Verify that captive portal is working on the switch.

Action
Connect a client to the interface ge-0/0/10. From the client, open a Web browser and request a webpage. The captive portal login page that you designed should be displayed. After you enter your login information and are authenticated against the RADIUS server, the Web browser should display either the page you requested or the post-authentication URL that you configured.

Troubleshooting
To troubleshoot captive portal, perform these tasks:

- Troubleshooting Captive Portal on page 1734

Troubleshooting Captive Portal

Problem
The switch does not return the captive portal login page when a user connected to a captive portal interface on the switch requests a webpage.

Solution
You can examine the ARP, DHCP, HTTPS, and DNS counters—if one or more of these counters are not incrementing, this provides an indication of where the problem lies. For example, if the client cannot get an IP address, you might check the switch interface to determine whether the DHCP counter is incrementing—if the counter increments, the DHCP packet was received by the switch.

```
user@switch> show captive-portal firewall ge-0/0/10.0
ge-0/0/10.0
  Filter name: dot1x_ge-0/0/10
Counters:
Name                  Bytes  Packets
  dot1x_ge-0/0/10_CP_arp        7616     119
  dot1x_ge-0/0/10_CP_dhcp        0       0
  dot1x_ge-0/0/10_CP_http        0       0
```
Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients

For 802.1X user authentication, EX Series switches support RADIUS authentication servers that are using Extensible Authentication Protocol–Tunneled TLS (EAP-TTLS) to authenticate Odyssey Access Client (OAC) supplicants. OAC networking software runs on endpoint computers (desktop, laptop, or notepad computers and supported wireless devices) and provides secure access to both wired and wireless networks.

This example describes how to configure an 802.1X-enabled interface on the switch to provide fallback support for OAC users who have entered incorrect login credentials:

- Requirements on page 1735
- Overview and Topology on page 1736
- Configuration on page 1737
- Verification on page 1738

Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.2 or later for EX Series switches
- One EX Series switch acting as an authenticator port access entity (PAE). The ports on the authenticator PAE form a control gate that blocks all traffic to and from supplicants until they are authenticated.
- One RADIUS authentication server that supports 802.1X. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.
- One OAC end device acting as a supplicant.

Before you begin configuring the fallback option, ensure that you have:

- Set up a connection between the switch and the RADIUS server. See "Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch" on page 1675.
- Configured EAP-TTLS on the server. See your RADIUS server documentation.
- Configured users on the RADIUS server. See your RADIUS server documentation.
Overview and Topology

OAC is networking software that runs on endpoint computers (desktop, laptop, or notepad) and supported wireless devices. OAC provides full support for EAP, which is required for secure wireless LAN access.

In this topology, OAC is deployed with an 802.1X-enabled switch and a RADIUS server. The switch functions as an enforcement point in the network security architecture. This topology:

- Ensures that only authorized users can connect.
- Maintains privacy of login credentials.
- Maintains data privacy over the wireless link.

This example includes the configuration of a server-reject VLAN on the switch, which can be used to prevent accidental lockout for users who have entered incorrect login credentials. These users can be given limited LAN access.

However, this fallback configuration is complicated by the fact that the OAC supplicant and RADIUS server are using EAP-TTLS. EAP-TTLS creates a secure encrypted tunnel between the server and the end device to complete the authentication process. When the user enters an incorrect login, the RADIUS server sends EAP failure messages directly to the client through this tunnel. The EAP failure message causes the client to restart the authentication procedure, so that the switch’s 802.1X authentication process tears down the session that was established with the switch using the server-reject VLAN. You can enable the remedial connection to continue by configuring:

- **eapol-block**—Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN. The block timer causes the authentication port access entity to ignore EAP start messages from the client, attempting to restart the authentication procedure.

  **NOTE:** The EAPoL block timer is triggered only after the retries on the 802.1X interface have been exhausted. You can configure retries to specify the number of times the switch attempts to authenticate the port after an initial failure. The default is three retries.

- **block-interval**—Configure the amount of time that you want the EAPoL block timer to continue to ignore EAP start messages. If you do not configure the block interval, the EAPoL block timer defaults to 120 seconds.

When the 802.1X interface ignores the EAP start messages from the client, the switch allows the existing remedial session that was established through the server-reject VLAN to remain open.

These configuration options apply to **single**, **single-secure**, and **multiple** supplicant authentication modes. In this example, the 802.1X interface is configured in single-suppliant mode.
Figure 20 on page 1737 shows an EX Series switch connecting an OAC end device to a RADIUS server, and indicates the protocols being used to connect the network entities.

Figure 20: EX Series Switch Connecting OAC to RADIUS Server Using EAP-TTLS Authentication

Table 206 on page 1737 describes the components in this OAC deployment:

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX Series switch</td>
</tr>
<tr>
<td>VLANs</td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>server-reject-vlan: VLAN name is remedial and VLAN ID is 700</td>
</tr>
<tr>
<td>802.1X interface</td>
<td>ge-0/0/8</td>
</tr>
<tr>
<td>OAC supplicant</td>
<td>EAP-TTLS</td>
</tr>
<tr>
<td>One RADIUS authentication server</td>
<td>EAP-TTLS</td>
</tr>
</tbody>
</table>

**Table 206: Components of the OAC Deployment**

**Configuration**

To configure fallback options for EAP-TTLS and OAC supplicants, perform this task:

To quickly configure the fallback options for EAP-TTLS and OAC supplicants, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans remedial vlan-id 700
set protocols dot1x authenticator interface ge-0/0/8 retries 4
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan remedial
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan eapol-block
set protocols dot1x authenticator interface ge-0/0/8 server-reject-vlan block-interval 130
```
To configure the fallback options for EAP-TTLS and OAC supplicants:

**Step-by-Step Procedure**

1. **TIP:** In this example, the switch has only one server-reject VLAN. Therefore, the configuration specifies `eapol-block` and `block-interval` directly after `server-reject-vlan`. However, if you have configured multiple VLANs on the switch, you should include the VLAN name or VLAN ID directly after `server-reject-vlan` to indicate which VLAN is being modified.

1. Configure a VLAN that will function as the server-reject VLAN to provide limited LAN access for users who have entered incorrect login credentials:

   ```
   [edit]
   user@switch# set vlans remedial vlan-id 700
   ```

2. Configure the number of times for the client to be prompted for username and password before an incorrect login is directed to the server-reject VLAN:

   ```
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set retries 4
   ```

3. Configure the 802.1X authenticator interface to use the server-reject VLAN as a fallback for incorrect logins:

   ```
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set server-reject-vlan remedial
   ```

4. Enable the EAPoL block timer on the 802.1X interface that is configured to belong to the server-reject VLAN:

   ```
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set server-reject-vlan eapol-block
   ```

5. Configure the amount of time for the EAPoL block to remain in effect:

   ```
   [edit protocols dot1x authenticator interface ge-0/0/8]
   user@switch# set server-reject-vlan block-interval 130
   ```

**Results**

Check the results of the configuration:

```
user@switch> show configuration
protocols {
  dot1x {
    authenticator {
      interface {
        ge-0/0/8.0 {
          supplicant single;
          retries 4;
          server-reject-vlan remedial block-interval 130 eapol-block;
        }
      }
    }
  }
}
```

**Verification**

To confirm that the configuration and the fallback options are working correctly, perform this task:

- **Verifying the Configuration of the 802.1X Interface on page 1739**
Verifying the Configuration of the 802.1X Interface

Purpose
Verify that the 802.1X interface is configured with the desired options:

Action
```
user@switch> show dot1x interface ge-0/0/8.0 detail
```

```
ge-0/0/8.0
Role: Authenticator
Administrative state: Auto
Supplicant mode: Single
Number of retries: 4
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Disabled
Mac Radius Restrict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 120 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPoL requests: 2
Guest VLAN member: guest
Number of connected supplicants: 1
Supplicant: tem, 2A:92:E6:F2:00:00
  Operational state: Authenticated
  Backend Authentication state: Idle
  Authentication method: Radius
  Authenticated VLAN: remedial
  Session Reauth interval: 120 seconds
  Reauthentication due in 68 seconds
```

Meaning
The `show dot1x ge-0/0/8 detail` output shows that the `ge-0/0/8` interface is in the **Authenticated** state and that it is using the **remedial** VLAN.

Related Documentation
- Understanding Authentication on EX Series Switches on page 1658
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742
- Configuring LLDP (CLI Procedure) on page 1745
- Configuring LLDP-MED (CLI Procedure) on page 1748
- VSA Match Conditions and Actions on page 1749
- Configuring Server Fail Fallback (CLI Procedure) on page 1752
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 1754
- Configuring Static MAC Bypass of Authentication (CLI Procedure) on page 1755
- Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure) on page 1756
- Configuring Captive Portal Authentication (CLI Procedure) on page 1757
IEEE 802.1X authentication provides network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

NOTE:
- You can also specify an 802.1X exclusion list to specify supplicants that can bypass authentication and be automatically connected to the LAN. See “Configuring Static MAC Bypass of Authentication (CLI Procedure)” on page 1755.
- You cannot configure 802.1X user authentication on interfaces that have been enabled for Q-in-Q tunneling.
- You cannot configure 802.1X user authentication on redundant trunk groups (RTGs). For more information on RTGs, see “Understanding Redundant Trunk Links on EX Series Switches” on page 2068.

Before you begin, specify the RADIUS server or servers to be used as the authentication server. See “Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure)” on page 1756.

To configure 802.1X on an interface:

1. Configure the supplicant mode as single (authenticates the first supplicant), single-secure (authenticates only one supplicant), or multiple (authenticates multiple supplicants):

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface ge-0/0/5 supplicant multiple
   ```

2. Enable reauthentication and specify the reauthentication interval:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface ge-0/0/5/0 reauthentication interval 5
   ```

3. Configure the interface timeout value for the response from the supplicant:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface ge-0/0/5 supplicant-timeout 5
   ```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface ge-0/0/5 server-timeout 5
   ```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface ge-0/0/5 transmit-period 60
   ```
6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out:

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/5 maximum-requests 5
```

7. Configure the number of times the switch attempts to authenticate the port after an initial failure. The port remains in a wait state during the quiet period after the authentication attempt.

```
[edit protocols dot1x]
user@switch# set authenticator interface ge-0/0/5 retries 1
```

**NOTE:** This setting specifies the number of tries before the switch puts the interface in a “HELD” state.

---

**Related Documentation**

- Configuring 802.1X Authentication (J-Web Procedure)
- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
- Monitoring 802.1X Authentication on page 1813
- Verifying 802.1X Authentication on page 1814
- Configuring LLDP (CLI Procedure) on page 1745
- Understanding Authentication on EX Series Switches on page 1658

---

**Configuring 802.1X RADIUS Accounting (CLI Procedure)**

RADIUS accounting permits statistical data about users logging onto or off a LAN to be collected and sent to a RADIUS accounting server. The statistical data gathered can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based upon the amount of time or type of services accessed.

To configure basic RADIUS accounting using the CLI:

1. Specify the accounting servers to which the switch will forward accounting statistics:

   ```
   [edit access]
   user@switch# set profile profile1 radius accounting-server [122.69.1.250 122.69.1.252]
   ```

2. Define the RADIUS accounting servers:

   ```
   [edit access]
   user@switch# set radius-server 122.69.1.250 secret juniper
   user@switch# set radius-server 122.69.1.252 secret juniper1
   ```

3. Enable accounting for an access profile:

   ```
   [edit access]
   user@switch# set profile profile1 accounting
   ```

4. Configure the RADIUS servers to use while sending accounting messages and updates:

   ```
   [edit access]
   user@switch# set profile profile1 accounting order radius
   ```

5. Configure the statistics to be collected on the switch and forwarded to the accounting server:

   ```
   [edit access]
   ```
6. Display accounting statistics collected on the switch:

   user@switch> show network-access aaa statistics accounting
   Accounting module statistics
   Requests received: 1
   Accounting Response failures: 0
   Accounting Response Success: 1
   Requests timeout: 0

7. Open an accounting log on the RADIUS accounting server using the server’s address, and view accounting statistics:

   [root@freeradius]# cd /usr/local/var/log/radius/radacct/122.69.1.250
   [root@freeradius 122.69.1.250]# ls
   detail-20071214

   [root@freeradius 122.69.1.250]# vi details-20071214

   User-Name = "000347e1bab9"
   NAS-Port = 67
   Acct-Status-Type = Stop
   Acct-Session-Id = "802.1x811912"
   Acct-Input-Octets = 17454
   Acct-Output-Octets = 4245
   Acct-Session-Time = 1221041249
   Acct-Input-Packets = 72
   Acct-Output-Packets = 53
   Acct-Terminate-Cause = Lost-Carrier
   Acct-Input-Gigawords = 0
   Acct-Output-Gigawords = 0
   Called-Station-Id = "00-19-e2-50-52-60"
   Calling-Station-Id = "00-03-47-e1-ba-b9"
   Event-Timestamp = "Sep 10 2008 16:52:39 PDT"
   NAS-Identifier = "esp48t-1b-01"
   NAS-Port-Type = Virtual

   User-Name = "000347e1bab9"
   NAS-Port = 67
   Acct-Status-Type = Start
   Acct-Session-Id = "802.1x811219"
   Called-Station-Id = "00-19-e2-50-52-60"
   Calling-Station-Id = "00-03-47-e1-ba-b9"
   Event-Timestamp = "Sep 10 2008 18:58:52 PDT"
   NAS-Identifier = "esp48t-1b-01"
   NAS-Port-Type = Virtual

Related Documentation

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 1675
- Understanding 802.1X and RADIUS Accounting on EX Series Switches on page 1664

Filtering 802.1X Supplicants Using RADIUS Server Attributes

There are two ways to configure the RADIUS server with port firewall filters:

- Include a match statement and corresponding action in the Juniper-Firewall-Filter attribute. The Juniper-Firewall-Filter attribute is a vendor-specific attribute (VSA) in
the Juniper dictionary on the RADIUS server. Use this attribute to configure simple filter
conditions for authenticated users. Nothing needs to be configured on the switch; all
of the configuration is on the RADIUS server.

- Apply a local firewall filter to users authenticated through the RADIUS server. Use this
  method for more complex filters. The firewall filter must be configured on each switch.

  **NOTE:** If the firewall filter configuration is modified after users are
  authenticated using the 802.1X authentication, then the established 802.1X
  authentication session must be terminated and re-established for the
  firewall filter configuration changes to take effect.

This example describes using FreeRADIUS software to configure VSAs. For specifics on
configuring your server, consult the AAA documentation that was included with your
server.

This topic includes the following tasks:

1. Configuring Match Statements on the RADIUS Server on page 1743
2. Applying a Port Firewall Filter from the RADIUS Server on page 1745

**Configuring Match Statements on the RADIUS Server**

You can configure simple filter conditions using the `Juniper-Switching-Filter` attribute in
the Juniper dictionary on the RADIUS server. These filters are then sent to a switch
whenever a new user is authenticated successfully. The filters are created and applied
on all EX Series switches that authenticate users through that RADIUS server without
the need to configure anything on each individual switch.

To configure the `Juniper-Switching-Filter` attribute, enter one or more match conditions
and a resulting action using the CLI for the RADIUS server. Enter the match statement
plus an action statement enclosed within quotes (" ") using the following syntax:

```plaintext
match <destination-mac mac-address> <source-vlan vlan-name> <source-dot1q-tag tag> <destination-ip ip-address> <ip-protocol protocol-id> <source-port port> <destination-port port>
}
action [allow | deny] <forwarding-class class-of-service> <loss-priority (low | medium | high)>}
```

See “VSA Match Conditions and Actions” on page 1749 for definitions of match statement
options.

To configure match conditions on the RADIUS server:

1. Verify that the Juniper dictionary is loaded on your RADIUS server and includes the
   filtering attribute `Juniper-Switching-Filter`, attribute ID 48:

   ```bash
   [root@freeradius]# cat /usr/local/share/freeradius/dictionary.juniper
   # dictionary.juniper
   ```
2. Enter the match conditions and actions. For example:

   - To deny authentication based on the 802.1Q tag (here, the 802.1Q tag is 10):
     
     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```
     
     For each relevant user, add the `Juniper-Switching-Filter` attribute:
     
     ```
     Juniper-Switching-Filter = "match source-dot1q-tag 10 action deny"
     ```

   - To deny access based on a destination IP address:
     
     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```
     
     For each relevant user, add the `Juniper-Switching-Filter` attribute:
     
     ```
     Juniper-Switching-Filter = "match destination-ip 192.168.1.0/31 action deny"
     ```

   - To set the packet loss priority (PLP) to high based on a destination MAC address and the IP protocol:
     
     ```
     [root@freeradius]# cd /usr/local/etc/raddb
     vi users
     ```
     
     For each relevant user, add the `Juniper-Switching-Filter` attribute:
     
     ```
     Juniper-Switching-Filter = "match destination-mac 00:04:0f:fd:ac:fe, ip-protocol 2, forwarding-class high, action loss-priority high"
     ```

     
     **NOTE:** For the forwarding-class option to be applied, the forwarding class must be configured on the switch. If it is not configured on the switch, this option is ignored. You must specify both the forwarding class and the packet loss priority.

3. Stop and restart the RADIUS process to activate the configuration.
Applying a Port Firewall Filter from the RADIUS Server

You can apply a firewall filter to user policies on the RADIUS server. The RADIUS server can then specify the firewall filters that are to be applied to each user that requests to authenticate. Use this method when the firewall filter has more extensive conditions or you want to use different conditions for the same filter on different switches. The firewall filters must be configured on each switch.

For more information about firewall filters, see “Firewall Filters for EX Series Switches Overview” on page 4088.

To apply a port firewall filter centrally from the RADIUS server:

1. Create the firewall filter on the local switch. In this example, the filter is called `filter1`.

2. Open the users file on the RADIUS server:

   ```
   [root@freeradius#] cd /usr/local/pool/raddb
   [root@freeradius#] vi users
   ```

3. For each relevant user, add the filter (here, the filter ID is `filter1`):

   ```
   Filter-Id = "filter1"
   ```

```

**NOTE:** Multiple filters are not supported on a single interface. However, you can support multiple filters for multiple users that are connected to the switch on the same interface by configuring a single filter with policies for each of those users.

4. Stop and restart the RADIUS process to activate the configuration.

Related Documentation

- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch on page 1719
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Understanding 802.1X and VSAs on EX Series Switches on page 1670

Configuring LLDP (CLI Procedure)

Devices use Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) to learn and distribute device
information on network links. The information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

This topic describes:

- Enabling LLDP on Interfaces on page 1746
- Adjusting LLDP Advertisement Settings on page 1746
- Adjusting SNMP Notification Settings of LLDP Changes on page 1747
- Specifying a Management Address for the LLDP Management TLV on page 1747
- Configuring LLDP Power Negotiation on page 1747

**Enabling LLDP on Interfaces**

LLDP is enabled on all interfaces by default. If it is disabled, you can enable LLDP by configuring it on all interfaces or on specific interfaces.

- To configure LLDP on all interfaces:
  
  ```
  [edit protocols lldp]
  user@switch# set interface all
  ```

- To configure LLDP on a specific interface:
  
  ```
  [edit protocols lldp]
  user@switch# set interface ge-0/0/3
  ```

**Adjusting LLDP Advertisement Settings**

You can adjust the following settings for LLDP advertisements for troubleshooting or verification purposes. The default values are applied when LLDP is enabled. For normal operations, we recommend that you do not adjust these settings from the default values.

- To specify the frequency at which LLDP advertisements are sent (in seconds):
  
  ```
  [edit protocols lldp]
  user@switch# set advertisement-interval 45
  ```

- To specify the number of seconds that LLDP information is held before it is discarded (the multiplier value is used in combination with the `advertisement-interval` value):
  
  ```
  [edit protocols lldp]
  user@switch# set hold-multiplier 5
  ```

- To specify the number of seconds the device delays before sending advertisements to neighbors after a change is made in a TLV (type, length, or value) element in LLDP or in the state of the local system, such as a change in hostname or management address, set the transmit delay. The transmit delay is enabled by default on switches to reduce the delay in notifying neighbors of a change in the local system. The default value is 2 seconds if the `advertisement-interval` value is set to 8 seconds or more or 1 second if the `advertisement-interval` value is set to less than 8 seconds.

  ```
  [edit protocols lldp]
  user@switch# set transmit-delay 2
  ```
NOTE: The advertisement-interval value must be greater than or equal to four times the transmit-delay value, or an error will be returned when you attempt to commit the configuration.

Adjusting SNMP Notification Settings of LLDP Changes

You can adjust the following settings for SNMP notifications of LLDP changes. If the values are not specified or if the interval values are set to 0, the notifications are disabled.

- To specify the frequency at which LLDP database changes are sent (in seconds):
  ```
  [edit protocols lldp]
  user@switch# set lldp-configuration-notification-interval 600
  ```

- To specify the frequency at which changes in topology global statistics are sent (in seconds):
  ```
  [edit protocols lldp]
  user@switch# set ptopo-configuration-trap-interval 600
  ```

- To specify the holding time (used in combination with the `ptopo-configuration-trap-interval` value) to determine the length of time that topology global statistics are held before they are discarded (in seconds):
  ```
  [edit protocols lldp]
  user@switch# set ptopo-configuration-maximum-hold-time 2147483647
  ```

Specifying a Management Address for the LLDP Management TLV

You can configure an IP management address to be used in the LLDP Management type, length, and value (TLV).

To configure the management address:

```
[edit protocols lldp]
user@switch# set management-address 192.168.0.1
```

Configuring LLDP Power Negotiation

LLDP power negotiation allows the switch’s Power over Ethernet (PoE) controller to dynamically allocate PoE power to PoE interfaces, based on the needs of the powered device, by negotiating with LLDP-enabled powered devices.

NOTE: LLDP power negotiation is not supported on EX3200 and EX4200 (except EX4200 PX models) switches.

LLDP power negotiation is supported on switches running PoE controller software version 4.04 or higher. For information about the PoE controller software, see “Upgrading the PoE Controller Software” on page 3967.

LLDP power negotiation is automatically enabled when the PoE management mode is set to `class`. 
• To disable LLDP power negotiation on switch interfaces:

```
[edit protocols lldp interface all power-negotiation]
user@switch# disable
```

• To disable LLDP power negotiation on a specific switch interface:

```
[edit protocols lldp interface ge-0/0/10 power-negotiation]
user@switch# disable
```

**Related Documentation**

- Configuring LLDP (J-Web Procedure)
- Configuring LLDP-MED (CLI Procedure) on page 1748
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665

## Configuring LLDP-MED (CLI Procedure)

Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) is an extension of LLDP. The EX Series switch uses LLDP-MED to support device discovery of VoIP telephones and to create location databases for these telephone locations.

LLDP-MED is turned on by default on EX Series switches.

This topic describes:

- Enabling LLDP-MED on Interfaces on page 1748
- Configuring Location Information Advertised by the Switch on page 1748
- Configuring for Fast Start on page 1749

### Enabling LLDP-MED on Interfaces

LLDP-MED is enabled on all interfaces by default. If it is disabled, you can enable LLDP-MED by configuring it on all interfaces or on specific interfaces.

**NOTE:** On switches running Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, configure LLDP-MED on the physical interface—for example, on ge-0/0/2. For more about ELS, see “Getting Started with Enhanced Layer 2 Software” on page 3.

To configure LLDP-MED on all interfaces or on a specific interface:

```
[edit protocols lldp-med]
user@switch# set interface (LLDP-MED) ge-0/0/2.0
```

### Configuring Location Information Advertised by the Switch

You can configure the location information that is advertised from the switch to the LLDP-MED device. You can specify a civic-based location (geographic location) or a location based on an ELIN (Emergency Location Identification Number):

- To specify a location by geography:

```
[edit protocols lldp-med]
user@switch# set interface ge-0/0/2.0 location civic-based country-code US
```
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 1 ca-value “El Dorado County”
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 2 ca-value CA
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 3 ca-value Somerset
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 6 ca-value “Mount Aukum Road”
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 19 ca-value 6450
user@switch# set interface ge-0/0/2.0 location civic-based ca-type 21 ca-value “Holiday Market”

To specify a location using an elin string:

[edit protocols lldp-med]
user@switch# set interface ge-0/0/2.0 location elin 4085551212

Configuring for Fast Start

You can specify the number of LLDP-MED advertisements sent from the switch in the first second after it has detected an LLDP-MED device. The default is 3; to set it to another value:

[edit protocols lldp-med]
user@switch# set fast-start 6

NOTE: If an interface is configured as a VoIP interface, then the switch does not wait for an attached phone to identify itself as an LLDP-MED device before it performs an LLDP-MED fast start after a graceful Routing Engine switchover (GRES) or a reboot. Instead, it immediately performs an LLDP-MED fast start after a GRES or reboot. This behavior prevents certain models of IP phones from resetting after a GRES.

Related Documentation

• Configuring LLDP (J-Web Procedure)
• Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
• Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch on page 1690
• Configuring LLDP (CLI Procedure) on page 1745
• Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665

VSA Match Conditions and Actions

EX Series switches and the QFX Series support the configuration of RADIUS server attributes specific to Juniper Networks. These attributes are known as vendor-specific attributes (VSAs). They are configured on RADIUS servers and work in combination with 802.1X authentication. Using VSAs, you can apply port firewall filter attributes as a subset of match conditions and actions sent from the RADIUS server to the switch as a result of successful 802.1X authentication.

Each term in a VSA configured through the RADIUS server consists of match conditions and an action. Match conditions are the values or fields that the packet must contain. You can define single, multiple, or no match conditions. If no match conditions are
specified for the term, the packet is accepted by default. The action is the action that
the switch takes if a packet matches the match conditions for the specific term. Allowed
actions are to accept a packet or to discard a packet.

The following guidelines apply when you specify match conditions and actions for VSAs:

- Both **match** and **action** statements are mandatory.
- Any or all options (separated by commas) may be included in each **match** and **action**
  statement.
- Fields separated by commas will be ANDed if they are of a different type. The same
types cannot be repeated.
- For OR cases (for example, match `10.1.1.0/24 OR 11.1.1.0/24`), apply multiple VSAs to
  the 802.1X supplicant.
- In order for the **forwarding-class** option to be applied, the forwarding class must be
  configured on the switch. If it is not configured on the switch, this option is ignored.

Table 207 on page 1750 describes the match conditions you can specify when configuring
a VSA using the **match** command on the RADIUS server. The string that defines a match
condition is called a **match statement**.

### Table 207: Match Conditions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-mac mac-address</td>
<td>Destination media access control (MAC) address of the packet.</td>
</tr>
<tr>
<td>source-vlan source-vlan</td>
<td>Name of the source VLAN.</td>
</tr>
<tr>
<td>source-dot1q-tag tag</td>
<td>Tag value in the 802.1Q header, in the range 0 through 4095.</td>
</tr>
<tr>
<td>destination-ip ip-address</td>
<td>Address of the final destination node.</td>
</tr>
<tr>
<td>ip-protocol protocol-id</td>
<td>IPv4 protocol value. In place of the numeric value, you can specify one of the following text synonyms: ah, egp (8), esp (50), gre (47), icmp (1), igmp (2), ipv6 (41), ospf (89), pim (103), rsvp (46), tcp (6), or udp (17)</td>
</tr>
<tr>
<td>source-port port</td>
<td>TCP or User Datagram Protocol (UDP) source port field. Normally, you specify this match statement in conjunction with the <strong>ip-protocol</strong> match statement to determine which protocol is being used on the port. In place of the numeric field, you can specify one of the text options listed under <strong>destination-port</strong>.</td>
</tr>
</tbody>
</table>
TCP or UDP destination port field. Normally, you specify this match in conjunction with the `ip-protocol` match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify one of the following text synonyms (the port numbers are also listed):

- afs (1483), bgp (179), biff (512), bootpc (68), bootps (67), cvspserv (2401), cmd (514), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20), http (80), https (443), ident (113), imap (143), kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), kshell (544), ldap (389), login (513), mobileip-agent (434), mobile-ip-mn (435), msdp (639), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), nfld (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radacct (1813), radius (1812), rip (520), rkin (2108), smtp (25), snmp (161), snmp-trap (162), sntp (444), socks (1080), ssh (22), snoop (111), syslog (514), telnet (23), tacacs+ (6), talk (517), tftp (69), timed (525), who (513), xdmcp (177), zephyr-clt (2103), zephyr-hm (2104)

When you define one or more terms that specify the filtering criteria, you also define the action to take if the packet matches all criteria. Table 208 on page 1751 shows the actions that you can specify in a term.

### Table 208: Actions for VSAs

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`(allow</td>
<td>deny)`</td>
</tr>
<tr>
<td>forwarding-class <code>class-of-service</code></td>
<td>(Optional) Classify the packet in one of the following forwarding classes:</td>
</tr>
<tr>
<td></td>
<td>• assured-forwarding</td>
</tr>
<tr>
<td></td>
<td>• best-effort</td>
</tr>
<tr>
<td></td>
<td>• expedited-forwarding</td>
</tr>
<tr>
<td></td>
<td>• network-control</td>
</tr>
<tr>
<td>loss-priority (low</td>
<td>medium</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742
- Understanding 802.1X and VSAs on EX Series Switches on page 1670
- Understanding VSAs on the QFX Series
Configuring Server Fail Fallback (CLI Procedure)

Server fail fallback allows you to specify how end devices connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends a RADIUS access-reject message.

802.1X and MAC RADIUS authentication work by using an authenticator port access entity (the EX Series switch) to block all traffic to and from an end device at the interface until the end device’s credentials are presented and matched on the authentication server (a RADIUS server). When the end device has been authenticated, the switch stops blocking and opens the interface to the end device.

When you set up 802.1X or MAC RADIUS authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. Because the authentication server grants or denies access to the end devices awaiting authentication, the switch does not receive access instructions for end devices attempting access to the LAN and normal authentication cannot be completed. Server fail fallback allows you to configure authentication alternatives that permit the switch to take appropriate actions toward end devices awaiting authentication or reauthentication.

NOTE: The authentication fallback method called server-reject VLAN provides limited access to a LAN, typically just to the Internet, for responsive end devices that are 802.1X-enabled but that have sent the wrong credentials. If the end device that is authenticated using the server-reject VLAN is an IP phone, voice traffic is not allowed.
To configure basic server fail fallback options using the CLI:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the end device had been successfully authenticated by a RADIUS server):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface ge-0/0/1 server-fail permit
  ```

- Configure an interface to prevent traffic flow from an end device to the LAN (as if the end device had failed authentication and had been rejected by the RADIUS server):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface ge-0/0/1 server-fail deny
  ```

- Configure an interface to move an end device to a specified VLAN if a RADIUS server timeout occurs (in this case, the VLAN name is `vlan1`):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface ge-0/0/1 server-fail vlan-name vlan1
  ```

- Configure an interface to recognize already connected end devices as reauthenticated if there is a RADIUS timeout during reauthentication (new users will be denied access):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface ge-0/0/1 server-fail use-cache
  ```

- Configure an interface that receives a RADIUS access-reject message from the authentication server to move end devices attempting LAN access on the interface to a specified VLAN already configured on the switch (in this case, the VLAN name is `vlan-sf`):

  ```
  [edit protocols dot1x authenticator]
  user@switch# set interface ge-0/0/1 server-reject-vlan vlan-sf
  ```

NOTE: If an IP phone is authenticated in the server-reject VLAN, voice traffic is not allowed.

Related Documentation
- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch on page 1707
- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Monitoring 802.1X Authentication on page 1813
- Understanding Server Fail Fallback and Authentication on EX Series Switches on page 1671
Configuring MAC RADIUS Authentication (CLI Procedure)

You can permit devices that are not 802.1X-enabled LAN access by configuring MAC RADIUS authentication on the EX Series switch interfaces to which the hosts are connected.

**NOTE:** You can also allow non-802.1X-enabled devices to access the LAN by configuring their MAC address for static MAC bypass of authentication.

You can configure MAC RADIUS authentication on an interface that also allows 802.1X authentication, or you can configure either authentication method alone.

If both MAC RADIUS and 802.1X authentication are enabled on the interface, the switch first sends the host three EAPOL requests to the host. If there is no response from the host, the switch sends the host's MAC address to the RADIUS server to check whether it is a permitted MAC address. If the MAC address is configured as permitted on the RADIUS server, the RADIUS server sends a message to the switch that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.

If MAC RADIUS authentication is configured on the interface but 802.1X authentication is not (by using the *mac-radius restrict* option), the switch attempts to authenticate the MAC address with the RADIUS server without delaying by attempting 802.1X authentication first.

Before you configure MAC RADIUS authentication, be sure you have:

- Configured basic access between the EX Series switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.

To configure MAC RADIUS authentication using the CLI:

- On the switch, configure the interfaces to which the nonresponsive hosts are attached for MAC RADIUS authentication, and add the *restrict* qualifier for interface ge-0/0/20 to have it use only MAC RADIUS authentication:

  ```
  [edit]
  user@switch# set protocols dot1x authenticator interface ge-0/0/19 mac-radius
  user@switch# set protocols dot1x authenticator interface ge-0/0/20 mac-radius restrict
  ```

- On a RADIUS authentication server, create user profiles for each nonresponsive host using the MAC address (without colons) of the nonresponsive host as the username and password (here, the MAC addresses are 00:04:0f:fd:ac:fe and 00:04:ae:cd:23:5f):

  ```
  [root@freeradius]#
  edit /etc/raddb
  vi users
  00040ff dacfe Auth-type:=Local, User-Password = "00040ff dacfe"
  0004ae cd23 5f Auth-type:=Local, User-Password = "0004ae cd23 5f"
  ```

**Related Documentation**

- Example: Configuring MAC RADIUS Authentication on an EX Series Switch on page 1713
Configuring Static MAC Bypass of Authentication (CLI Procedure)

You can configure a static MAC bypass list (sometimes called the exclusion list) on the switch to specify MAC addresses of devices allowed access to the LAN without 802.1X or MAC RADIUS authentication requests to the RADIUS server.

To configure the static MAC bypass list:

- Specify a MAC address to bypass authentication:

  [edit protocols dot1x]
  user@switch#  set authenticator static 00:04:0f:fd:ac:fe

- Configure a supplicant to bypass authentication if connected through a particular interface:

  [edit protocols dot1x]
  user@switch#  set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5

- You can configure a supplicant to be moved to a specific VLAN after it is authenticated:

  [edit protocols dot1x]
  user@switch#  set authenticator static 00:04:0f:fd:ac:fe interface ge-0/0/5 vlan-assignment default-vlan

Related Documentation

- Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch on page 1704
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Configuring 802.1X Authentication (J-Web Procedure)
Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure)

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant’s credentials or MAC address are presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the switch for each RADIUS server to which you will connect.

To configure a RADIUS server on the switch:

1. Define the IP address of the RADIUS server, the RADIUS server authentication port number, and the secret password. You can define more than one RADIUS server. The secret password on the switch must match the secret password on the server:

   [edit access]
   user@switch# set radius-server 10.0.0.100 port 1812 secret abc

   **NOTE:** Specifying the authentication port is optional, and port 1812 is the default. However, we recommend that you configure it in order to avoid confusion as some RADIUS servers might refer to an older default.

2. (Optional) Specify the IP address by which the switch is identified by the RADIUS server. If you do not specify this, the RADIUS server uses the address of the interface sending the RADIUS request. We recommend that you specify this IP address because if the request gets diverted on an alternate route to the RADIUS server, the interface relaying the request might not be an interface on the switch:

   [edit access]
   user@switch# set access radius-erversource-address 10.93.14.100

3. Configure the authentication order, making radius the first method of authentication:

   [edit access]
   user@switch# set profile profile1 authentication-order radius

4. Create a profile and specify the list of RADIUS servers to be associated with the profile. For example, you might choose to group your RADIUS servers geographically by city. This feature enables easy modification whenever you want to change to a different set of authentication servers:

   [edit access profile]
   user@switch# set atlanta radius authentication-server 10.0.0.100 10.2.14.200

5. Specify the group of servers to be used for 802.1X or MAC RADIUS authentication by identifying the profile name:

   [edit access profile]
   user@switch# set protocols dot1x authenticator authentication-profile-name denver

6. Configure the IP address of the EX Series switch in the list of clients on the RADIUS server. For specifics on configuring the RADIUS server, consult the documentation for your server.
Related Documentation

- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 1754
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741

Configuring Captive Portal Authentication (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Captive Portal Authentication (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Configure captive portal authentication (hereafter referred to as captive portal) on an EX Series switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See “Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch” on page 2073.
- Generated an SSL certificate and installed it on the switch. See “Generating SSL Certificates to Be Used for Secure Web Access” on page 418.
- Configured basic access between the EX Series switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.
- Designed your captive portal login page. See “Designing a Captive Portal Authentication Login Page on an EX Series Switch” on page 1759.

This topic includes the following tasks:

- Configuring Secure Access for Captive Portal on page 1757
- Enabling an Interface for Captive Portal on page 1758
- Configuring Bypass of Captive Portal Authentication on page 1758

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate my-signed-cert
```
NOTE: You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@switch# set switch-options authentication-whitelist 00:10:12:e0:28:22
```

NOTE: Optionally, you can use `set switch-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0` to limit the scope to the interface.

NOTE: If the client is already attached to the switch, you must clear its MAC address from the captive portal authentication by using the `clear captive-portal mac-address session-mac-addr` command after adding its MAC address to the whitelist. Otherwise the new entry for the MAC address will not be added to the Ethernet switching table and the authentication bypass will not be allowed.

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 1730
- Understanding Authentication on EX Series Switches on page 1658
Designing a Captive Portal Authentication Login Page on an EX Series Switch

You can set up captive portal authentication on your switch to redirect all Web browser requests to a login page that requires the user to input a username and password before they are allowed access. Upon successful authentication, the user is allowed access to the network and redirected to the original page requested.

Junos OS provides a customizable template for the captive portal window that allows you to easily design and modify the look of the captive portal login page. You can modify the design elements of the template to change the look of your captive portal login page and to add instructions or information to the page. You can also modify any of the design elements of a captive portal login page.

The first screen displayed before the captive login page requires the user to read the “Terms and Conditions of Use”. By clicking the Agree button, the user can access the captive portal login page.

Figure 21 on page 1759 shows an example of a captive portal login page:

Figure 21: Example of a Captive Portal Login Page

Table 209 on page 1759 summarizes the configurable elements of a captive portal login page.

Table 209: Configurable Elements of a Captive Portal Login Page

<table>
<thead>
<tr>
<th>Element</th>
<th>CLI Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Footer background color</td>
<td>footerbgcolor hex-color</td>
<td>The HTML hexadecimal code for the background color of the captive portal login page footer.</td>
</tr>
</tbody>
</table>
Table 209: Configurable Elements of a Captive Portal Login Page (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>CLI Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Footer message</td>
<td>footer-message text-string</td>
<td>Text displayed in the footer of the captive portal login page. You can include copyright information, links, and additional information such as help instructions, legal notices, or a privacy policy. The default text shown in the footer is Copyright © 2010, Juniper Networks Inc.</td>
</tr>
<tr>
<td>Footer text color</td>
<td>footer-text-color color</td>
<td>Color of the text in the footer. The default color is white.</td>
</tr>
<tr>
<td>Form header background color</td>
<td>form-header-bgc hex-color</td>
<td>The HTML hexadecimal code for the background color of the header bar across the top of the form area of the captive portal login page.</td>
</tr>
<tr>
<td>Form header message</td>
<td>form-header-message text-string</td>
<td>Text displayed in the header of the captive portal login page. The default text is Captive Portal User Authentication.</td>
</tr>
<tr>
<td>Form header text color</td>
<td>form-header-text-color color</td>
<td>Color of the text in the form header. The default color is black.</td>
</tr>
<tr>
<td>Form reset button label</td>
<td>form-reset-label label-name</td>
<td>Using the Reset button, the user can clear the username and password fields on the form.</td>
</tr>
<tr>
<td>Form submit button label</td>
<td>form-submit-label label-name</td>
<td>Using the Login button, the user can submit the login information.</td>
</tr>
<tr>
<td>Header background color</td>
<td>header-bgc hex-color</td>
<td>The HTML hexadecimal code for the background color of the captive portal login page header.</td>
</tr>
<tr>
<td>Header logo</td>
<td>header-logo filename</td>
<td>Filenname of the file containing the image of the logo that you want to appear in the header of the captive portal login page. The image file can be in GIF, JPEG, or PNG format. You can upload a logo image file to the switch. Copy the logo to the /var/tmp directory on the switch (during commit, the files are saved to persistent locations). If you do not specify a logo image, the Juniper Networks logo is displayed.</td>
</tr>
<tr>
<td>Header message</td>
<td>header-message text-string</td>
<td>Text displayed in the page header. The default text is User Authentication.</td>
</tr>
<tr>
<td>Header text color</td>
<td>header-text-color color</td>
<td>Color of the text in the header. The default color is white.</td>
</tr>
<tr>
<td>Post-authentication URL</td>
<td>post-authentication-url url</td>
<td>URL to which the users are directed on successful authentication. By default, users are directed to the page they had originally requested.</td>
</tr>
</tbody>
</table>

To design the captive portal login page:

1. (Optional) Upload your logo image file to the switch:
   ```
   user@switch> file copy ftp://username:prompt@ftp.hostname.net/var/tmp/my-logo.jpeg
   ```
2. Configure the custom options to specify the background colors and text displayed in the captive portal page:
[edit system services captive-portal]
user@switch# set custom-options header-bgcolor #006600
set custom-options header-message "Welcome to Our Network"
set custom-options banner-message "Please enter your username and password". The banner
displays the message "XXXXXXX" by default. The user can modify this message.
set custom-options footer-message "Copyright ©2010, Our Network"

Now you can commit the configuration.

---

**NOTE:** For the custom options that you do not specify, the default value is used.

---

Related Documentation

- Example: Setting Up Captive Portal Authentication on an EX Series Switch
- Understanding Authentication on EX Series Switches on page 1658
- captive-portal

Controlling Authentication Session Timeouts (CLI Procedure)

For 802.1X and MAC RADIUS authentication sessions, the timeout of the session depends on the reauthentication value that you configure. Additionally, unless you configure it not to, the session is removed from the authentication session table when the MAC address ages out of the Ethernet switching table (when the value specified for the mac-table-aging-time is exceeded).

Before you begin:

- Specify the RADIUS server or servers to be used as the authentication server. See “Specifying RADIUS Server Connections on an EX Series Switch (CLI Procedure)” on page 1756.
- Configure 802.1X authentication on the switch. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 1740.
To configure the authentication session time on all interfaces:

```
[edit]
user@switch# set protocols dot1x authenticator interface all seconds;
```

To configure the authentication session time on a single interface:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name seconds;
```

To disable removal of authentication sessions from the authentication session table when a MAC address ages out of the Ethernet switching table, remove the binding of the authentication table to the Ethernet switching table.

To remove the binding on all interfaces:

```
[edit]
user@switch# set protocols dot1x authenticator interface all no-mac-table-binding;
```

To remove the binding on a single interface:

```
[edit]
user@switch# set protocols dot1x authenticator interface interface-name no-mac-table-binding;
```

### Related Documentation

- Configuring MAC Table Aging (CLI Procedure)
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
- Understanding Authentication on EX Series Switches on page 1658
- Understanding Authentication Session Timeout on page 1673

### Configuration Statements

- [edit access] Configuration Statement Hierarchy on EX Series Switches on page 1762
- [edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches on page 1769

#### [edit access] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit access] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit access] Hierarchy Level on page 1763
- Unsupported Statements in the [edit access] Hierarchy Level on page 1767
Supported Statements in the [edit access] Hierarchy Level

The following hierarchy shows the [edit access] configuration statements supported on EX Series switches:

access {
    address-assignment {
        abated-utilization;
        abated-utilization-v6;
        high-utilization;
        high-utilization-v6;
        neighbor-discovery-router-advertisement;
    }
    pool name {
        family {
            inet {
                dhcp-attributes {
                    boot-file filename;
                    boot-server server-address;
                    domain-name domain-name;
                    grace-period seconds;
                    maximum-lease-time (length | infinite);
                    name-server ip-address;
                    netbios-node-type (b-node | h-node | m-node | p-node);
                    option option-identifier-code;
                    option-match {
                        option-82 {
                            circuit-id match-value;
                            remote-id match-value;
                        }
                    }
                    router ip-address;
                    server-identifier;
                    tftp-server;
                    wins-server ip-address;
                }
                host;
                network;
                range;
                xauth-attributes;
            }
        }
        inet6 {
            dhcp-attributes;
            prefix;
            range;
        }
    }
    link name {
        family {
            inet;
            inet6;
        }
    }
    address-pool pool-name {

address address-or-prefix;
address-range <low lower-limit> <high upper-limit>;
}
address-protection;
domain {
delimiter characters;
map name {
  aaa-logical-system name {
  }
  aaa-routing-instance;
  aaa-routing-instance aaa-routing-instance;
  access-profile;
  address-pool;
  dynamic-profile;
  padn destination-ip-address;
  strip-domain;
  target-logical-system;
  target-routing-instance;
}
parse-direction (left-to-right | right-to-left);
}
domain-name-server address;
domain-name-server-inet address;
domain-name-server-inet6 address;
group-profile;
gx-plus {
global {
  include-ipv6;
  max-outstanding-requests;
}
partition {
  destination-host;
  destination-realm;
  diameter-instance;
}
}
ldap-options {
assemble {
  common-name name;
}
base-distinguished-name name;
revert-interval seconds;
search {
  admin-search {
    distinguished-name name;
    password password;
  }
  search-filter filter;
}
}
ldap-server address {
  port number;
  retry number;
  routing-instance routing-instance;
  source-address address;
  timeout seconds;
ppp-options; profile profile-name {
  accounting {
    accounting-stop-on-access-denied;
    accounting-stop-on-failure;
    coa-immediate-update;
    duplication;
    immediate-update;
    order (radius | none);
    statistics (time | volume-time);
    wait-for-acct-on-ack;
  }
  accounting-order (radius | [accounting-order-data-list]);
  address-assignment {
    pool;
  }
  authentication-order [(ldap | none | password | radius | secureid)];
  authorization-order (jsrc | [authorization-order-data-list]);
  client client-name {
    chap-secret chap-secret;
    client-group;
    firewall-user {
      password password;
    }
    ike;
    no-rfc2406;
    pap-password password;
  }
  client-name-filter {
    count number;
    domain-name name;
    separator character;
  }
  domain-name-server;
  domain-name-server-inet;
  domain-name-server-inet6;
  ldap-options {
    assemble {
      common-name name;
    }
    base-distinguished-name name;
    revert-interval seconds;
    search {
      admin-search {
        distinguished-name name;
        password password;
      }
      search-filter filter;
    }
  }
  ldap-server address {
    port number;
    retry number;
    routing-instance routing-instance;
    source-address address;
}
timeout seconds;
}
provisioning-order {
  gx-plus;
  jsr;
}
radius {
  accounting-server [server-addresses];
  attributes {
    exclude [exclude-options];
    ignore [ignore-options];
  }
  authentication-server [server-addresses];
  options {
    accounting-session-id-format (decimal | description);
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    coa-dynamic-variable-validation;
    ethernet-port-type-virtual;
    interface-description-format {
      exclude-adapter;
      exclude-sub-interface;
    }
    juniper-dsl-attributes;
    nas-identifier nas-identifier;
    nas-port-extended-format {
      adapter-width adapter-width;
      ae-width ae-width;
      port-width port-width;
      slot-width slot-width;
      stacked-vlan-width stacked-vlan-width;
      vlan-width vlan-width;
    }
    nas-port-id-delimiter nas-port-id-delimiter;
    nas-port-id-format {
      agent-circuit-id;
      agent-remote-id;
      interface-description;
      nas-identifier;
    }
    nas-port-type {
      ethernet;
    }
    revert-interval seconds;
    vlans-nas-port-stacked-format;
  }
}
radius-server address {
  max-outstanding-requests max-outstanding-requests;
  port port-number;
  retry retry;
  routing-instance instance-name;
  secret secret;
  source-address address;
  timeout seconds;
}
service {
    accounting-order {
        activation-protocol;
        radius;
    }
}

session-options {
    client-group [group-names];
    client-idle-timeout minutes;
    client-session-timeout minutes;
}

radius-options {
    interim-rate number;
    interim-update-tolerance interim-update-tolerance;
    request-rate number;
    revert-interval interval;
}

radius-server server-address {
    accounting-port port-number;
    max-outstanding-requests number;
    port port-number;
    retry attempts;
    routing-instance instance-name;
    secret password;
    source-address address;
    timeout seconds;
}

securid-server server-name {
    configuration-file file-path;
}

terminate-code {
}

Unsupported Statements in the [edit access] Hierarchy Level

All statements in the [edit access] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 210: Unsupported [edit access] Configuration Statements on EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>[edit access terminate-code]</td>
</tr>
<tr>
<td>administrative-reset</td>
<td>[edit access terminate-code aaa shutdown]</td>
</tr>
<tr>
<td>authentication-denied</td>
<td>[edit access terminate-code aaa deny]</td>
</tr>
<tr>
<td>client-request</td>
<td>[edit access terminate-code aaa dhcp]</td>
</tr>
</tbody>
</table>
Table 210: Unsupported [edit access] Configuration Statements on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>compliance</td>
<td>[edit access ppp-options]</td>
</tr>
<tr>
<td>deny</td>
<td>[edit access terminate-code aaa]</td>
</tr>
<tr>
<td>dhcp</td>
<td>[edit access terminate-code]</td>
</tr>
<tr>
<td>group-profile</td>
<td>[edit access]</td>
</tr>
<tr>
<td>ike</td>
<td>[edit access profile client]</td>
</tr>
<tr>
<td>initiate-dead-peer-detection</td>
<td>[edit access profile client ike]</td>
</tr>
<tr>
<td>lost-carrier</td>
<td>[edit access terminate-code dhcp]</td>
</tr>
<tr>
<td>nak</td>
<td>[edit access terminate-code dhcp]</td>
</tr>
<tr>
<td>nas-logout</td>
<td>[edit access terminate-code dhcp]</td>
</tr>
<tr>
<td>no-offers</td>
<td>[edit access terminate-code dhcp]</td>
</tr>
<tr>
<td>no-resources</td>
<td>[edit access terminate-code aaa deny]</td>
</tr>
<tr>
<td>ppp-options</td>
<td>[edit access]</td>
</tr>
<tr>
<td>preference</td>
<td>[edit access profile client ike reverse-route]</td>
</tr>
<tr>
<td>remote-reset</td>
<td>[edit access terminate-code aaa shutdown]</td>
</tr>
<tr>
<td>rfc</td>
<td>[edit access ppp-options compliance]</td>
</tr>
<tr>
<td>reverse-route</td>
<td>[edit access profile client ike]</td>
</tr>
<tr>
<td>server-request-timeout</td>
<td>[edit access terminate-code aaa deny]</td>
</tr>
<tr>
<td>shutdown</td>
<td>[edit access terminate-code aaa]</td>
</tr>
<tr>
<td>terminate-code</td>
<td>[edit access]</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 1675
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741
- Security Features for EX Series Switches Overview on page 4085
This topic lists supported and unsupported configuration statements in the [edit protocols dot1x] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit protocols dot1x] Hierarchy Level on page 1769
- Unsupported Statements in the [edit protocols dot1x] Hierarchy Level on page 1770

**Supported Statements in the [edit protocols dot1x] Hierarchy Level**

The following hierarchy shows the [edit protocols dot1x] configuration statements supported on EX Series switches:

```
protocols {
    dot1x {
        authenticator {
            authentication-profile-name access-profile-name;
            interface (all | [ interface-names ] ) {
                disable;
                guest-vlan (vlan-id | vlan-name);
                mac-radius {
                    flap-on-disconnect;
                    restrict;
                }
                maximum-requests number;
                no-reauthentication;
                quiet-period seconds;
                reauthentication {
                    interval seconds;
                }
                retries number;
                server-fail (deny | permit | use-cache | vlan-id | vlan-name);
                server-reject-vlan (vlan-id | vlan-name) {
                    eapol-block;
                    block-interval block-interval;
                }
                server-timeout seconds;
                supplicant (single | single-secure | multiple);
                supplicant-timeout seconds;
                transmit-period seconds;
            }
            no-mac-table-binding {
                interface interface-names
            }
        }
    }
}
```
static mac-address
}  
static mac-address {
  interface interface-names;
  vlan-assignment (vlan-id |vlan-name);
}
}
}
}
}

traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable> <match regex>;
  flag flag ;
}

Unsupported Statements in the [edit protocols dot1x] Hierarchy Level

All statements in the [edit protocols dot1x] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

• Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX Series Switch on page 1679
• Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
• Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch on page 1707
• Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 1735
• Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch on page 1704
• 802.1X for EX Series Switches Overview on page 1655
• [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
accounting (Access Profile)

Syntax

```plaintext
accounting {
  accounting-stop-on-access-deny;
  accounting-stop-on-failure;
  address-change-immediate-update;
  coa-immediate-update;
  coa-no-override service-class-attribute;
  duplication;
  duplication-vrf {
    access-profile-name profile-name;
    vrf-name vrf-name;
  }
  immediate-update;
  order [ accounting-method ];
  send-acct-status-on-config-change
  statistics (time | volume-time);
  update-interval minutes;
  wait-for-acct-on-ack;
}
```

Hierarchy Level

[edit access profile profile-name]

Release Information

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description

Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

The remaining statements are explained separately.

Required Privilege

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Per-Subscriber Session Accounting
- Understanding RADIUS Accounting Duplicate Reporting
accounting-order

Syntax
accounting-order (radius | [accounting-order-data-list]);

Hierarchy Level
[edit access profile profile-name]

Release Information
Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Enable RADIUS accounting for an L2TP profile.

Options
radius—Use the RADIUS accounting method.

[accounting-order-data-list]—Set of data listing the accounting order to be used, enclosed by brackets. This can be any combination of accounting methods, up to and including and entire list of the entire accounting order.

Required Privilege
Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
• Configuring Access Profiles for L2TP or PPP Parameters

accounting-port

Syntax
accounting-port port-number;

Hierarchy Level
[edit access radius-server server-address],
[edit access profile profile-name radius-server server-address]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Configure the port number on which to contact the accounting server.

Options
port-number—Port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).

Required Privilege
Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
• Configuring Router or Switch Interaction with RADIUS Servers
• Configuring Authentication and Accounting Parameters for Subscriber Access
• Configuring RADIUS Authentication for L2TP
address-assignment (Address-Assignment Pools)

Syntax

address-assignment {
  abated-utilization percentage;
  abated-utilization-v6 percentage;
  high-utilization percentage;
  high-utilization-v6 percentage;
  neighbor-discovery-router-advertisement ndra-pool-name;
  pool pool-name {
    family family {
      dhcp-attributes {
        protocol-specific attributes;
      }
      host hostname {
        hardware-address mac-address;
        ip-address ip-address;
      }
      network ip-prefix/<prefix-length>;
      prefix ipv6-prefix;
      range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length prefix-length;
      }
      range pool-name;
    }
  }
}

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure address-assignment pools that can be used by different client applications.

NOTE: Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

Options pool-name—Name assigned to an address-assignment pool.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • Address-Assignment Pools Overview on page 1206
• Configuring Address-Assignment Pools
address-protection

Syntax

```plaintext
address-protection;
```

Hierarchy Level

- [edit access],
- [edit logical-systems logical-system-name routing-instances routing-instance-name access]

Release Information

- Statement introduced in Junos OS Release 11.2.
- Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Prevents IPv6 prefixes from being used more than once when AAA is used to supply IPv6 prefixes for router advertisement.

If enabled, the router checks the following attributes received from external servers:

- Framed-IPv6-Prefix
- Framed-IPv6-Pool

The router then takes one of the following actions:

- If a prefix overlaps with a prefix in an address pool, the prefix is taken from the pool if it is available.
- If the prefix is already in use, it is rejected as unavailable.
- If the prefix length requested from the external server does not match the pool's prefix length exactly, the authentication request is denied. If configured, the Acct-Stop message includes a termination cause.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Duplicate Prefix Protection for Router Advertisement
- Duplicate Prefix Protection for NDRA
Authorization Order

Syntax
authorization-order (jsrc | [authorization-order-data-list]);

Hierarchy Level
[edit access profile profile-name]

Release Information
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Configure AAA to use JSRC in an SRC environment to request authorization from the SAE when verifying that a DHCP subscriber can access the router. When you include this statement, AAA ignores any configured authentication order settings. This statement is ignored for non-DHCP subscribers.

Options
- jsrc—Use JSRC application to communicate with the SAE for subscriber authorization. JSRC is the only application that is currently available.
- [authorization-order-data-list]—Set of data listing the authorization order to be used, enclosed by brackets. This can be any combination of authorization methods, up to and including the entire list of the entire authorization order.

Required Privilege
- admin—to view this statement in the configuration.
- admin-control—to add this statement to the configuration.

Related Documentation
- Configuring JSRC
- Authorizing Subscribers with JSRC
**authentication-order**

Syntax  
authentication-order [(none | ldap | password | radius | secureid)];

Hierarchy Level  
[edit access profile profile-name]

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
(EX and QFX Series only) Configure the order of authentication, authorization, and accounting (AAA) servers to use while sending authentication messages.

Default  
Not enabled

Options  
none—No authentication for specified subscribers.


password—Locally configured password in access profile.

radius—RADIUS authentication.

securid—RSA SecurID authentication.

Required Privilege  
Level  
admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Related Documentation  
•  Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 1675

•  Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741
**authentication-whitelist**

Syntax  
authentication-whitelist {  
  mac-address {  
    interface interface-name;  
    vlan-assignment {  
      vlan-id | vlan-name;  
    }  
  }  
}

Hierarchy Level  
[edit ethernet-switching-options].  
[edit switch-options]

Release Information  
Statement introduced in Junos OS Release 10.1 for EX Series switches.  

Description  
Configure MAC addresses for which RADIUS authentication is to be bypassed.

Required Privilege Level  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

Related Documentation  
• Example: Setting Up Captive Portal Authentication on an EX Series Switch  
• Example: Setting Up Captive Portal Authentication on an EX Series Switch on page 1730  
• Configuring Captive Portal Authentication (CLI Procedure)  
• Configuring Captive Portal Authentication (CLI Procedure) on page 1757

**client-accounting-algorithm**

Syntax  
client-accounting-algorithm (direct | round-robin);

Hierarchy Level  
[edit access profile profile-name radius options]

Release Information  
Statement introduced in Junos OS Release 10.0.  
Statement introduced in Junos OS for EX Series switches Release 13.2X50-D10.

Description  
Configure the access method the router uses to access RADIUS accounting servers.

Default  
direct

Options  
direct—Use the direct method.  
round-robin—Use the round-robin method.

Required Privilege Level  
admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration.

Related Documentation  
• Configuring RADIUS Server Parameters for Subscriber Access  
• Configuring RADIUS Server Options for Subscriber Access
**client-authentication-algorithm**

**Syntax**

client-authentication-algorithm (direct | round-robin);

**Hierarchy Level**

[edit access profile profile-name radius options]

**Release Information**

Statement introduced in Junos OS Release 10.0.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Configure the access method the router uses to access RADIUS authentication servers.

**Default**

direct

**Options**

direct—Use the direct method.

round-robin—Use the round-robin method.

**Required Privilege Level**

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**

• Configuring RADIUS Server Parameters for Subscriber Access
• Configuring RADIUS Server Options for Subscriber Access

**coa-dynamic-variable-validation**

**Syntax**

coa-dynamic-variable-validation;

**Hierarchy Level**

[edit access profile profile-name radius options]

**Release Information**

Statement introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message.

**Default**

If you do not configure this statement, the router does not apply any incorrect variable updates but does make any other changes to the client profile dynamic variables, and then responds with an ACK message.

**Required Privilege Level**

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**

• Configuring RADIUS Server Options for Subscriber Access
• Configuring RADIUS Server Parameters for Subscriber Access
**destination-host (Gx-Plus)**

Syntax  
destination-host hostname;

Hierarchy Level  
[edit access gx-plus partition partition-name]

Release Information  
Statement introduced in Junos OS Release 11.2.  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  
Configure the host on which the PCRF application resides.

Options  
* hostname—Host on which the PCRF is installed.

Required Privilege Level  
* admin—To view this statement in the configuration.  
* admin-control—To add this statement to the configuration.

Related Documentation  
* Configuring Gx-Plus  
* Configuring the Gx-Plus Partition

**destination-realm (Gx-Plus)**

Syntax  
destination-realm realm;

Hierarchy Level  
[edit access gx-plus partition partition-name]

Release Information  
Statement introduced in Junos OS Release 11.2.  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  
Configure the realm in which the PCRF host resides.

Options  
* realm—Realm in which the PCRF host resides.

Required Privilege Level  
* admin—To view this statement in the configuration.  
* admin-control—To add this statement to the configuration.

Related Documentation  
* Configuring Gx-Plus  
* Configuring the Gx-Plus Partition
diameter-instance (Gx-Plus)

**Syntax**
diameter-instance instance-name;

**Hierarchy Level**
[edit access gx-plus partition partition-name]

**Release Information**
Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**
Specify the Diameter instance associated with the Gx-Plus partition.

**Options**
instance-name—Name of the Diameter instance. Currently, only master is supported.

**Required Privilege**
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Gx-Plus
- Configuring the Gx-Plus Partition
domain (Domain Map)

Syntax

```plaintext
domain {
    delimiter [delimiter-character];
    map domain-map-name {
        aaa-logical-system logical-system-name {
            aaa-routing-instance routing-instance-name;
        }
        aaa-routing-instance routing-instance-name;
        access-profile profile-name;
        address-pool pool-name;
        dynamic-profile profile-name;
        padn destination-address {
            mask destination-mask;
            metric route-metric;
        }
        strip-domain;
        target-logical-system logical-system-name {
            target-routing-instance routing-instance-name;
        }
        target-routing-instance routing-instance-name;
        tunnel-profile profile-name;
        tunnel-switch-profile profile-name;
    }
    parse-direction (left-to-right | right-to-left);
}
```

Hierarchy Level

[edit access]

Release Information

Statement introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure a domain map, which is used to map access options and session parameters for subscriber sessions.

The remaining statements are explained separately.

Required Privilege Level

admin—to view this statement in the configuration.
admin-control—to add this statement to the configuration.

Related Documentation

- Configuring a Domain Map
**domain-name-server (Routing Instances and Access Profiles)**

**Syntax**
```
domain-name-server dns-address;
```

**Hierarchy Level**
- [edit access],
- [edit access profile]

**Release Information**
Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**
Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access profile profile-name] hierarchy level. You can configure more than one address by including the statement multiple times.

**NOTE:** A DNS name server address configured with this statement is lower in preference than one configured with the domain-name-server-inet statement.

**Options**
- `dns-address`—IPv4 address of the DNS name server.

**Required Privilege Level**
- admin—To view this statement in the configuration
- admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring DNS Name Server Addresses for Subscriber Management
- DNS Name Server Address Overview
domain-name-server-inet (Routing Instances and Access Profiles)

Syntax  
domain-name-server-inet dns-address;

Hierarchy Level  
[edit access],  
[edit access profile]

Release Information  
Statement introduced in Junos OS Release 12.3.  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  
Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access profile profile-name] hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is higher in preference than one configured with the domain-name-server statement.

Options  
dns-address—IPv4 address of the DNS name server.

Required Privilege  
admin—To view this statement in the configuration  
admin-control—To add this statement to the configuration.

Related Documentation  
• Configuring DNS Name Server Addresses for Subscriber Management  
• DNS Name Server Address Overview
domain-name-server-inet6 (Routing Instances and Access Profiles)

Syntax  
domain-name-server-inet6 dns-address;

Hierarchy Level  
[edit access],  
[edit access profile]

Release Information  
Statement introduced in Junos OS Release 12.3.  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  
Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access profile profile-name] hierarchy level. You can configure more than one address by including the statement multiple times.

Options  
dns-address—IPv6 address of the DNS name server.

Required Privilege  
Level  
admin—To view this statement in the configuration  
admin-control—To add this statement to the configuration.

Related Documentation  
• Configuring DNS Name Server Addresses for Subscriber Management  
• DNS Name Server Address Overview

ethernet-port-type-virtual

Syntax  
ethernet-port-type-virtual;

Hierarchy Level  
[edit access profile profile-name radius options]

Release Information  
Statement introduced in Junos OS Release 9.1.  
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description  
Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of ethernet in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of virtual.

NOTE: This statement takes precedence over the nas-port-type statement if you include both statements in the same access profile.

Required Privilege  
Level  
admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration.

Related Documentation  
• Configuring RADIUS Server Options for Subscriber Access  
• Configuring RADIUS Server Parameters for Subscriber Access
**global (Gx-Plus)**

Syntax

```
global {
  include-ipv6;
  max-outstanding-requests number;
}
```

Hierarchy Level [edit access gx-plus]


Description Configure global attributes for the Gx-Plus application. The remaining statements are explained separately.

Required Privilege Level

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

Related Documentation
- *Configuring Gx-Plus*

**gx-plus (Gx-Plus)**

Syntax

```
gx-plus {
  global {
    include-ipv6;
    max-outstanding-requests number;
  }
  partition partition-name {
    diameter-instance instance-name;
    destination-host hostname;
    destination-realm realm;
  }
}
```

Hierarchy Level [edit access]


Description Configure the Gx-Plus application to interact with a PCRF to authorize and provision subscribers. The remaining statements are explained separately.

Required Privilege Level

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

Related Documentation
- *Configuring Gx-Plus*
ignore

**Syntax**

```
ignore {
  dynamic-iflset-name;
  framed-ip-netmask;
  input-filter;
  logical-system-routing-instance;
  output-filter;
}
```

**Hierarchy Level**

[edit access profile profile-name radius attributes]

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description**

Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router or switch processes the attributes it receives from the external server.

**Options**

- `dynamic-iflset-name`—Ignore Interface-Set/Dynamic-Ifiset-Name (VSA 26-130).
- `framed-ip-netmask`—Ignore Framed-IP-Netmask (RADIUS attribute 9).
- `input-filter`—Ignore Ingress-Policy-Name (VSA 26-10).
- `logical-system-routing-instance`—Ignore Virtual-Router (VSA 26-1).
- `output-filter`—Ignore Egress-Policy-Name (VSA 26-11).

**Required Privilege Level**

- `admin`—To view this statement in the configuration.
- `admin-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring RADIUS Server Parameters for Subscriber Access](#)
include-ipv6 (Gx-Plus)

Syntax include-ipv6;

Hierarchy Level [edit access gx-plus global]


Description Include IPv6 subscribers in Gx-Plus provisioning requests.

Default By default, IPv6 subscribers are not included.

Required Privilege
Level

Related Documentation
• Configuring Gx-Plus Global Attributes
• Configuring Gx-Plus
## interface (Static MAC Bypass)

**Syntax**  
interface [interface-names];

**Hierarchy Level**  
[edit protocols dot1x authenticator authentication-profile-name static mac-address],  
[edit ethernet-switching-options authentication-whitelist mac-address],  
[edit switch-options on page 2027 authentication-whitelist mac-address]

**Release Information**  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  

**Description**  
Configure interfaces on which the specified MAC addresses are allowed to bypass RADIUS authentication and allowed to connect to the LAN without authentication.

**Options**  
* interface-names—List of interfaces.

**Required Privilege Level**  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**  
- show dot1x static-mac-address on page 1835  
- Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch on page 1704  
  - Example: Setting Up Captive Portal Authentication on an EX Series Switch  
  - Example: Setting Up Captive Portal Authentication on an EX Series Switch  
  - Configuring Captive Portal Authentication (CLI Procedure)
interface (VoIP)

Syntax

interface (all|interface-name|access-ports)
  vlan vlan-name;
  forwarding-class <assured-forwarding|best-effort|expedited-forwarding|
  network-control>;
}

Hierarchy Level

- For platforms with ELS:
  [edit switch-options on page 2027 voip]
- For platforms without ELS:
  [edit ethernet-switching-options voip],

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level [edit switch-options] introduced in Junos OS Release 13.2X50-D10. (See
“Getting Started with Enhanced Layer 2 Software” on page 3 for information about
ELS.)

Description

Enable voice over IP (VoIP) for all interfaces or specific interfaces.

Options

all | interface-name | access-ports—Enable VoIP on all interfaces, on a specific interface,
  or on all access ports.

Required Privilege

Level

system—To view this statement in the configuration.
  system-control—To add this statement to the configuration.

Related Documentation

- Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
- Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication
- Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support
**interface-description-format**

**Syntax**

```plaintext
interface-description-format {
    exclude-adapter;
    exclude-sub-interface;
}
```

**Hierarchy Level**

[edit access profile profile-name radius options]

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options `exclude-adapter` and `exclude-sub-interface` introduced in Junos OS Release 10.4.

**Description**

Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the device includes both the subinterface and the adapter in the interface description.

**Options**

- `exclude-adapter`—Exclude the adapter from the interface description.
- `exclude-sub-interface`—Exclude the subinterface from the interface description.

**Required Privilege**

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

**Related Documentation**

- Configuring RADIUS Server Options for Subscriber Access
- RADIUS Server Options for Subscriber Access
juniper-dsl-attributes

Syntax  
juniper-dsl-attributes;

Hierarchy Level  
[edit access profile profile-name radius options]

Release Information  
Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  
Configure AAA to add Juniper Networks DSL VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:

- Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)—Default configured advisory transmit speed.
- Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)—Default configured advisory receive speed.

Default  
The Juniper Networks DSL VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.

Required Privilege
Level  
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
- Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages
- Configuring ANCP
max-outstanding-requests (Gx-Plus)

Syntax
max-outstanding-requests number;

Hierarchy Level
[edit accessgx-plus global]

Release Information
Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Limit the number of outstanding requests to the PCRF that Gx-Plus can retry when the requests are improperly answered. Too many requests risks overloading the PCRF and increases the chance of losing messages.

Options
number—Number of outstanding requests from Gx-Plus to the PCRF that can exist at any time.
Default: 40
Range: 2 through 40

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
• Configuring Gx-Plus Global Attributes
• Configuring Gx-Plus

nas-identifier

Syntax
nas-identifier identifier-value;

Hierarchy Level
[edit accessprofile profile-name radius options]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.

Options
identifier-value—String to use for authentication and accounting requests.
Range: 1 through 64 characters

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
• Configuring RADIUS Server Options for Subscriber Access
• Configuring RADIUS Server Parameters for Subscriber Access
**nas-port-extended-format (Access Profile)**

**Syntax**

```plaintext
nas-port-extended-format {
  adapter-width width;
  ae-width width;
  port-width width;
  slot-width width;
  stacked;
  stacked-vlan-width width;
  vlan-width width;
  atm {
    adapter-width width;
    port-width width:
    slot-width width;
    vci-width width:
    vpi-width width;
  }
}
```

**Hierarchy Level**

```
[edit access profile profile-name radius options]
```

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Option `ae-width` introduced in Junos OS Release 12.1.
Option `stacked` introduced in Junos OS Release 12.3.
Option `atm` introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
Option `atm` supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

**Description**

In an access profile, configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute. You can use the same access profile to configure the NAS-Port extended format for Ethernet subscribers and ATM subscribers.

**Options**

- `adapter-width width`—Number of bits in the adapter field.
- `ae-width width`—Number of bits in the aggregated Ethernet identifier field.
- `port-width width`—Number of bits in the port field.
- `slot-width width`—Number of bits in the slot field.
- `stacked`—Include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format.
- `stacked-vlan-width width`—Number of bits in the SVLAN ID field.
- `vlan-width width`—Number of bits in the VLAN ID field.
- `atm`—Configure the NAS-Port extended format for ATM subscribers; options include:
  - `adapter-width width`—Number of bits in the adapter field.
• **port-width width**—Number of bits in the port field.
• **slot-width width**—Number of bits in the slot field.
• **vci-width width**—Number of bits in the ATM virtual circuit identifier (VCI) field.
• **vpi-width width**—Number of bits in the ATM virtual path identifier (VPI) field.

**NOTE:** Each field can be 0 through 32 bits wide; however, the total of the widths of all fields must not exceed 32 bits, or the configuration fails. The router may truncate the values of individual fields depending on the bit width you specify.

### Required Privilege
- **Level**
  - admin—To view this statement in the configuration.
  - admin-control—To add this statement to the configuration.

### Related Documentation
- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access

### nas-port-id-delimiter (Subscriber Management)

**Syntax**

```
ns-port-id-delimiter delimiter-character;
```

**Hierarchy Level**

```
[edit access profile profile-name radius options]
```

**Release Information**

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the `nas-port-id-format` statement.

**Default**

The hash (#) character.

**Options**

- `delimiter-character`—Character used for the delimiter.

**Required Privilege**

- **Level**
  - admin—To view this statement in the configuration.
  - admin-control—To add this statement to the configuration.

**Related Documentation**

- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access
- Configuring a NAS-Port-ID with Additional Options
nas-port-id-format (Subscriber Management)

Syntax

```
nas-port-id-format { 
  agent-circuit-id; 
  agent-remote-id; 
  interface-description; 
  nas-identifier; 
} 
```

Hierarchy Level

```
[edit access profile profile-name radius options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Specify the information that the router includes in the NAS-Port-ID (RADIUS attribute 87) that it is passed to the RADIUS server during authentication and accounting. You can include any combination of the optional values.

Default

The router includes the interface description.

Options

- `agent-circuit-id`—Include the agent circuit ID from either DHCP option 82 or the DSL forum VSAs.
- `agent-remote-id`—Include the agent remote ID from either DHCP option 82 or the DSL forum VSAs.
- `interface-description`—Include the interface description.
- `nas-identifier`—Include the NAS identifier value (RADIUS attribute 32).

Required Privilege

- `admin`—To view this statement in the configuration.
- `admin-control`—To add this statement to the configuration.

Related Documentation

- Configuring RADIUS Server Options for Subscriber Access
- Configuring RADIUS Server Parameters for Subscriber Access
- Configuring a NAS-Port-ID with Additional Options
**nas-port-type (Subscriber Management)**

**Syntax**

```
    nas-port-type {
        ethernet {
            port-type;
        }
    }
```

**Hierarchy Level**

```
[edit access profile profile-name radius options]
```

**Release Information**

Statement introduced in Junos OS Release 11.4.  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Specify the port type used to authenticate subscribers. The router includes the port type in RADIUS attribute 61 (NAS-Port-Type attribute).

---

**NOTE:** This statement is ignored if the ethernet-port-type-virtual statement is included in the same access profile.

---

**Default**

The router uses a port type of `ethernet`.

**Options**

*port-type*—One of the following port types:

- `value`—A value from 0-65535
- `adsl-cap`—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- `adsl-dmt`—Asymmetric DSL, discrete multitone (DMT)
- `async`—Asynchronous
- `cable`—Cable
- `ethernet`—Ethernet
- `fddi`—Fiber Distributed Data Interface
- `g3-fax`—G.3 Fax
- `hdlc-clear-channel`—HDLC Clear Channel
- `iapp`—Inter-Access Point Protocol (IAPP)
- `idsl`—ISDN DSL
- `isdn-sync`—ISDN Synchronous
- `isdn-v110`—ISDN Async V.110
- `isdn-v120`—ISDN Async V.120
- `piafs`—Personal Handyphone System (PHS) Internet Access Forum Standard
- `sdsl`—Symmetric DSL
• sync—Synchronous
• token-ring—Token Ring
• virtual—Virtual
• wireless—Other wireless
• wireless-1x-ev—Wireless 1xEV
• wireless-cdma2000—Wireless code division multiple access (CDMA) 2000
• wireless-ieee80211—Wireless 802.11
• wireless-umts—Wireless universal mobile telecommunications system (UMTS)
• x25—X.25
• x75—X.75
• xdsl—DSL of unknown type

Required Privilege
Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

• Configuring RADIUS Server Options for Subscriber Access
• Configuring RADIUS Server Parameters for Subscriber Access
options (Access Profile)

Syntax

```plaintext
options {
    accounting-session-id-format (decimal | description);
    calling-station-id-delimiter delimiter-character;
    calling-station-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
    }
    client-accounting-algorithm (direct | round-robin);
    client-authentication-algorithm (direct | round-robin);
    coa-dynamic-variable-validation;
    ethernet-port-type-virtual;
    access-loop-id-local;
    interface-description-format {
        exclude-adapter;
        exclude-sub-interface;
    }
    ip-address-change-notify message;
    juniper-dsl-attributes;
    nas-identifier identifier-value;
    nas-port-extended-format {
        adapter-width width;
        ae-width width;
        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
        atm {
            adapter-width width;
            port-width width;
            slot-width width;
            vci-width width;
            vpi-width width;
        }
    }
    nas-port-id-delimiter delimiter-character;
    nas-port-id-format {
        agent-circuit-id;
        agent-remote-id;
        interface-description;
        nas-identifier;
    }
    nas-port-type {
        ethernet {
            port-type;
        }
    }
    revert-interval interval;
    vlan-nas-port-stacked-format;
}
```
Hierarchy Level  [edit access profile profile-name radius]

Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description  Configure the options used by RADIUS authentication and accounting servers.

The remaining statements are explained separately.

Required Privilege  Level  admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation  • Configuring RADIUS Server Options for Subscriber Access
• RADIUS Server Options for Subscriber Access

partition (Gx-Plus)

Syntax  partition partition-name {
  diameter-instance instance-name;
  destination-host hostname;
  destination-realm realm;
}

Hierarchy Level  [edit access gx-plus]

Release Information  Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  Configure a Gx-Plus partition.

Options  partition-name—Name of the Gx-Plus partition.

The remaining statements are explained separately.

Required Privilege  Level  admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation  • Configuring Gx-Plus
• Configuring the Gx-Plus Partition
port

Syntax    port port-number;

Hierarchy Level    [edit access radius-server server-address],
                   [edit access profile profile-name radius-server server-address]

Release Information    Statement introduced before Junos OS Release 7.4.
                       Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description    Configure the port number on which to contact the RADIUS server.

Options    port-number—Port number on which to contact the RADIUS server.
            Default: 1812 (as specified in RFC 2865)

Required Privilege Level    system—To view this statement in the configuration.
                             system-control—To add this statement to the configuration.

Related Documentation
  • Configuring Router or Switch Interaction with RADIUS Servers
  • Configuring Authentication and Accounting Parameters for Subscriber Access
provisioning-order

Syntax  
provisioning-order (gx-plus | jsr);

Hierarchy Level  
[edit access profile profile-name]

Release Information  
Support for Gx-Plus introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  
Configure AAA to use the specified application for subscriber service provisioning.

Options  
gx-plus—Specify Gx-Plus as the application used to communicate with a PCRF for subscriber service provisioning.

jsr—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.

Required Privilege  
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation  
- Configuring JSRC
- Provisioning Subscribers with JSRC
- Configuring Gx-Plus
- Provisioning Subscribers with Gx-Plus
radius (Access Profile)

Syntax

```
radius {
  accounting-server [ ip-address ];
  attributes {
    exclude
    ...
  }
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system-routing-instance;
    output-filter;
  }
}
authentication-server [ ip-address ];
options {
  accounting-session-id-format (decimal | description);
  calling-station-id-delimiter delimiter-character;
  calling-station-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    nas-identifier;
  }
  client-accounting-algorithm (direct | round-robin);
  client-authentication-algorithm (direct | round-robin);
  coa-dynamic-variable-validation;
  ethernet-port-type-virtual;
  interface-description-format {
    exclude-adapter;
    exclude-sub-interface;
  }
  ip-address-change-notify message;
  juniper-dsl-attributes;
  nas-identifier identifier-value;
  nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
    atm {
      adapter-width width;
      port-width width;
      slot-width width;
      vci-width width;
      vpi-width width;
    }
  }
  nas-port-id-delimiter delimiter-character;
  nas-port-id-format {
    agent-circuit-id;
  }
}
```
agent-remote-id;
interface-description;
nas-identifier;
}
nas-port-type {
  ethernet {
    port-type;
  }
}
revert-interval interval;
vlan-nas-port-stacked-format;
}

Hierarchy Level
[edit access profile profile-name]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

Required Privilege
Level
admin—to view this statement in the configuration.
admin-control—to add this statement to the configuration.

Related Documentation
• Configuring RADIUS Server Parameters for Subscriber Access
• RADIUS Server Options for Subscriber Access
retry

Syntax retry attempts;

Hierarchy Level [edit access radius-server server-address],
[edit access profile profile-name radius-server server-address]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the number of times that the router or switch is allowed to attempt to contact a RADIUS authentication or accounting server.

Options attempts—Number of times that the router is allowed to attempt to contact a RADIUS server.

Range: 1 through 10

Default: 3

Required Privilege Level system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

• Configuring Authentication and Accounting Parameters for Subscriber Access
• Configuring Router or Switch Interaction with RADIUS Servers
• Example: Configuring CHAP Authentication with RADIUS
• Configuring RADIUS Authentication for L2TP
• timeout on page 1808
revert-interval

**Syntax**
```
revert-interval interval;
```

**Hierarchy Level**
```
[edit access profile profile-name radius options],
[edit access radius-options]
```

**Release Information**
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description**
Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified interval expires. If the server is then reachable, it is used in accordance with the order of the server list.

**Options**
- `interval`—Amount of time to wait.
  - **Range:** 0 through 604800 seconds
  - **Default:** 60 seconds

**Required Privilege Level**
- `admin`—To view this statement in the configuration.
- `admin-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring RADIUS Server Options for Subscriber Access
- Configuring Authentication and Accounting Parameters for Subscriber Access

routing-instance

**Syntax**
```
routing-instance routing-instance-name:
```

**Hierarchy Level**
```
[edit access radius-server server-address],
[edit access profile profile-name radius-server server-address]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the routing instance used to send RADIUS packets to the RADIUS server.

**Options**
- `routing-instance-name`—Routing instance name.

**Required Privilege Level**
- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring the PPP Authentication Protocol
- Configuring Authentication and Accounting Parameters for Subscriber Access
secret

**Syntax**
```
secret password;
```

**Hierarchy Level**
- [edit access profile profile-name radius-server server-address]
- [edit access radius-disconnect client-address]
- [edit access radius-server server-address]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.

**Options**
- **password**—Password to use; it can include spaces if the character string is enclosed in quotation marks.

**Required Privilege**
- **Level**
  - system—To view this statement in the configuration.
  - system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Configuring Router or Switch Interaction with RADIUS Servers
- Example: Configuring CHAP Authentication with RADIUS
- Configuring RADIUS Authentication for L2TP
- Configuring the RADIUS Disconnect Server for L2TP
- Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)

send-acct-status-on-config-change (Access Profile)

**Syntax**
```
send-acct-status-on-config-change;
```

**Hierarchy Level**
```
[edit access profile profile-name accounting]
```

**Release Information**
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**
Configure the router's authd process to send an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is removed from an access profile.

**Required Privilege**
- **Level**
  - admin—To view this statement in the configuration.
  - admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring RADIUS Server Parameters for Subscriber Access
- Configuring Per-Subscriber Session Accounting
service (Service Accounting)

Syntax

```
service {
    accounting-order (activation-protocol | radius);
}
```

Hierarchy Level

```
[edit access profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Define the subscriber service accounting configuration.

The remaining statement is explained separately.

Required Privilege

Level

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Service Accounting with JSRC
- Service Accounting with JSRC

source-address

Syntax

```
source-address source-address;
```

Hierarchy Level

```
[edit access radius-server server-address],
[edit access profile profile-name radius-server server-address]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.

Options

```
source-address—Valid IPv4 address configured on one of the router or switch interfaces.
```

On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.

Required Privilege

Level

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers
- Configuring Authentication and Accounting Parameters for Subscriber Access
- Example: Configuring CHAP Authentication with RADIUS
- Configuring RADIUS Authentication for L2TP
timeout (RADIUS)

Syntax

timeout seconds;

Hierarchy Level

[edit access radius-server server-address],
[edit access profile profile-name radius-server server-address]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure the amount of time that the local router or switch waits to receive a response from a RADIUS server.

Options

seconds—Amount of time to wait.
Range: 1 through 90 seconds
Default: 3 seconds

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

• Configuring Router or Switch Interaction with RADIUS Servers
• Configuring Authentication and Accounting Parameters for Subscriber Access
• Example: Configuring CHAP Authentication with RADIUS
• Configuring RADIUS Authentication for L2TP
vlan-assignment

Syntax
vlan-assignment (vlan-id | vlan-name);

Hierarchy Level
[edit protocols dot1x authenticator authentication-profile-name static (Protocols 802.1X) mac-address],
[edit ethernet-switching-options authentication-whitelist],
[edit switch-options on page 2027 authentication-whitelist]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure the VLAN that is associated with the list of MAC addresses that are excluded from RADIUS authentication.

Options
vlan-id | vlan-name—The name of the VLAN or the VLAN tag identifier to associate with the device. The VLAN already exists on the switch.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• show dot1x static-mac-address on page 1835
• Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch on page 1704
• Example: Setting Up Captive Portal Authentication on an EX Series Switch
• Understanding Authentication on EX Series Switches on page 1658
• Example: Setting Up Captive Portal Authentication on an EX Series Switch
• Configuring Captive Portal Authentication (CLI Procedure)
vlan-nas-port-stacked-format

Syntax
vlan-nas-port-stacked-format;

Hierarchy Level
[edit access profile profile-name radius options]

Release Information
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

Required Privilege Level
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation
• Configuring RADIUS Server Options for Subscriber Access
• Configuring Authentication and Accounting Parameters for Subscriber Access

voip

Syntax
voip { interface (all | [interface-name | access-ports]) { vlan vlan-name ; forwarding-class <assured-forwarding | best-effort | expedited-forwarding | network-control> ; } }

Hierarchy Level
[edit ethernet-switching-options],
[edit switch-options on page 2027]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure voice over IP (VoIP) interfaces.
The remaining statements are explained separately.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• Example: Setting Up VoIP with 802.1X and LLDP-MED on an EX Series Switch
• Example: Configuring VoIP on an EX Series Switch Without Including 802.1X Authentication
• Example: Configuring VoIP on an EX Series Switch Without Including LLDP-MED Support
### wait-for-acct-on-ack (Access Profile)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>wait-for-acct-on-ack;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit access profile profile-name accounting]</td>
</tr>
</tbody>
</table>
| Release Information | Statement introduced in Junos OS Release 12.3.  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches. |
| Description | Configure the router’s authd process to wait for an Acct-On-Ack response message from RADIUS before sending new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information. |
| Required Privilege Level | admin—To view this statement in the configuration.  
admin-control—To add this statement to the configuration. |
| Related Documentation | • Configuring RADIUS Server Parameters for Subscriber Access  
• Configuring Per-Subscriber Session Accounting |
CHAPTER 30

Administration

- Routine Monitoring on page 1813
- Operational Commands on page 1815

Routine Monitoring

- Monitoring 802.1X Authentication on page 1813
- Verifying 802.1X Authentication on page 1814

Monitoring 802.1X Authentication

**Purpose**

Use the monitoring feature to display details of authenticated users and users who have failed authentication.

**Action**

To display authentication details in the J-Web interface, select Monitoring > Security > 802.1X.

To display authentication details in the CLI, enter the following commands:

- `show dot1x interface detail | display xml`
- `show dot1x interface detail <interface> | display xml`
- `show dot1x auth-failed-users`

**Meaning**

The details displayed include:

- A list of authenticated users.
- The total number of users connected.
- A list of users who have failed authentication

You can also specify an interface for which the details must be displayed.

**Related Documentation**

- *Configuring 802.1X Authentication (J-Web Procedure)*
- *Configuring 802.1X Interface Settings (CLI Procedure)* on page 1740
- *Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch* on page 1684
Verifying 802.1X Authentication

**Purpose** Verify that supplicants are being authenticated on an interface on an EX Series switch with the interface configured for 802.1X authentication, and display the method of authentication being used.

**Action** Display detailed information about an interface configured for 802.1X (here, the interface is `ge-0/0/16`):

```bash
user@switch> show dot1x interface ge-0/0/16.detail
ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Strict: Disabled
  Reauthentication: Enabled Reauthentication interval: 40 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 1
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user5, 00:30:48:8C:66:BD
    Operational state: Authenticated
    Authentication method: Radius
    Authenticated VLAN: v200
    Reauthentication due in 17 seconds
```

**Meaning** The sample output from the `show dot1x interface detail` command shows that the **Number of connected supplicants** is 1. The supplicant that was authenticated and is now connected to the LAN is known as **user5** on the RADIUS server and has the MAC address **00:30:48:8C:66:BD**. The supplicant was authenticated by means of the 802.1X authentication method called **Radius** authentication. When the **Radius** authentication method is used, the supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected. The sample output also shows that the supplicant is connected to VLAN v200.

Other 802.1X authentication methods supported on EX Series switches in addition to the RADIUS method are:

- **Guest VLAN**—A nonresponsive host is granted Guest-VLAN access.
- **MAC Radius**—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.
- **Server-fail deny**—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default.
• **Server-fail permit**—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.

• **Server-fail use-cache**—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are granted access, but new supplicants are denied LAN access.

• **Server-fail VLAN**—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)

**Related Documentation**

- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- *Configuring 802.1X Authentication (J-Web Procedure)*
- Configuring MAC RADIUS Authentication (CLI Procedure) on page 1754
- Configuring Server Fail Fallback (CLI Procedure) on page 1752

**Operational Commands**
clear captive-portal

Syntax: clear captive-portal (firewall [interface-names] | interface (802.1X) (all | [interface-names]) | mac-address [mac-addresses])

Release Information: Command introduced in Junos OS Release 10.1 for EX Series switches.

Description: Reset the authentication state of a captive portal interface or captive-portal firewall statistics on one or more interfaces.

Options:
- **firewall [interface-names]** — Resets captive portal statistics on all interfaces or on the specified interface.
- **interface (all | interface-names)** — Resets the authentication state of users connected to all interfaces or the specified interfaces.
- **mac-address mac-addresses** — Resets the authentication state for the specified MAC addresses.

Required Privilege: view

Related Documentation:
- show captive-portal authentication-failed-users on page 1822
- show captive-portal interface on page 1825
- show captive-portal firewall on page 1823
- Example: Setting Up Captive Portal Authentication on an EX Series Switch
- Configuring Captive Portal Authentication (CLI Procedure)

List of Sample Output:
- clear captive-portal interface on page 1817
- clear captive-portal interface on page 1817
- clear captive-portal mac-address on page 1817
- clear captive-portal firewall on page 1817

Output Fields:
Table 211 on page 1816 lists the output fields for the clear captive-portal interface command. (The clear captive-portal firewall and clear captive-portal mac-address commands have no output). Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which captive portal has been configured.</td>
</tr>
</tbody>
</table>
Table 211: clear captive-portal interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The state of the port:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Authenticated</strong>—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Authenticating</strong>—The client is authenticating through the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Connecting</strong>—Switch is attempting to contact the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Initialize</strong>—The interface link is down.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Held</strong>—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the connected client on the interface.</td>
</tr>
<tr>
<td>User</td>
<td>Users connected to the captive portal interface.</td>
</tr>
</tbody>
</table>
clear dot1x

Syntax

```
clear dot1x (firewall <counter-name> | interface <[interface-name]> | mac-address [mac-addresses] | statistics <interface interface-name>)
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches. firewall option added in Junos OS Release 9.5 for EX Series switches.

Description

Reset the authentication state of an interface or delete 802.1X statistics from the switch. When you reset an interface using the interface or mac-address options, reauthentication on the interface is also triggered. The switch sends out a multicast message on the interface to restart the authentication of all connected supplicants. If a MAC address is reset, then the switch sends out a unicast message to that specific MAC address to restart authentication.

If a supplicant is sending traffic when the clear dot1x interface command is issued, the authenticator immediately initiates reauthentication. This process happens quickly, and it might seem that reauthentication did not occur. To verify that reauthentication has happened, issue the show dot1x interface detail command. The values for Reauthentication due and Reauthentication interval will be about the same.

**CAUTION:** When you clear the learned MAC addresses from an interface using the clear dot1x interface command, all MAC addresses are cleared, including those in static MAC bypass list.

Options

```
firewall <counter-name>—Clear 802.1X firewall counter statistics. If the counter-name option is specified, clear 802.1X firewall statistics for that counter.

interface <[interface-name]>—Reset the authentication state of all the supplicants (also, clears all the authentication bypassed clients) connected to the specified interface (when the interface is an authenticator) or reset the authentication state for the interface itself (when the interface is a supplicant).

mac-address [mac-addresses]—Reset the authentication state of the specified MAC addresses.

statistics <interface interface-name>—Clear 802.1X statistics on all 802.1X-enabled interfaces. If the interface option is specified, clear 802.1X firewall statistics for that interface or interfaces.
```

Required Privilege Level

view

Related Documentation

- show dot1x on page 1828
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
• Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742

List of Sample Output  
clear dot1x firewall c1 on page 1819  
clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0 on page 1819  
clear dot1x mac-address 00:04:ae:cd:23:5f on page 1819  
clear dot1x statistics interface ge-1/0/1 on page 1819

Sample Output  
clear dot1x firewall c1

user@switch>  clear dot1x firewall c1  
clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0  
user@switch>  clear dot1x interface ge-1/0/0 ge-2/0/0 ge-2/0/0 ge5/0/0  
clear dot1x mac-address 00:04:ae:cd:23:5f  
user@switch>  clear dot1x mac-address 00:04:ae:cd:23:5f  
clear dot1x statistics interface ge-1/0/1  
user@switch>  clear dot1x statistics interface ge-1/0/1
clear lldp neighbors

**Syntax**
```
clear lldp neighbors
<interface interface>
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Clear the learned remote neighbor information on all or selected interfaces.

**Options**
- `none`—Clear the remote neighbor information on all interfaces.
- `interface interface`—(Optional) Clear the remote neighbor information from one or more selected interfaces.

**Required Privilege Level**
view

**Related Documentation**
- show lldp on page 1837
- Configuring LLDP (CLI Procedure) on page 1745
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665

**List of Sample Output**
clear lldp neighbors on page 1820
clear lldp neighbors interface ge-0/1/1.0 on page 1820

**Sample Output**
clear lldp neighbors
```
user@switch> clear lldp neighbors
```
clear lldp neighbors interface ge-0/1/1.0
```
user@switch> clear lldp neighbors interface ge-0/1/1.0
```
clear lldp statistics

Syntax

```
clear lldp statistics
<interface interface>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Clear LLDP statistics on one or more interfaces.

Options

- **none**—Clears LLDP statistics on all interfaces.
- **interface interface-names**—(Optional) Clear LLDP statistics on one or more interfaces.

Required Privilege

- **view**

Related Documentation

- Configuring LLDP (CLI Procedure) on page 1745
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665

List of Sample Output

- clear lldp statistics on page 1821
- clear lldp statistics interface ge-0/1/1.0 on page 1821

Sample Output

clear lldp statistics

```
user@switch> clear lldp statistics
```

clear lldp statistics interface ge-0/1/1.0

```
user@switch> clear lldp statistics interface ge-0/1/1.0
```
show captive-portal authentication-failed-users

Syntax  
show captive-portal authentication-failed-users

Release Information  
Command introduced in Junos OS Release 10.1 for EX Series switches.

Description  
Display the users that have failed captive portal authentication.

Required Privilege  
Level view

Related Documentation  
- show captive-portal interface on page 1825
- show captive-portal firewall on page 1823
- clear captive-portal on page 1816
- Example: Setting Up Captive Portal Authentication on an EX Series Switch
- Configuring Captive Portal Authentication (CLI Procedure)

List of Sample Output  
show captive-portal authentication-failed-users on page 1822

Output Fields  
Table 212 on page 1822 lists the output fields for the show captive-portal authentication-failed-users command. Output fields are listed in the approximate order in which they appear.

Table 212: show captive-portal authentication-failed-users Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The MAC address configured to bypass captive portal authentication.</td>
<td>all</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address configured statically on the interface.</td>
<td>all</td>
</tr>
<tr>
<td>User</td>
<td>Name of the user that has failed captive portal authentication.</td>
<td>all</td>
</tr>
<tr>
<td>Failure Count</td>
<td>The number of times that 802.1X authentication has failed on the interface.</td>
<td>all</td>
</tr>
</tbody>
</table>

Sample Output

show captive-portal authentication-failed-users

user@switch> show captive-portal authentication-failed-users

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC address</th>
<th>User</th>
<th>Failure Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/17.0</td>
<td>00:37:00:00:00:00</td>
<td>003700000000</td>
<td>28</td>
</tr>
<tr>
<td>ge-0/0/20.0</td>
<td>00:04:10:00:00:00</td>
<td>000410000000</td>
<td>32</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
<td>00:00:03:00:0a:00</td>
<td>000003000a00</td>
<td>4</td>
</tr>
<tr>
<td>ge-0/0/19.0</td>
<td>00:00:03:00:0b:00</td>
<td>000003000b00</td>
<td>18</td>
</tr>
</tbody>
</table>
show captive-portal firewall

Syntax

```
show captive-portal firewall
   <brief | detail>
   <interface-name>
   <interface-name> detail
```

Release Information

Command introduced in Junos OS Release 10.1 for EX Series switches.

Description

Display information about the firewall filters for each user that is authenticated on each captive portal interface.

Options

- **none**—Display all the firewall filters on all captive portal interfaces.
- **brief | detail**—(Optional) Display the specified level of output.
- **interface-name**—(Optional) Display all the terms of the firewall filters for the specified interface.
- **interface-name detail**—(Optional) Display all of the terms of the firewall filters for the specified interface.

Required Privilege

- **view**

Related Documentation

- show captive-portal authentication-failed-users on page 1822
- show captive-portal interface on page 1825
- clear captive-portal on page 1816
- Example: Setting Up Captive Portal Authentication on an EX Series Switch
- Configuring Captive Portal Authentication (CLI Procedure)

List of Sample Output

- show captive-portal firewall brief on page 1823
- show captive-portal firewall ge-0/0/10.0 on page 1824
- show captive-portal firewall on page 1824

Output Fields

Output fields for the `show captive-portal firewall` command include any action modifier specified in firewall filters except policers. Policers are not supported in the terms of the internally generated dynamic firewall filters that are created when multiple supplicants authenticate on 802.1X-enabled interfaces.

Sample Output

```
user@switch> show captive-portal firewall brief
Captive Portal Information:
Interface   State      MAC address     User
```

Copyright © 2013, Juniper Networks, Inc.
show captive-portalfirewall ge-0/0/10.0

user@switch> show captive-portalfirewall ge-0/0/10.0
Filter name: dot1x_ge-0/0/10
Counters:
<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_ge-0/0/10_CP_arp</td>
<td>7616</td>
<td>119</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_dhcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_http</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_https</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_t_dns</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_u_dns</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show captive-portalfirewall

user@switch> show captive-portalfirewall
Filter name: dot1x_ge-0/0/0
Counters:
<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_ge-0/0/0_CP_arp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_dhcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_http</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_https</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_t_dns</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/0_CP_u_dns</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Filter name: dot1x_ge-0/0/1
Counters:
<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_ge-0/0/1_CP_arp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_dhcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_http</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_https</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_t_dns</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/1_CP_u_dns</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Filter name: dot1x_ge-0/0/10
Counters:
<table>
<thead>
<tr>
<th>Name</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x_ge-0/0/10_CP_arp</td>
<td>7616</td>
<td>119</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_dhcp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_http</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_https</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_t_dns</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dot1x_ge-0/0/10_CP_u_dns</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Filter name: dot1x_ge-0/0/11
**show captive-portal interface**

**Syntax**

```
show captive-portal interface
  <interface-name>
detail
```

**Release Information**
Command introduced in Junos OS Release 10.1 for EX Series switches.

**Description**
Display the current operational state of all captive portal interfaces with the list of connected users and the configured values of captive portal attributes on the interfaces.

**Options**
- `none`—Display all captive portal interfaces.
- `interface-name`—(Optional) Display the state for the specified captive portal interface and lists the MAC address and user names of any clients authenticated on the interface.
- `interface-name detail`—(Optional) Displays the configured values of captive portal attributes on the specified captive portal interface.

**Required Privilege Level**
view

**Related Documentation**
- `show captive-portal authentication-failed-users on page 1822`
- `show captive-portal firewall on page 1823`
- `captive-portal`
- `clear captive-portal on page 1816`
- *Example: Setting Up Captive Portal Authentication on an EX Series Switch*
- *Configuring Captive Portal Authentication (CLI Procedure)*

**List of Sample Output**
- `show captive-portal interface (Only captive portal is enabled) on page 1827`
- `show captive-portal interface (Both 802.1X authentication and captive portal are enabled) on page 1827`
- `show captive-portal interface detail (Only captive portal is enabled) on page 1827`
- `show captive-portal interface detail (Both 802.1X authentication and captive portal are enabled) on page 1827`

**Output Fields**
Table 213 on page 1825 lists the output fields for the `show captive-portal interface` command. Output fields are listed in the approximate order in which they appear.

**Table 213: show captive-portal interface Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which captive portal has been configured.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 213: show captive-portal interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>The state of the interface:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authenticated</strong>—The client has been authenticated through the RADIUS server or has been permitted access through server fail fallback.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Authenticating</strong>—The client is authenticating through the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Connecting</strong>—Switch is attempting to contact the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Initialize</strong>—The interface link is down.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Held</strong>—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.</td>
<td></td>
</tr>
<tr>
<td><strong>MAC address</strong></td>
<td>The MAC address of the connected client on the interface.</td>
<td>brief</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>Users connected to the captive portal interface.</td>
<td>brief</td>
</tr>
<tr>
<td><strong>Fallen back</strong></td>
<td>Indicates when 802.1X authentication and captive portal are both enabled on an interface:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If 802.1X authentication and captive portal are both enabled, <strong>CP fallen back</strong> status is <strong>Yes</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If 802.1X authentication and captive portal are not both enabled, <strong>CP fallen back</strong> status is <strong>No</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Supplicant mode</strong></td>
<td>Mode used to authenticate clients—multiple, single, or single-suppliant.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Number of retries</strong></td>
<td>Number of times the user can attempt to submit authentication information.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Quiet period</strong></td>
<td>Time, in seconds, after a user exceeds the maximum number of retries before they can attempt to authenticate.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Configured CP session timeout</strong></td>
<td>Time, in seconds, that a client can be idle before the session expires.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server timeout</strong></td>
<td>Time, in seconds, that an interface will wait for a reply when relaying a response from the client to the authentication server before timing out and invoking the server-fail action.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Number of connected supplicants</strong></td>
<td>Number of users connecting through the captive portal interface. Information for each user includes:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>Supplicant</strong>—User name and MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Operational state</strong>—See State (above).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Dynamic CP session timeout</strong>—Timeout value dynamically downloaded from the RADIUS server for this user, if any.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CP Session expiration due in</strong>—Time remaining in session.</td>
<td></td>
</tr>
</tbody>
</table>
Sample Output

show captive-portal interface (Only captive portal is enabled)

```
show captive-portal interface
Captive Portal Information:
Interface      State           MAC address          User          Fallen back
ge-0/0/1.0     Connecting      00:30:48:8c:66:bd    No User
ge-0/0/10.0    Connecting      00:30:48:8c:66:bd    No User
ge-0/0/5.0     Authenticated   00:30:48:8d:7a:9b    abcdeX      No
```

show captive-portal interface (Both 802.1X authentication and captive portal are enabled)

```
show captive-portal interface
Captive Portal Information:
Interface      State           MAC address          User          Fallen back
ge-0/0/1.0     Connecting      00:30:48:8c:66:bd    No User
ge-0/0/10.0    Connecting      00:30:48:8c:66:bd    No User
ge-0/0/5.0     Authenticated   00:30:48:8d:7a:9b    abcdeX      Yes
```

show captive-portal interface detail (Only captive portal is enabled)

```
show captive-portal interface detail ge-6/0/5.0
Supplicant mode: Multiple
Number of retries: 3
Quiet period: 60 seconds
Configured CP session timeout: 3600 seconds
Server timeout: 15 seconds
CP fallen back: No
Number of connected supplicants: 1
  Supplicant: abcdeX, 00:30:48:8d:7a:9b
    Operational state: Authenticated
    Dynamic CP Session Timeout: 3600 seconds
    CP Session Expiration due in: 3583 seconds
```

show captive-portal interface detail (Both 802.1X authentication and captive portal are enabled)

```
show captive-portal interface detail ge-6/0/5.0
Supplicant mode: Multiple
Number of retries: 3
Quiet period: 60 seconds
Configured CP session timeout: 3600 seconds
Server timeout: 15 seconds
CP fallen back: Yes
Number of connected supplicants: 1
  Supplicant: abcdeX, 00:30:48:8d:7a:9b
    Operational state: Authenticated
    Dynamic CP Session Timeout: 3600 seconds
    CP Session Expiration due in: 3583 seconds
```
show dot1x

Syntax

```
show dot1x
  <brief | detail>
  <interface interface-name>
```

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display the current operational state of all ports with the list of connected users. This command displays the list of connected supplicants received from the RADIUS authentication server regardless of the session state—that is, for both authenticated supplicants and for supplicants that attempted authentication.

Options

```
none—Display information for all authenticator ports.
brief | detail—(Optional) Display the specified level of output.
interface interface-name—Display information for the specified port with a list of connected supplicants.
```

Required Privilege
Level
view

Related Documentation

- clear dot1x on page 1818
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch on page 1684
- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch on page 1707
- Example: Configuring Fallback Options on EX Series Switches for EAP-TTLS Authentication and Odyssey Access Clients on page 1735
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742
- Verifying 802.1X Authentication on page 1814

List of Sample Output
- show dot1x interface brief on page 1831
- show dot1x interface detail on page 1831

Output Fields
Table 214 on page 1828 lists the output fields for the `show dot1x` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of a port.</td>
<td>All levels</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the connected supplicant on the port.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 214: show dot1x Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Role</strong></td>
<td>The 802.1X authentication role of the interface. When 802.1X is enabled on an interface, the role is <strong>Authenticator</strong>. As <strong>Authenticator</strong>, the interface blocks LAN access until a supplicant is authenticated through 802.1X or MAC RADIUS authentication.</td>
<td>brief, detail</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The state of the port:</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authenticated</strong>—The supplicant has been authenticated through the RADIUS server or has been permitted access through server fail fallback.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Authenticating</strong>—The supplicant is authenticating through the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Held</strong>—An action has been triggered through server fail fallback during a RADIUS server timeout. A supplicant is denied access, permitted access through a specified VLAN, or maintains the authenticated state granted to it before the RADIUS server timeout occurred.</td>
<td></td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>The user name of the connected supplicant</td>
<td>brief</td>
</tr>
<tr>
<td><strong>Administrative state</strong></td>
<td>The administrative state of the port:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>auto</strong>—Traffic is allowed through the port based on the authentication result. (Default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>force-authorize</strong>—All traffic flows through the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to <strong>dynamic</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>force-unauthorize</strong>—All traffic drops on the port irrespective of the authentication result. This state is not allowed on an interface whose VLAN membership has been set to <strong>dynamic</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Supplicant</strong></td>
<td>The mode for the supplicant:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>single</strong>—Authenticates only the first supplicant. All other supplicants who connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>single-secure</strong>—Allows only one supplicant to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>multiple</strong>—Allows multiple supplicants to connect to the port. Each supplicant is authenticated individually.</td>
<td></td>
</tr>
<tr>
<td><strong>Quiet period</strong></td>
<td>The number of seconds the port remains in the wait state following a failed authentication exchange with the supplicant before reattempting the authentication. The default value is 60 seconds. The range is 0 through 65,535 seconds.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Transmit period</strong></td>
<td>The number of seconds the port waits before retransmitting the initial EAPOL PDUs to the supplicant. The default value is 30 seconds. The range is 1 through 65,535 seconds.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 214: show dot1x Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC radius</strong></td>
<td>MAC RADIUS authentication:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• enabled—The switch sends an EAPOL request to the connecting host to attempt 802.1X authentication and if the connecting host is unresponsive, the switch tries to authenticate using the MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• disabled—The default. The switch will not attempt to authenticate the MAC address of the connecting host.</td>
<td></td>
</tr>
<tr>
<td><strong>MAC radius restrict</strong></td>
<td>The authentication method is restricted to MAC RADIUS only. 802.1X authentication is not enabled.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Reauthentication</strong></td>
<td>The reauthentication state:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• disable—Periodic reauthentication of the client is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• interval—Sets the periodic reauthentication time interval. The default value is 3600 seconds. The range is 1 through 65,535 seconds.</td>
<td></td>
</tr>
<tr>
<td><strong>Supplicant timeout</strong></td>
<td>The number of seconds the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request. The default value is 30 seconds. The range is 1 through 60 seconds.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Server timeout</strong></td>
<td>The number of seconds the port waits for a reply when relaying a response from the supplicant to the authentication server before timing out. The default value is 30 seconds. The range is 1 through 60 seconds.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Maximum EAPOL requests</strong></td>
<td>The maximum number of retransmission times of an EAPOL request packet to the supplicant before the authentication session times out. The default value is 2. The range is 1 through 10.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Number of clients bypassed because of authentication</strong></td>
<td>The number of non-802.1X clients granted access to the LAN by means of static MAC bypass. The following fields are displayed:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Client—MAC address of the client.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vlan—The name of the VLAN to which the client is connected.</td>
<td></td>
</tr>
<tr>
<td><strong>Guest VLAN member</strong></td>
<td>The VLAN to which a supplicant is connected when the supplicant is authenticated using a guest VLAN. If a guest VLAN is not configured on the interface, this field displays &lt;not configured&gt;.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Number of connected supplicants</strong></td>
<td>The number of supplicants connected to a port.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Supplicant</strong></td>
<td>The user name and MAC address of the connected supplicant.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 214: show dot1x Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication method</td>
<td>The 802.1X authentication method used for a supplicant:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>Guest VLAN</strong>—A supplicant is connected to the LAN through the guest VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC Radius</strong>—A nonresponsive host is authenticated based on its MAC address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Radius</strong>—A supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Server-fail deny</strong>—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Server-fail permit</strong>—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Server-fail use-cache</strong>—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are reauthenticated, but new supplicants are denied LAN access.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Server-fail VLAN</strong>—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)</td>
<td></td>
</tr>
<tr>
<td>Authenticated VLAN</td>
<td>The VLAN to which the supplicant is connected.</td>
<td>detail</td>
</tr>
<tr>
<td>Dynamic filter</td>
<td>User policy filter sent by the RADIUS server.</td>
<td>detail</td>
</tr>
<tr>
<td>Session Reauth interval</td>
<td>The configured reauthentication interval.</td>
<td>detail</td>
</tr>
<tr>
<td>Reauthentication due in</td>
<td>The number of seconds in which reauthentication will occur again for the connected supplicant.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

```
show dot1x interface brief

user@switch> show dot1x interface brief
802.1X Information:
Interface          Role      State       MAC address          User
ge-0/0/1           Authenticator Authenticated 00:a0:d2:18:1a:c8  user1
ge-0/0/2           Authenticator Connecting 00:a6:55:f2:94:ae  user3

show dot1x interface detail

user@switch> show dot1x interface ge-0/0/16.0 detail

ge-0/0/16.0
Role: Authenticator
Administrative state: Auto
```
Supplicant mode: Single
Number of retries: 3
Quiet period: 60 seconds
Transmit period: 30 seconds
Mac Radius: Enabled
Mac Radius Strict: Disabled
Reauthentication: Enabled
Configured Reauthentication interval: 40 seconds
Supplicant timeout: 30 seconds
Server timeout: 30 seconds
Maximum EAPOL requests: 1
Guest VLAN member: <not configured>
Number of connected supplicants: 1
  Supplicant: abc, 00:30:48:BC:66:BD
    Operational state: Authenticated
    Authentication method: Radius
    Authenticated VLAN: v200
  Reauthentication due in 17 seconds
show dot1x authentication-failed-users

**Syntax**
show dot1x authentication-failed-users

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Displays supplicants (users) that have failed 802.1X authentication.

**Required Privilege Level**
view

**Related Documentation**
- clear dot1x on page 1818
- Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch on page 1704
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740

**List of Sample Output**
show dot1x authentication-failed-users on page 1833

**Output Fields**
Table 215 on page 1833 lists the output fields for the `show dot1x authentication-failed-users` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The MAC address configured to bypass 802.1X authentication.</td>
<td>all</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address configured statically on the interface.</td>
<td>all</td>
</tr>
<tr>
<td>User</td>
<td>The user that is configured on the RADIUS server and that has failed 802.1X authentication.</td>
<td>all</td>
</tr>
<tr>
<td>Failure Count</td>
<td>The number of times that 802.1X authentication has failed on the interface.</td>
<td>all</td>
</tr>
</tbody>
</table>

**Sample Output**

```
user@switch> show dot1x authentication-failed-users

Interface     MAC address          User            Failure Count
ge-0/0/17.0   00:37:00:00:00:00    003700000000        28
ge-0/0/20.0   00:04:10:00:00:00    000410000000        32
ge-0/0/18.0   00:00:03:00:0a:00    000003000a00        4
ge-0/0/19.0   00:00:03:00:0b:00    000003000b00        18
```

Copyright © 2013, Juniper Networks, Inc.
show dot1x firewall

Syntax
show dot1x firewall <interface interface-name>

Release Information
Command introduced in Junos OS Release 9.5 for EX Series switches.

Description
Displays information about the firewall filters for each user or nonresponsive host that is authenticated on each 802.1X-enabled interface that is configured for multiple supplicants. For example, if the firewall filter is configured with a term for counters, the command shows the count for each user.

Options
interface interface-names—(Optional) Display information for the specified interface.

Required Privilege
view

Related Documentation
- clear dot1x on page 1818
- Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 4186

List of Sample Output
show dot1x firewall on page 1834
show dot1x firewall on page 1834

Output Fields
Output fields include any action modifier that is specified in firewall filters.

Sample Output
show dot1x firewall

(Showing counter action)

user@switch> show dot1x firewall
Filter: dot1x-filter-ge-0/0/3
Counters
counter1_dot1x_ge-0/0/3_user1 342
counter1_dot1x_ge-0/0/3_user2 857

show dot1x firewall

(Showing policer action)

user@switch> show dot1x firewall
Filter: dot1x_ge-0/0/0
Counters
pl-t1 494946
show dot1x static-mac-address

Syntax  
show dot1x static-mac-address <(interface [interface-name])>

Release Information  
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Displays all the static MAC addresses that are configured to bypass 802.1X authentication on the switch.

Options  
interface [interface-name]—(Optional) Display static MAC addresses for a specific interface.

Required Privilege  
view

Related Documentation  
- clear dot1x on page 1818
- Example: Configuring Static MAC Bypass of Authentication on an EX Series Switch on page 1704
- Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure) on page 2131
- Configuring 802.1X Interface Settings (CLI Procedure) on page 1740
- Understanding Authentication on EX Series Switches on page 1658

List of Sample Output  
show dot1x static-mac-address on page 1835
show dot1x static-mac-address interface ge-0/0/0.1 on page 1836

Output Fields  
Table 216 on page 1835 lists the output fields for the show dot1x static-mac-address command. Output fields are listed in the approximate order in which they appear.

Table 216: show dot1x static-mac-address Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
<td>The MAC address of the device that is configured to bypass 802.1X authentication.</td>
<td>all</td>
</tr>
<tr>
<td>VLAN-Assignment</td>
<td>The name of the VLAN to which the device is assigned.</td>
<td>all</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the interface on which authentication is bypassed for a given MAC address.</td>
<td>all</td>
</tr>
</tbody>
</table>

Sample Output

show dot1x static-mac-address

user@switch> show dot1x static-mac-address

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN-Assignment</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:11:22:33</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show dot1x static-mac-address interface ge-0/0/0.1

```
user@switch> show dot1x static-mac-address interface ge-0/0/0.1

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN-Assignment</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:12:24:12</td>
<td>support</td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td>00:00:00:72:30:58</td>
<td>support</td>
<td>ge-0/0/1.0</td>
</tr>
</tbody>
</table>
```
# show lldp

**Syntax**

```plaintext
show lldp <detail>
```

**Release Information**


**Description**

Display information about Link Layer Discovery Protocol (LLDP) and Link Level Discovery Protocol–Media Endpoint Discovery (LLDP-MED) configuration and capabilities on the switch. LLDP and LLDP-MED are used to learn about and to distribute device information on network links.

**NOTE:** LLDP-MED is not available on the QFX Series.

**Options**

- `none`—Display LLDP information for all interfaces.
- `detail`—(Optional) Display detailed LLDP information for all interfaces.

**NOTE:** fast-start is not available on the QFX Series.

**Required Privilege Level**

`view`

**Related Documentation**

- Configuring LLDP (CLI Procedure) on page 1745
- Configuring LLDP-MED (CLI Procedure) on page 1748
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665
- Configuring LLDP
- Understanding LLDP

**List of Sample Output**

- `show lldp` on page 1840
- `show lldp detail` on page 1840

**Output Fields**

Table 217 on page 1838 lists the output fields for the `show lldp` command. Output fields are listed in the approximate order in which they appear.
Table 217: show lldp Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP</td>
<td>LLDP operating state. The state can be enabled or disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>NOTE</strong>:</td>
<td>If a VLAN that has been configured for untagged packets on an interface also has Layer 2 protocol tunneling (L2PT) enabled for LLDP, the LLDP operating state for that interface is displayed as disabled.</td>
<td></td>
</tr>
<tr>
<td>Advertisement interval</td>
<td>Frequency, in seconds, at which LLDP advertisements are sent.</td>
<td>All levels</td>
</tr>
<tr>
<td>This value is set by the advertisement-interval configuration statement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmit delay</td>
<td>Seconds of delay before advertisements are sent to neighbors following a change to a TLV (type, length, or value) element in the LLDP protocol or to the state of the local system, such as a change in hostname or management address. You can set this value to reduce the delay in notifying neighbors of a change in the local system.</td>
<td></td>
</tr>
<tr>
<td>This value is set by the transmit-delay configuration statement.</td>
<td>All levels</td>
<td></td>
</tr>
<tr>
<td>Hold timer</td>
<td>Multiplier used in combination with the advertisement-interval value to determine the length of time LLDP information is held before it is discarded.</td>
<td></td>
</tr>
<tr>
<td>This value is set by the hold-multiplier configuration statement.</td>
<td>All levels</td>
<td></td>
</tr>
<tr>
<td>Notification interval</td>
<td>How often LLDP trap notifications are generated as a result of LLDP database changes. If the interval value is 0, LLDP trap notifications of database changes are disabled.</td>
<td></td>
</tr>
<tr>
<td>This value is set by the lldp-configuration-notification-interval configuration statement.</td>
<td>All levels</td>
<td></td>
</tr>
<tr>
<td>Config Trap Interval</td>
<td>How often LLDP trap notifications are generated as a result of changes in topology—for example, when an endpoint connects or disconnects. If the interval value is 0, LLDP trap notifications of topology changes are disabled.</td>
<td></td>
</tr>
<tr>
<td>This value is set by the topo-configuration-trap-interval configuration statement.</td>
<td>All levels</td>
<td></td>
</tr>
<tr>
<td>Connection Hold timer</td>
<td>Amount of time the system maintains dynamic topology entries.</td>
<td></td>
</tr>
<tr>
<td>This value is set by the topo-configuration-maximum-hold-time configuration statement.</td>
<td>All levels</td>
<td></td>
</tr>
<tr>
<td>LLDP-MED</td>
<td>LLDP-MED operating state. The state can be enabled or disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>MED fast start count</td>
<td>Number of advertisements sent from a switch to a device, such as a VoIP telephone, when the device is first detected by the switch. These increased advertisements are temporary. After a device and a switch exchange information and can communicate, advertisements are reduced to one per second.</td>
<td></td>
</tr>
<tr>
<td>This value is set by the fast-start configuration statement.</td>
<td>All levels</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface for which LLDP configuration information is being reported.</td>
<td>All levels</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 217: show lldp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP</td>
<td>LLDP operating state. The state can be <strong>enabled</strong> or <strong>disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Power Negotiation</td>
<td>LLDP power negotiation operating state. The state can be <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbor count</td>
<td>Total number of new LLDP neighbors detected since the last switch reboot.</td>
<td>detail</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface that is advertising VLAN information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Vlan-id</td>
<td>VLAN tag associated with the interface sending LLDP frames. If the interface is not a member of a VLAN, the VLAN ID is advertised as 0.</td>
<td>detail</td>
</tr>
<tr>
<td>Vlan-name</td>
<td>VLAN name associated with the VLAN ID.</td>
<td>detail</td>
</tr>
<tr>
<td>LLDP basic TLVs supported</td>
<td>Basic TLVs supported on the switch:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>Chassis identifier</strong>—TLV that advertises the MAC address associated with the local system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Port identifier</strong>—TLV that advertises the port identification for the specified port in the local system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Port description</strong>—Interface name for the port.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>System name</strong>—TLV that advertises the user-configured name of the local system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>System description</strong>—TLV that advertises the system description containing information about the software and current image running on the system. This information is taken from the software and is not configurable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>System capabilities</strong>—TLV that advertises the primary functions performed by the system—for example, bridge or router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Management address</strong>—TLV that advertises the IP management address of the local system.</td>
<td></td>
</tr>
<tr>
<td>Supported LLDP 802 TLVs</td>
<td>802.3 TLVs supported on the switch:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC/PHY configuration status</strong>—TLV that advertises information about the physical interface, such as autonegotiation status and support and MAU type. The information is based on the physical interface structure and is not configurable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Power via MDI</strong>—TLV that advertises MDI power support, PSE power pair, and power class information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link aggregation</strong>—TLV that advertises if the interface is aggregated and its aggregated interface ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum frame size</strong>—TLV that advertises the maximum transmission unit (MTU) of the interface sending LLDP frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Port VLAN tag</strong>—TLV that advertises the VLAN tag configured on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Port VLAN name</strong>—TLV that advertises the VLAN name configured on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
Table 217: show lldp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported LLDP MED TLVs</td>
<td>LLDP-MED TLVs supported on the switch:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>- LLDP MED capabilities—TLV that advertises the primary function of the port. The capabilities values range from 0 through 15:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 0—Capabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 1—Network Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 2—Location Identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 3—Extended Power via MDI-PSE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 4—Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 5–15—Reserved</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Network policy—TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types—such as voice or streaming video—802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Endpoint location—TLV that advertises the physical location of the endpoint.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Extended power Via MDI—TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show lldp

```
user@switch> show lldp
LLDP                   : Enabled
Advertisement interval : 30 seconds
Transmit delay         : 2 seconds
Hold timer             : 4 seconds
Notification interval  : 0 Second(s)
Config Trap Interval   : 0 seconds
Connection Hold timer  : 300 seconds
 LLDP MED               : Disabled
 MED fast start count   : 3 Packets

Interface      Parent Interface    LLDP        LLDP-MED     Power Negotiation
all            -                   Enabled     Enabled      Enabled
```

detail

```
user@switch> show lldp detail
LLDP                   : Enabled
Advertisement interval : 30 seconds
Transmit delay         : 2 seconds
Hold timer             : 4 seconds
Notification interval  : 0 Second(s)
Config Trap Interval   : 0 seconds
Connection Hold timer  : 300 seconds
 LLDP MED               : Disabled
 MED fast start count   : 3 Packets
```
### Interface Neighbor count

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>LLDP</th>
<th>LLDP-MED</th>
<th>Power Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>-</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Interface and Vlan-id

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Vlan-id</th>
<th>Vlan-name</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>100</td>
<td>v100</td>
</tr>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>101</td>
<td>v101</td>
</tr>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>4000</td>
<td>v4000</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>100</td>
<td>v100</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>101</td>
<td>v101</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>100</td>
<td>v100</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>101</td>
<td>v101</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>4000</td>
<td>v4000</td>
</tr>
</tbody>
</table>

LLDP basic TLVs supported:
- Chassis identifier
- Port identifier
- Port description
- System name
- System description
- System capabilities
- Management address

Supported LLDP 802 TLVs:
- MAC/PHY configuration/status
- Power via MDI
- Link aggregation
- Maximum frame size
- Port VLAN tag
- Port VLAN name

Supported LLDP MED TLVs:
- LLDP MED capabilities
- Network policy
- Endpoint location
- Extended power
- Via MDI
show lldp local-information

Syntax     show lldp local-information


Description Display the information that the switch provides in Link Layer Discovery Protocol (LLDP) advertisements to its neighbors.

Required Privilege Level view

Related Documentation • Configuring LLDP (CLI Procedure) on page 1745
• Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665
• management-address
• Configuring LLDP
• Understanding LLDP

List of Sample Output show lldp local-information (EX Series Switch) on page 1843

Output Fields Table 218 on page 1842 lists the output fields for the show lldp local-information command. Output fields are listed in the approximate order in which they appear.

Table 218: show lldp local-information Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Local Information</td>
<td>Information about the local system (the switch):</td>
</tr>
<tr>
<td>LLDP Local Information</td>
<td>• Chassis ID—MAC address associated with the switch.</td>
</tr>
<tr>
<td>LLDP Local Information</td>
<td>• System name—User-configured name of the switch.</td>
</tr>
<tr>
<td>LLDP Local Information</td>
<td>• System desc—System description containing information about the switch model and</td>
</tr>
<tr>
<td>LLDP Local Information</td>
<td>current software image running on the switch. This information is taken from the</td>
</tr>
<tr>
<td>LLDP Local Information</td>
<td>software and is not configurable.</td>
</tr>
</tbody>
</table>

System Capabilities Capabilities (such as bridge or router) that are supported or enabled on the system.

Management Information Details of the management information: Port Name, Port Address (such as 10.204.34.35), Address Type (such as ipv4 or ipv6), Port ID (SNMP interface index), Port ID Subtype, and Port Subtype.

The Port Subtype displays:

• ifIndex(2)—IP address of the switch’s management Ethernet interface (me0) or virtual management Ethernet (VME) interface address (for a virtual chassis) is used to manage the switch.

• unknown(1)—IP management address has been configured with set protocols lldp management-address.
Table 218: show lldp local-information Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Name of the local interface which is configured for either LLDP or LLDP-MED.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the local interface</td>
</tr>
<tr>
<td></td>
<td>belongs.</td>
</tr>
<tr>
<td>SNMP Index</td>
<td>SNMP interface index.</td>
</tr>
<tr>
<td>Interface description</td>
<td>User-configured port description.</td>
</tr>
<tr>
<td>Status</td>
<td>Administrative status of the interface: either <strong>up</strong> or <strong>down</strong>.</td>
</tr>
<tr>
<td>Tunneling</td>
<td>Status of tunneling on the interface: either <strong>enabled</strong> or <strong>disabled</strong>.</td>
</tr>
</tbody>
</table>

Sample Output

show lldp local-information (EX Series Switch)

current@switch> show lldp local-information

LLDP Local Information details

Chassis ID : 00:1d:b5:aa:b9:f0
System name : switch
System descr : Juniper Networks, Inc. ex8208, version 10.4I0 [builder] Build
date: 2010-11-17 12:38:30 UTC

System Capabilities
  Supported : Bridge Router
  Enabled : Bridge Router

Management Information
  Port Name : -
  Port Address : 10.93.54.6
  Address Type : IPv4
  Port ID : 34
  Port ID Subtype : local(7)
  Port Subtype : ifIndex(2)

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Parent Interface</th>
<th>SNMP Index</th>
<th>Interface description</th>
<th>Status</th>
<th>Tunneling</th>
</tr>
</thead>
<tbody>
<tr>
<td>me0.0</td>
<td>-</td>
<td>34</td>
<td>-</td>
<td>Down</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>769</td>
<td>xe-3/0/0.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>770</td>
<td>xe-3/0/1.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>771</td>
<td>xe-3/0/2.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/3.0</td>
<td>ae31.0</td>
<td>772</td>
<td>xe-3/0/3.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/4.0</td>
<td>ae31.0</td>
<td>577</td>
<td>xe-3/0/4.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/5.0</td>
<td>ae31.0</td>
<td>578</td>
<td>xe-3/0/5.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/6.0</td>
<td>ae31.0</td>
<td>579</td>
<td>xe-3/0/6.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
<tr>
<td>xe-3/0/7.0</td>
<td>ae31.0</td>
<td>581</td>
<td>xe-3/0/7.0</td>
<td>Up</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
show lldp neighbors

Syntax

show lldp neighbors
<interface interface>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the information about neighboring devices learned by the switch by using the Link Layer Discovery Protocol (LLDP).

NOTE: The Chassis ID TLV has a subtype for Network Address Family. The supported network address families are IPv4 and IPv6. LLDP frames are validated only if the Network Address subtype of the Chassis ID TLV has a value of 1 (IPv4) or 2 (IPv6). For any other value, the transmitting device is detected by LLDP as a neighbor and displayed in the output of the "show lldp neighbors" command, but is not assigned to the VLAN.

Options

none—Display LLDP neighbor information for all interfaces.

interface interface—(Optional) Display LLDP neighbor information for a selected interface.

Required Privilege Level

view

Related Documentation

• Configuring LLDP (CLI Procedure) on page 1745
• Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665

List of Sample Output

show lldp neighbors on page 1847
show lldp neighbors interface ge-0/0/2 on page 1847
show lldp neighbors interface ge-0/0/0.0 (for a VoIP Avaya Telephone with LLDP-MED Support) on page 1848
show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch) on page 1850

Output Fields

Table 219 on page 1844 lists the output fields for the show lldp neighbors command. Output fields are listed in the approximate order in which they appear.

Table 219: show lldp neighbors Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Interface</td>
<td>List of local interfaces for which neighbor information is available.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>List of aggregated Ethernet interfaces, if any, to which the local interfaces belong.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>List of chassis identifiers for neighbors.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port info</td>
<td>List of port information gathered from neighbors. This could be the port identifier or port description.</td>
</tr>
<tr>
<td>System name</td>
<td>List of system names gathered from neighbors.</td>
</tr>
<tr>
<td>LLDP Neighbor Information</td>
<td>Information about both the local system (the switch) and a neighbor system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Local Information</td>
<td>Information about the local system (appears when the interface option is used).</td>
</tr>
<tr>
<td>Index</td>
<td>Local interface index (appears when the interface option is used).</td>
</tr>
<tr>
<td>Time to live</td>
<td>Number of seconds for which this information is valid (appears when the interface option is used).</td>
</tr>
<tr>
<td>Time mark</td>
<td>Date and timestamp of information (appears when the interface option is used).</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Name of the local physical interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the interface option is used).</td>
</tr>
<tr>
<td>Local Port ID</td>
<td>Local interface SNMP index (appears when the interface option is used).</td>
</tr>
<tr>
<td>Ageout Count</td>
<td>Number of times the complete set of information advertised by the neighbor has been deleted from LLDP neighbor information maintained by the local system because the information timeliness interval has expired (appears when the interface option is used).</td>
</tr>
<tr>
<td>Neighbor Information</td>
<td>Information about a neighbor system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Chassis type</td>
<td>Type of chassis identifier supplied, such as MAC address (appears when the interface option is used).</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis identifier of the chassis type listed (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port type</td>
<td>Type of port identifier supplied, such as locally assigned (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port identifier of the port type listed (appears when the interface option is used).</td>
</tr>
<tr>
<td>Port description</td>
<td>Port description (appears when the interface option is used).</td>
</tr>
</tbody>
</table>
Table 219: show lldp neighbors Output Fields  (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System name</td>
<td>Name supplied by the system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>System Description</td>
<td>Description supplied by the system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>System capabilities</td>
<td>Capabilities (such as Bridge, Router, and Telephone) that are supported or enabled by the system on the interface (appears when the interface option is used).</td>
</tr>
<tr>
<td>Management Info</td>
<td>Details of management information: Type (such as ipv4 or ipv6), Address (such as 10.204.34.35), Port ID, Subtype, Interface Subtype, and organization identifier (OID) (appears when the interface option is used).</td>
</tr>
<tr>
<td></td>
<td>The Interface Subtype displays:</td>
</tr>
<tr>
<td></td>
<td>• ifIndex(2)—IP address of the neighbor's management Ethernet interface (me0) or virtual management Ethernet (VME) interface address (for a virtual chassis) is used to manage the switch.</td>
</tr>
<tr>
<td></td>
<td>• unknown(1)—Neighbor's IP management address has been configured with set protocols lldp management-address.</td>
</tr>
<tr>
<td>Media Info</td>
<td>Additional details about the endpoint device appear when a device that supports LLDP-MED is attached to the interface. The specific details depend upon the capabilities of the device. Details might include: Media endpoint class (such as Class 3 for communication devices such as IP phones), MED Hardware revision, MED Firmware revision, MED Software revision, MED Serial number, MED Manufacturer name, MED Model name.</td>
</tr>
<tr>
<td>Organization Info</td>
<td>One or more entries listing remote information by organizationally unique identifier (OUI), Subtype, Index, and Info (appears when the interface option is used).</td>
</tr>
<tr>
<td>Age</td>
<td>How long the neighbor has been identified (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Name of the local physical interface (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>Chassis identifier of the chassis type listed (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>Port description</td>
<td>Port description (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
<tr>
<td>System name</td>
<td>NetBIOS name of the host (appears when the interface option is used and NetBIOS snooping is enabled on the switch).</td>
</tr>
</tbody>
</table>
## Sample Output

**show lldp neighbors**

```
user@switch> show lldp neighbors

<table>
<thead>
<tr>
<th>Local Interface</th>
<th>Parent Interface</th>
<th>Chassis Id</th>
<th>Port info</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-3/0/4.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/0/0.0</td>
<td>newyork31</td>
</tr>
<tr>
<td>xe-3/0/5.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/0/1.0</td>
<td>newyork31</td>
</tr>
<tr>
<td>xe-3/0/6.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/0/2.0</td>
<td>newyork31</td>
</tr>
<tr>
<td>xe-3/0/7.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/0/3.0</td>
<td>newyork31</td>
</tr>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/1/0.0</td>
<td>newyork31</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/1/1.0</td>
<td>newyork31</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/1/2.0</td>
<td>newyork31</td>
</tr>
<tr>
<td>xe-3/0/3.0</td>
<td>ae31.0</td>
<td>b0:c6:9a:63:80:40</td>
<td>xe-0/1/3.0</td>
<td>newyork31</td>
</tr>
</tbody>
</table>
```

**show lldp neighbors interface ge-0/0/2**

```
user@switch> show lldp neighbors interface ge-0/0/2

LLDP Neighbor Information:
Local Information:
Local Interface : ge-0/0/2.0
Parent Interface : -
Local Port ID : 507
Ageout Count : 0

Neighbour Information:
Chassis type : Mac address
Chassis ID : 00:1f:12:38:7f:c0
Port type : Locally assigned
Port ID : 507
Port description : ge-0/0/2.0
System name : bng-l48p5-dev

System Description : Juniper Networks, Inc. ex4200-48p , version 10.4I0 Build
date: 2010-11-30 09:32:17 UTC

System capabilities
Supported : Bridge Router
Enabled : Bridge Router

Management Info
  Type : IPv4
  Address : 10.204.96.235
  Port ID : 34
Subtype : 1
  Interface Subtype : ifIndex(2)
  OID : 1.3.6.1.2.1.31.1.1.1.34
Media endpoint class : Network Connectivity

Organization Info
  OUI : 0.12.f
  Subtype : 1
  Index : 1
  Info : 22A8360000

Organization Info
  OUI : 0.12.f
```
show lldp neighbors interface ge-0/0/0.0 (for a VoIP Avaya Telephone with LLDP-MED Support)

user@switch> show lldp neighbors interface ge-0/0/0.0

LLDP Neighbor Information:
Local Information:
Index: 20 Time to live: 120 Time mark: Thu Apr 15 22:26:22 2010 Age: 16 secs
Local Interface : ge-0/0/0.0
Parent Interface : -
Local Port ID : 517
Ageout Count : 0

Neighbour Information:
Chassis type : Network address
Chassis ID : 0.0.0.0
Port type : Mac address
Port ID : 00:04:0d:fc:55:48
System name : AVAFC5548

System capabilities
Supported : Bridge Telephone
Enabled : Bridge

Management Info
Type : IPv4
Address : 0.0.0.0
Port ID : 1
Subtype : 1
Interface Subtype : ifIndex(2)
OID : 1.3.6.1.2.1.31.1.1.1.1.1.1.1.1.1

Media endpoint class: Class III Device

MED Hardware revision : 4610D01A
MED Firmware revision : b10d01b2_9.bin
MED Software revision : a10d01b2_9.bin
MED Serial number : 07N510103424
MED Manufacturer name : Avaya
MED Model name : 4610

Organization Info
OUI : 0.18.15
Subtype : 1
Index : 1
Info : 036CA00010

Organization Info
OUI : 0.18.15
Subtype : 1
Index : 2
Info : 002303

Organization Info
OUI : 0.18.15
Subtype : 2
Index : 3
Info : 014001AE
Organization Info
OUI : 0.18.15
Subtype : 5
Index : 4
Info : 3436313044303141

Organization Info
OUI : 0.18.15
Subtype : 6
Index : 5
Info : 62313064303162325F392E62696E

Organization Info
OUI : 0.18.15
Subtype : 7
Index : 6
Info : 61313064303162325F392E62696E

Organization Info
OUI : 0.18.15
Subtype : 8
Index : 7
Info : 30374E353130313033343234

Organization Info
OUI : 0.18.15
Subtype : 9
Index : 8
Info : 4176617961

Organization Info
OUI : 0.18.15
Subtype : 10
Index : 9
Info : 34363130

Organization Info
OUI : 0.18.15
Subtype : 1
Index : 10
Info : 000028003C

Organization Info
OUI : 0.18.15
Subtype : 3
Index : 11
Info : 00000000

Organization Info
OUI : 0.18.15
Subtype : 4
Index : 12
Info : 000000000000000000000000

Organization Info
OUI : 0.18.15
Subtype : 5
Index : 13
Info : 00000000

Organization Info
OUI      : 0.18.15
Subtype  : 6
Index    : 14
Info     : 00000000

Organization Info
OUI      : 0.18.15
Subtype  : 7
Index    : 15
Info     : 01

show lldp neighbors interface ge-0/0/5.0 (with NetBIOS Snooping Enabled on the Switch)

user@switch> show lldp neighbors interface ge-0/0/5
Age: 299999 secs
Local Interface    : ge-0/0/5.0
Parent Interface   : -
Chassis ID         : 00:10:94:00:00:02
Port description   : 169.254.58.17
System name        : JNPRU\
show lldp remote-global-statistics

Syntax
show lldp remote-global-statistics

Release Information
Command introduced in Junos OS Release 10.0 for EX Series switches.

Description
Display remote Link Layer Discovery Protocol (LLDP) global statistics.

Options
This command has no options.

Required Privilege Level
view

Related Documentation
- Configuring LLDP (CLI Procedure) on page 1745
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665

List of Sample Output
show lldp remote-global-statistics on page 1852

Output Fields
Table 220 on page 1851 describes the output fields for the show lldp remote-global-statistics command. Output fields are listed in the approximate order in which they appear.

Table 220: show lldp remote-global-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP Remote Database Table Counters</td>
<td>Information about remote database table counters.</td>
</tr>
<tr>
<td>LastchangeTime</td>
<td>Time elapsed between LLDP agent startup and the last change to the remote database table information.</td>
</tr>
<tr>
<td>Inserts</td>
<td>Number of insertions made in the remote database table.</td>
</tr>
<tr>
<td>Deletes</td>
<td>Number of deletions made in the remote database table.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of LLDP frames dropped from the remote database table because of errors.</td>
</tr>
<tr>
<td>Ageouts</td>
<td>Number of remote database table entries that have aged out of the table.</td>
</tr>
</tbody>
</table>
Sample Output

show lldp remote-global-statistics

```
user@host> show lldp remote-global-statistics
user@host> show lldp remote-global-statistics
LLDP Remote Database Table Counters
LastchangeTime          Inserts    Deletes    Drops    Ageouts
00:00:76 (76 sec)       192        0          0        0
```
show lldp statistics

Syntax

show lldp statistics

<interface interface>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display LLDP statistics for all interfaces or for the specified interface.

Options

none—Display LLDP statistics for all interfaces.

interface interface—(Optional) Display LLDP statistics for the specified interface.

Required Privilege

view

Related Documentation

- Configuring LLDP (CLI Procedure) on page 1745
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches on page 1665

List of Sample Output

show lldp statistics on page 1854

show lldp statistics interface xe-3/0/0.0 on page 1854

Output Fields

Table 221 on page 1853 lists the output fields for the show lldp statistics command. Output fields are listed in the approximate order in which they appear.

Table 221: show lldp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
<tr>
<td>Parent Interface</td>
<td>Name of the aggregated Ethernet interface, if any, to which the interface belongs.</td>
</tr>
<tr>
<td>NOTE: Because LLDP packets are transmitted and received on member interfaces only, statistics are available only for the member interfaces, not for the aggregated interface.</td>
<td></td>
</tr>
<tr>
<td>Received</td>
<td>Total number of LLDP frames received on an interface.</td>
</tr>
<tr>
<td>Unknown TLVs</td>
<td>Number of unrecognized LLDP TLVs received on an interface.</td>
</tr>
<tr>
<td>With Errors</td>
<td>Number of invalid LLDP TLVs received on an interface.</td>
</tr>
<tr>
<td>Discarded</td>
<td>Number of LLDP TLVs received and then discarded on an interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Total number of LLDP frames that were transmitted on an interface.</td>
</tr>
<tr>
<td>Untransmitted</td>
<td>Total number of LLDP frames that were untransmitted on an interface.</td>
</tr>
</tbody>
</table>
### Sample Output

**show lldp statistics**

```
user@switch> show lldp statistics

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Received</th>
<th>Unknown TLVs</th>
<th>With Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>1564</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/1.0</td>
<td>ae31.0</td>
<td>1564</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/2.0</td>
<td>ae31.0</td>
<td>1565</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/3.0</td>
<td>ae31.0</td>
<td>1566</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/4.0</td>
<td>ae31.0</td>
<td>1598</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/5.0</td>
<td>ae31.0</td>
<td>1598</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/6.0</td>
<td>ae31.0</td>
<td>1596</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-3/0/7.0</td>
<td>ae31.0</td>
<td>1597</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-5/0/6.0</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>xe-5/0/7.0</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Discarded TLVs  Transmitted  Untransmitted
0               3044         1
0               3044         1
0               3044         1
0               3044         1
0               3075         1
0               3075         1
0               3075         1
0               3075         1
0               17312        0
0               17312        0
```

**show lldp statistics interface xe-3/0/0.0**

```
user@switch> show lldp statistics interface xe-3/0/0.0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Parent Interface</th>
<th>Received</th>
<th>Unknown TLVs</th>
<th>With Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-3/0/0.0</td>
<td>ae31.0</td>
<td>1566</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Discarded TLVs  Transmitted  Untransmitted
0               3046         1
```
**show network-access aaa statistics accounting**

### Syntax

```
show network-access aaa statistics accounting
```

### Release Information

- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for QFX Series switches.

### Description

Display authentication, authorization, and accounting (AAA) accounting statistics.

### Required Privilege Level

```
view
```

### Related Documentation

- `accounting-server`
- `accounting-stop-on-access-deny`
- Configuring 802.1X RADIUS Accounting (CLI Procedure) on page 1741
- Configuring RADIUS Accounting

### List of Sample Output

**Show network-access aaa statistics accounting on page 1855**

### Output Fields

Table 222 on page 1855 lists the output fields for the `show network-access aaa statistics accounting` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>The number of accounting-request packets sent from a switch to a RADIUS accounting server.</td>
</tr>
<tr>
<td>Accounting Response failures</td>
<td>The number of accounting-response failure packets sent from the RADIUS accounting server to the switch.</td>
</tr>
<tr>
<td>Accounting Response Success</td>
<td>The number of accounting-response success packets sent from the RADIUS accounting server to the switch.</td>
</tr>
<tr>
<td>Requests timedout</td>
<td>The number of requests-timedout packets sent from the RADIUS accounting server to the switch.</td>
</tr>
</tbody>
</table>

### Sample Output

```
user@switch> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 1
  Accounting Response failures: 0
  Accounting Response Success: 1
  Requests timedout: 0
```
**Syntax**

```show network-access aaa statistics authentication```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

**Description**

Display authentication, authorization, and accounting (AAA) authentication statistics.

**Required Privilege Level**

`view`

**Related Documentation**

- `authentication-server`
- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 1675

**List of Sample Output**

- `show network-access aaa statistics authentication` on page 1856
- `show network-access aaa statistics authentication (in QFX Series Switches)` on page 1856

**Output Fields**

Table 223 on page 1856 lists the output fields for the `show network-access aaa statistics authentication` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>The number of authentication requests received by the switch.</td>
</tr>
<tr>
<td>Accepts</td>
<td>The number of authentication accepts received by the RADIUS server.</td>
</tr>
<tr>
<td>Rejects</td>
<td>The number authentication rejects sent by the RADIUS server.</td>
</tr>
<tr>
<td>Challenges</td>
<td>The number of authentication challenges sent by the RADIUS server.</td>
</tr>
</tbody>
</table>

**Sample Output**

**show network-access aaa statistics authentication**

```user@switch> show network-access aaa statistics authentication
Authentication module statistics
 Requests received: 2
 Accepts: 1
 Rejects: 0
 Challenges: 1
```

**show network-access aaa statistics authentication (in QFX Series Switches)**

```user@lfd0> show network-access aaa statistics authentication
Authentication module statistics
 Requests received: 2
 Accepts: 1
```
Rejects: 0
Challenges: 1
**show network-access aaa statistics dynamic-requests**

**Syntax**
show network-access aaa statistics dynamic-requests;

**Release Information**

**Description**
Display authentication, authorization, and accounting (AAA) authentication statistics for disconnects.

**Required Privilege Level**
view

**Related Documentation**
- *authentication-server*
  - Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch on page 1675

**List of Sample Output**
show network-access aaa statistics authentication on page 1858

**Output Fields**
Table 224 on page 1858 lists the output fields for the `show network-access aaa statistics dynamic-requests` command. Output fields are listed in the approximate order in which they appear.

**Table 224: show network-access aaa statistics dynamic-requests Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests received</td>
<td>The number of dynamic requests received by the RADIUS server.</td>
</tr>
<tr>
<td>Processed successfully</td>
<td>The number of dynamic requests successfully processed by the RADIUS server.</td>
</tr>
<tr>
<td>Errors during processing</td>
<td>The number of errors that occurred while the RADIUS server was processing the dynamic request.</td>
</tr>
<tr>
<td>Silently dropped</td>
<td>The number of silently dropped requests.</td>
</tr>
</tbody>
</table>

**Sample Output**

show network-access aaa statistics authentication

```
user@switch> show network-access aaa statistics dynamic-requests
Dynamic-requests module statistics
  Requests received:  0
  Processed successfully:  0
  Errors during processing:  0
  Silently dropped:  0
```
PART 11

Class of Service

- Overview on page 1861
- Configuration on page 1895
- Administration on page 1975
- Troubleshooting Procedures on page 2009
CHAPTER 31

Overview

- CoS Overview on page 1861

CoS Overview

- Junos OS CoS for EX Series Switches Overview on page 1862
- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Understanding CoS Code-Point Aliases on page 1866
- Understanding CoS Classifiers on page 1869
- Understanding CoS Forwarding Classes on page 1872
- Understanding CoS Congestion Management on page 1875
- Understanding CoS Schedulers on page 1880
- Understanding CoS Two-Color Marking on page 1887
- Understanding CoS Rewrite Rules on page 1887
- Understanding Port Shaping and Queue Shaping for CoS on EX Series Switches on page 1889
- Understanding Junos OS EZQoS for CoS Configurations on EX Series Switches on page 1890
- Understanding CoS Queues on EX8200 Line Cards That Include Oversubscribed Ports on page 1891
Junos OS CoS for EX Series Switches Overview

When a network experiences congestion and delay, some packets must be dropped. Junos operating system (Junos OS) class of service (CoS) divides traffic into classes to which you can apply different levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to rules that you configure.

For interfaces that carry IPv4, IPv6, and MPLS traffic, you can configure Junos OS CoS features to provide multiple classes of service for different applications. CoS also allows you to rewrite the Differentiated Services code point (DSCP), IP precedence, 802.1p, or EXP CoS bits of packets egressing out of an interface, thus allowing you to tailor packets for the remote peers’ network requirements. See Understanding Using CoS with MPLS Networks on EX Series Switches for more information about CoS for MPLS networks.

CoS provides multiple classes of service for different applications. You can configure multiple forwarding classes for transmitting packets, define which packets are placed into each output queue, and schedule the transmission service level for each queue.

In designing CoS applications, you must give careful consideration to your service needs and thoroughly plan and design your CoS configuration to ensure consistency and interoperability across all platforms in a CoS domain.

Because Juniper Networks EX Series Ethernet Switches implement CoS in hardware rather than in software, you can experiment with and deploy CoS features without affecting packet-forwarding and switching performance.

NOTE: CoS policies can be enabled or disabled on each interface of an EX Series switch. Also, each physical and logical interface on the switch can have custom CoS rules associated with it. When CoS is used in an MPLS network, there are some additional restrictions. See Understanding Using CoS with MPLS Networks on EX Series Switches.

- How Junos OS CoS Works on page 1862
- Default CoS Behavior on EX Series Switches on page 1863

How Junos OS CoS Works

Junos OS CoS works by examining traffic entering at the edge of your network. The switches classify traffic into defined service groups to provide the special treatment of traffic across the network. For example, voice traffic can be sent across certain links, and data traffic can use other links. In addition, the data traffic streams can be serviced differently along the network path. As the traffic leaves the network at the far edge, you can rewrite the traffic to meet the policies of the targeted peer.

To support CoS, you must configure each switch in the network. Generally, each switch examines the packets that enter it to determine their CoS settings. These settings then dictate which packets are transmitted first to the next downstream switch. Switches at the edges of the network might be required to alter the CoS settings of the packets that enter the network to classify the packets into the appropriate service groups.
Figure 22 on page 1863 represents the network scenario of an enterprise. Switch A is receiving traffic from various network nodes such as desktop computers, servers, surveillance cameras, and VoIP telephones. As each packet enters, Switch A examines the packet’s CoS settings and classifies the traffic into one of the groupings defined by the enterprise. This definition allows Switch A to prioritize resources for servicing the traffic streams it receives. Switch A might alter the CoS settings of the packets to better match the enterprise’s traffic groups.

When Switch B receives the packets, it examines the CoS settings, determines the appropriate traffic groups, and processes the packets according to those settings. It then transmits the packets to Switch C, which performs the same actions. Switch D also examines the packets and determines the appropriate groups. Because Switch D sits at the far end of the network, it can rewrite the CoS bits of the packets before transmitting them.

Figure 22: Packet Flow Across the Network

Default CoS Behavior on EX Series Switches

If you do not configure any CoS settings on the switch, the software performs some CoS functions to ensure that user traffic and protocol packets are forwarded with minimum delay when the network is experiencing congestion. Some CoS settings, such as classifiers, are automatically applied to each logical interface that you configure. Other settings, such as rewrite rules, are applied only if you explicitly associate them with an interface.

Related Documentation

- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Understanding Junos OS EZQoS for CoS Configurations on EX Series Switches on page 1890
- Example: Configuring CoS on EX Series Switches on page 1895
- Example: Combining CoS with MPLS on EX Series Switches

Understanding Junos OS CoS Components for EX Series Switches

This topic describes the Juniper Networks Junos operating system (Junos OS) class-of-service (CoS) components for Juniper Networks EX Series Ethernet Switches:

- Code-Point Aliases on page 1864
- Policers on page 1864
• Classifiers on page 1864
• Forwarding Classes on page 1864
• Tail Drop Profiles on page 1865
• Schedulers on page 1865
• Rewrite Rules on page 1865

**Code-Point Aliases**

A code-point alias assigns a name to a pattern of code-point bits. You can use this name instead of the bit pattern when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules.

**Policers**

Policers limit traffic of a certain class to a specified bandwidth and *burst size*. Packets exceeding the policer limits can be discarded. You define policers with filters that can be associated with input interfaces.

For more information about policers, see “Understanding the Use of Policers in Firewall Filters” on page 4155.

**NOTE:** You can configure policers to discard packets that exceed the rate limits. If you want to configure CoS parameters such as loss-priority and forwarding-class, you must use firewall filters.

**Classifiers**

Packet classification associates incoming packets with a particular CoS servicing level. In Juniper Networks Junos operating system (Junos OS), *classifiers* associate packets with a forwarding class and loss priority and assign packets to output queues based on the associated forwarding class. Junos OS supports two general types of classifiers:

- Behavior aggregate or CoS value traffic classifiers—Examines the CoS value in the packet header. The value in this single field determines the CoS settings applied to the packet. BA classifiers allow you to set the forwarding class and loss priority of a packet based on the Differentiated Services code point (DSCP) value, IP precedence value, and IEEE 802.1p value.

- Multifield traffic classifiers—Examines multiple fields in the packet such as source and destination addresses and source and destination port numbers of the packet. With multifield classifiers, you set the forwarding class and loss priority of a packet based on firewall filter rules.

**Forwarding Classes**

Forwarding classes group the packets for transmission. Based on forwarding classes, you assign packets to output queues. Forwarding classes affect the forwarding, scheduling, and marking policies applied to packets as they transit a switch. By default, four categories of forwarding classes are defined: best effort, assured forwarding, expedited forwarding, and...
and network control. For EX Series switches, 16 forwarding classes are supported, providing
granular classification capability.

**Tail Drop Profiles**

Drop profile is a mechanism that defines parameters that allow packets to be dropped
from the network. Drop profiles define the meanings of the loss priorities. When you
configure drop profiles you are essentially setting the value for queue fullness. The queue
fullness represents a percentage of the queue used to store packets in relation to the
total amount that has been allocated for that specific queue.

Loss priorities set the priority of dropping a packet. Loss priority affects the scheduling
of a packet without affecting the packet’s relative ordering. You can use the loss priority
setting to identify packets that have experienced congestion. Typically you mark packets
exceeding some service level with a high loss priority.

**Schedulers**

Each switch interface has multiple queues assigned to store packets. The switch
determines which queue to service based on a particular method of scheduling. This
process often involves determining which type of packet should be transmitted before
another. You can define the priority, bandwidth, delay buffer size, and tail drop profiles
to be applied to a particular queue for packet transmission.

A scheduler map associates a specified forwarding class with a scheduler configuration.
You can associate up to four user-defined scheduler maps with the interfaces.

**Rewrite Rules**

A rewrite rule sets the appropriate CoS bits in the outgoing packet, thus allowing the next
downstream device to classify the packet into the appropriate service group. Rewriting,
or marking, outbound packets is useful when the switch is at the border of a network and
must alter the CoS values to meet the policies of the targeted peer.

---

**NOTE:** Egress firewall filters can also assign forwarding class and loss priority
so that the packets are rewritten based on forwarding class and loss priority.

---

**Related Documentation**

- Understanding CoS Code-Point Aliases on page 1866
- Understanding CoS Classifiers
- Understanding CoS Forwarding Classes
- Understanding CoS Tail Drop Profiles
- Understanding CoS Schedulers on page 1880
- Understanding CoS Two-Color Marking on page 1887
- Understanding CoS Rewrite Rules on page 1887
- Example: Configuring CoS on EX Series Switches on page 1895
Understanding CoS Code-Point Aliases

A code-point alias assigns a name to a pattern of code-point bits. You can use this name instead of the bit pattern when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules.

Behavior aggregate classifiers use class-of-service (CoS) values such as Differentiated Services code points (DSCPs), IP precedence, and IEEE 802.1p bits to associate incoming packets with a particular CoS servicing level. On a switch, you can assign a meaningful name or alias to the CoS values and use this alias instead of bits when configuring CoS components. These aliases are not part of the specifications but are well known through usage. For example, the alias for DSCP 101110 is widely accepted as ef (expedited forwarding).

When you configure classes and define classifiers, you can refer to the markers by alias names. You can configure user-defined classifiers in terms of alias names. If the value of an alias changes, it alters the behavior of any classifier that references it.

This topic covers:

- Default Code-Point Aliases on page 1866

Default Code-Point Aliases

Table 225 on page 1866 shows the default mappings between the bit values and standard aliases.

Table 225: Default Code-Point Aliases

<table>
<thead>
<tr>
<th>CoS Value Types</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSCP CoS Values</strong></td>
<td></td>
</tr>
<tr>
<td>ef</td>
<td>101110</td>
</tr>
<tr>
<td>af11</td>
<td>001010</td>
</tr>
<tr>
<td>af12</td>
<td>001100</td>
</tr>
<tr>
<td>af13</td>
<td>001110</td>
</tr>
<tr>
<td>af21</td>
<td>010010</td>
</tr>
<tr>
<td>af22</td>
<td>010100</td>
</tr>
<tr>
<td>af23</td>
<td>010110</td>
</tr>
<tr>
<td>af31</td>
<td>011010</td>
</tr>
<tr>
<td>af32</td>
<td>011100</td>
</tr>
<tr>
<td>af33</td>
<td>011110</td>
</tr>
</tbody>
</table>
### Table 225: Default Code-Point Aliases (continued)

<table>
<thead>
<tr>
<th>CoS Value Types</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>af41</td>
<td>100010</td>
</tr>
<tr>
<td>af42</td>
<td>100100</td>
</tr>
<tr>
<td>af43</td>
<td>100110</td>
</tr>
<tr>
<td>be</td>
<td>000000</td>
</tr>
<tr>
<td>cs1</td>
<td>001000</td>
</tr>
<tr>
<td>cs2</td>
<td>010000</td>
</tr>
<tr>
<td>cs3</td>
<td>011000</td>
</tr>
<tr>
<td>cs4</td>
<td>100000</td>
</tr>
<tr>
<td>cs5</td>
<td>101000</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110000</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111000</td>
</tr>
</tbody>
</table>

**IEEE 802.1p CoS Values**

<table>
<thead>
<tr>
<th>CoS Value Types</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td>ef</td>
<td>100</td>
</tr>
<tr>
<td>ef1</td>
<td>101</td>
</tr>
<tr>
<td>af11</td>
<td>010</td>
</tr>
<tr>
<td>af12</td>
<td>011</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111</td>
</tr>
</tbody>
</table>

**Legacy IP Precedence CoS Values**

<table>
<thead>
<tr>
<th>CoS Value Types</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td>ef</td>
<td>010</td>
</tr>
</tbody>
</table>
Table 225: Default Code-Point Aliases (continued)

<table>
<thead>
<tr>
<th>CoS Value Types</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>efl</td>
<td>011</td>
</tr>
<tr>
<td>af11</td>
<td>100</td>
</tr>
<tr>
<td>af12</td>
<td>101</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111</td>
</tr>
</tbody>
</table>

Related Documentation
- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921
- Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
Understanding CoS Classifiers

Packet classification associates incoming packets with a particular class-of-service (CoS) servicing level. Classifiers associate packets with a forwarding class and loss priority, and packets are associated to an output queue based on the forwarding class. You can define classifiers for IPv4 and IPv6 traffic to network interfaces, aggregated Ethernet interfaces (also known as link aggregation groups (LAGs)), integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces (RVIs)), Layer 3 interfaces, and Layer 3 VLAN-tagged logical interfaces.

There are two general types of classifiers:

- Behavior aggregate (BA) classifiers
- Multifield (MF) classifiers

You can configure both a BA classifier and an MF classifier on an interface. If you do this, the BA classification is performed first and then the MF classification. If the two classification results conflict, the MF classification result overrides the BA classification result.

On Juniper Networks EX8200 Ethernet Switches, you can specify BA classifiers for bridged multidestination traffic and for IP multidestination traffic. A BA classifier for multicast packets is applied to all interfaces on the EX8200 switch.

**NOTE:** EX8200 switches implement the on-demand allocation of memory space for ternary content addressable memory (TCAM) so that when additional TCAM space is required for CoS classifiers, it is allocated from the free TCAM space or from the unused TCAM space. An error log message is generated when you configure CoS classifiers to use memory space that exceeds the available TCAM space that includes both the free and unused space.

This topic describes:

- Behavior Aggregate Classifiers on page 1869
- Multifield Classifiers on page 1871

**Behavior Aggregate Classifiers**

The behavior aggregate classifier maps packets to a forwarding class and a loss priority. The forwarding class determines the output queue for a packet. The loss priority is used by a scheduler to control packet discard during periods of congestion.

There are three types of BA classifiers:

- Differentiated Services Code Point (DSCP) for IP DiffServ
- IP precedence bits
- IEEE 802.1p CoS bits
BA classifiers are based on fixed-length fields, which makes them computationally more efficient than MF classifiers. Therefore core devices, which handle high traffic volumes, are normally configured to perform BA classification.

**Default Behavior Aggregate Classification**

Juniper Networks Junos operating system (Junos OS) automatically assigns implicit default BA classifiers to logical interfaces based on the type of interface. Table 226 on page 1870 lists different types of interfaces and the corresponding implicit default BA classification.

### Table 226: Default BA Classification

<table>
<thead>
<tr>
<th>Type of Interface</th>
<th>Default BA Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trunk and Circuit Cross-Connect (CCC) interfaces</td>
<td>ieee8021p-default</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This BA classification for a CCC interface is applicable only for EX8200 switches.</td>
</tr>
<tr>
<td>Layer 3 interface (IPv4)</td>
<td>dscp-default</td>
</tr>
<tr>
<td>Layer 3 interface (IPv6)</td>
<td>dscp-ipv6-default</td>
</tr>
<tr>
<td>Access interface</td>
<td>Untrusted</td>
</tr>
<tr>
<td>Routed VLAN interface (RVI)</td>
<td>No default classification</td>
</tr>
<tr>
<td>MPLS</td>
<td>EXP</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This BA classification is applicable only for EX8200 switches.</td>
</tr>
</tbody>
</table>

When you explicitly associate a BA classifier with a logical interface, you are overriding the implicit (default) BA classifier with an explicit BA classifier.

Table 227 on page 1870 describes the BA classifier types you can configure on Layer 2 and Layer 3 interfaces.

### Table 227: Allowed BA Classification

<table>
<thead>
<tr>
<th>Type of Interface</th>
<th>Allowed BA Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Interface</td>
<td>IEEE 802.1p, IP precedence, DSCP, DSCP IPv6</td>
</tr>
<tr>
<td>Layer 3 interface (IPv4)</td>
<td>IEEE 802.1p, IP precedence, DSCP</td>
</tr>
<tr>
<td>Layer 3 interface (IPv6)</td>
<td>IEEE 802.1p, IP precedence, DSCP IPv6</td>
</tr>
</tbody>
</table>

You can configure all the allowed classifier types on the same logical interface or on different logical interfaces. If you need to apply all classifier rules on the same logical interface, configure the classifier rules allowed for both IPv4 and IPv6 on the logical interface.
If you have not explicitly configured a classifier on a logical interface, the default classifiers are assigned and classification works as follows:

- To a logical interface configured with an IPv4 address, a DSCP classifier is assigned by default, and IPv4 and IPv6 packets are classified using the DSCP classifier.
- To logical interface configured with an IPv6 address, a DSCP IPv6 classifier is assigned by default, and IPv4 and IPv6 packets are classified using the DSCP IPv6 classifier.

**NOTE:** On EX8200 switches, you can configure either one classifier of type DSCP or IEEE802.1p, or you can configure one classifier each of type DSCP and IEEE802.1p.

You can configure integrated routing and bridging (IRB) interfaces (also known as routed VLAN interfaces (RVIs)) to classify packets. After you do this, the User Priority (UP) bits in the incoming packets are rewritten according to the default IEEE 802.1p rewrite rule, except on EX8200 switches. On EX8200 switches, you must explicitly assign the default IEEE 802.1p rewrite rule to RVIs.

**NOTE:** By default, all BA classifiers classify traffic into either the best-effort forwarding class or the network-control forwarding class.

**Multifield Classifiers**

Multifield classifiers examine multiple fields in a packet such as source and destination addresses and source and destination port numbers of the packet. With MF classifiers, you set the forwarding class and loss priority of a packet based on firewall filter rules.

MF classification is normally performed at the network edge because of the general lack of support for DSCP or IP precedence classifiers in end-user applications. On an edge switch, an MF classifier provides the filtering functionality that scans through a variety of packet fields to determine the forwarding class for a packet. Typically, any classifier performs matching operations on the selected fields against a configured value.

**Related Documentation**

- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Classifiers (CLI Procedure) on page 1923
- Defining CoS Classifiers (J-Web Procedure) on page 1925
Understanding CoS Forwarding Classes

Class-of-Service (CoS) forwarding classes can be thought of as output queues. In effect, the result of classifying packets is the identification of an output queue for a particular packet. For a classifier to assign an output queue to a packet, it must associate the packet with one of the following forwarding classes:

- best-effort (be)—Provides no service profile. Loss priority is typically not carried in a CoS value.
- expedited-forwarding (ef)—Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service.
- assured-forwarding (af)—Provides a group of values you can define and includes four subclasses: AF1, AF2, AF3, and AF4, each with two drop probabilities: low and high.
- network-control (nc)—Supports protocol control and thus is typically high priority.
- multicast best-effort (mcast-be)—Provides no service profile for multicast packets.
- multicast expedited forwarding (mcast-ef)—Supports high-priority multicast packets.
- multicast assured-forwarding (mcast-af)—Provides two drop profiles; high, and low, for multicast packets.

NOTE: The forwarding classes multicast expedited-forwarding, multicast assured-forwarding, and multicast best-effort are applicable only to Juniper Networks EX8200 and Juniper Networks EX4300 Ethernet Switches.

Juniper Networks EX Series Ethernet Switches support up to 16 forwarding classes, thus allowing granular packet classification. For example, you can configure multiple classes of expedited forwarding (EF) traffic such as EF, EF1, and EF2.

EX Series switches except EX4300 switches support up to eight output queues. Therefore, if you configure more than eight forwarding classes, you must map multiple forwarding classes to single output queues. EX4300 switches support up to 12 output queues. On EX8200 Virtual Chassis, you can configure only eight forwarding classes and you can assign only one forwarding class to each output queue.

NOTE: On EX8200 Virtual Chassis, the queue number seven carries Virtual Chassis port (VCP) traffic and can also carry high-priority user traffic.

This topic describes:

- Default Forwarding Classes on page 1873
Default Forwarding Classes

Table 228 on page 1873 shows the four default forwarding classes defined for unicast traffic, and Table 229 on page 1873 shows the three default forwarding classes defined for multicast traffic.

NOTE: The default forwarding classes for multicast traffic are applicable only to EX8200 switches.

You can rename the forwarding classes associated with the queues supported on your switch. Assigning a new class name to an output queue does not alter the default classification or scheduling that is applicable to that queue. However, because CoS configurations can be quite complicated, we recommend that you avoid altering the default class names or queue number associations.

Table 228: Default Forwarding Classes for Unicast Traffic

<table>
<thead>
<tr>
<th>Forwarding Class Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort (be)</td>
<td>The software does not apply any special CoS handling to packets with 000000 in the DiffServ field. This is a backward compatibility feature. These packets are usually dropped under congested network conditions.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>expedited-forwarding (ef)</td>
<td>The software delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for packets in this service class. The software accepts excess traffic in this class, but in contrast to the assured forwarding class, the out-of-profile expedited-forwarding class packets can be forwarded out of sequence or dropped.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>assured-forwarding (af)</td>
<td>The software offers a high level of assurance that the packets are delivered as long as the packet flow from the customer stays within a certain service profile that you define.</td>
</tr>
<tr>
<td></td>
<td>The software accepts excess traffic, but it applies a tail drop profile to determine that excess packets are dropped, and not forwarded.</td>
</tr>
<tr>
<td></td>
<td>Two drop probabilities (low and high) are defined for this service class.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>network-control (nc)</td>
<td>The software delivers packets in this service class with a high priority. (These packets are not delay-sensitive.)</td>
</tr>
<tr>
<td></td>
<td>Typically, these packets represent routing protocol hello or keep alive messages. Because loss of these packets jeopardizes proper network operation, packet delay is preferable to packet discard for these packets.</td>
</tr>
</tbody>
</table>

Table 229: Default Forwarding Classes for Multicast Traffic

<table>
<thead>
<tr>
<th>Forwarding Class Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast best-effort (mcast-be)</td>
<td>The software does not apply any special CoS handling to multicast packets. These packets are usually dropped under congested network conditions.</td>
</tr>
</tbody>
</table>
### Table 229: Default Forwarding Classes for Multicast Traffic (continued)

<table>
<thead>
<tr>
<th>Forwarding Class Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast expedited-forwarding (mcast-ef)</td>
<td>The software delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for multicast packets in this service class. The software accepts excess traffic in this class, but in contrast to the multicast assured forwarding class, out-of-profile multicast expedited-forwarding class packets can be forwarded out of sequence or dropped.</td>
</tr>
<tr>
<td>multicast assured-forwarding (mcast-af)</td>
<td>The software offers a high level of assurance that the multicast packets are delivered as long as the packet flow from the customer stays within a certain service profile that you define. The software accepts excess traffic, but it applies a tail drop profile to determine if the excess packets are dropped and not forwarded. Two drop probabilities (low and high) are defined for this service class.</td>
</tr>
<tr>
<td>multicast network-control (mcast-nc)</td>
<td>The software delivers packets in this service class with a high priority. (These packets are not delay-sensitive.) Typically, these packets represent routing protocol hello or keep alive messages. Because loss of these packets jeopardizes proper network operation, packet delay is preferable to packet discard for these packets.</td>
</tr>
</tbody>
</table>

The following rules govern queue assignment:

- CoS configurations that specify more queues than the switch can support are not accepted. If you commit such a configuration, the commit fails and a message displays that states the number of queues available.
- All default CoS configurations are based on queue number. The name of the forwarding class that is displayed in the default configuration for a queue number is that of the forwarding class currently associated with that queue.

**Related Documentation**

- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Example: Configuring CoS on EX Series Switches on page 1895
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927
- Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
Understanding CoS Congestion Management

A congestion in a network occurs because of various parameters and some packets must be dropped to avoid congestion and to facilitate easy flow of traffic in the network. On Juniper Networks EX Series Ethernet Switches, class of service (CoS) provides congestion management mechanisms for a switch to drop arriving packets based on certain parameters when a queue is full. Based on the EX Series switch that you are using, packets are dropped depending on the priority of a packet or on both priority and drop probability of a packet.

You can specify parameters at the [edit class-of-service drop-profiles] hierarchy level for dropping packets and reference the parameters in a scheduler configuration.

This topic describes:

- Weighted Tail Drop Congestion Management on page 1875
- Weighted Random Early Detection Congestion Management on page 1876

Weighted Tail Drop Congestion Management

A weighted tail drop (WTD) is a congestion management mechanism for packets to be dropped from the tail of the queue when the queue reaches a certain buffer capacity (that is, the fill level), and hence the name weighted tail drop. The packets that are dropped are based on priority and are those marked with a packet loss priority (PLP) of high. You can configure a WTD profile (a WTD mechanism) usually on edge devices in a network.

**NOTE:** A WTD profile is supported only on the Juniper Networks EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, and EX6200 Ethernet Switches.

When you configure a WTD profile, you are essentially setting the value for queue fullness. The queue fullness represents a percentage of the memory, known as delay-buffer bandwidth, that is used to store packets in relation to the total amount of memory that has been allocated for that specific queue. The delay-buffer bandwidth provides packet buffer space to absorb burst traffic up to the specified duration of delay. When the specified delay buffer becomes full, packets are dropped from the tail of the buffer.

By default, if you do not configure any drop profile, WTD profile is in effect and functions as the primary mechanism for managing congestion.

**NOTE:** The default WTD profile associated with the packets whose PLP is low cannot be modified. You can configure custom drop profile only for those packets whose PLP is high.
Weighted Random Early Detection Congestion Management

In a weighted random early detection (WRED) congestion management mechanism, random packets with a PLP of low or high are gradually dropped (based on drop probability) when the queue reaches a certain buffer capacity (that is, fill level).

NOTE: The WRED mechanism is supported only on Juniper Networks EX4300 standalone switches, EX4300 Virtual Chassis, Juniper Networks EX8200 standalone switches, and EX8200 Virtual Chassis.

Following are the different implementations of WRED:

- Segmented Drop Profile
- Interpolated Drop Profile

From a high level, segmented drop profile is a stair-step-like drop profile, whereas interpolated drop profile is a smoother (curve) drop profile. Figure 23 on page 1877 and Figure 24 on page 1878 show a graphical representation of segmented and interpolated drop profiles. Regardless of the implementation, a drop profile represents a graph where the x-axis represents the percentage of fill level (l) and the y-axis represents the percentage of drop probability (p). The origin (0,0) represents the drop profile in which the drop probability is 0 percent when the queue fullness is 0 percent, and the point (100,100) represents that the drop probability is 100 percent when the queue fullness is 100 percent. Although the formation of graph lines in Figure 23 on page 1877 and Figure 24 on page 1878 is different, the application of the profile is the same. When a packet reaches the head of the queue, a random number between 0 and 100 is calculated. This random number is plotted against the drop profile graph using the current queue fullness of that particular queue. When the random number falls above the graph line, the packet is transmitted. When the number falls below the graph line, the packet is dropped from the network.

The following sections discuss the WRED drop profile implementations and parameters:

- Segmented Drop Profile on page 1876
- Interpolated Drop Profile on page 1877
- Drop Profile Parameters on page 1879

Segmented Drop Profile

In a segmented drop profile configuration, you can define multiple data points for fill level and drop probability. Figure 23 on page 1877 shows a graphical representation of a segmented drop profile.
To create the profile’s graph line, the software begins at the bottom-left corner of the graph, representing a 0 percent fill level and a 0 percent drop probability (that is the point (0,0)). The configuration draws a line directly to the right until it reaches the first defined fill level (that is, 25 percent represented in the graph on the x-axis). The software then continues the line vertically until the first drop probability is reached (that is, 25 percent represented in the graph in the y-axis). This process is repeated for all of the defined fill levels and drop probabilities until the top-right corner of the graph is reached (that is point (100,100) in the graph).

Interpolated Drop Profile

An interpolated drop profile configuration forms a smoother graph line compared to the graph in a segmented drop profile configuration. In this method of congestion management also, a switch uses multiple drop profile values to drop incoming packets to reduce congestion in the output queue.

Following are interpolated drop profile configurations on EX Series switches:

- Interpolated Drop Profile Configuration on EX Series Switches Except EX4300 Switches on page 1877
- Interpolated Drop Profile Configuration on EX4300 Switches on page 1878

Interpolated Drop Profile Configuration on EX Series Switches Except EX4300 Switches

An interpolated drop profile on all EX Series switches except EX4300 switches automatically generates 64 pairs of data points on the graph beginning at (0, 0) and
Figure 24 on page 1878 shows a graphical representation of an interpolated drop profile.

**Figure 24: Graphical Representation of an Interpolated Drop Profile on EX Series Switches Except EX4300 Switches**

**Interpolated Drop Profile Configuration on EX4300 Switches**

On EX4300 switches, you can set two queue fill levels and two drop probabilities in each drop profile. The two fill levels and the two drop probabilities create two pairs of values. The first fill level and the first drop probability create one value pair and the second fill level and the second drop probability create the second value pair.

**NOTE:** You can configure a maximum of 64 drop profiles on EX4300 switches.

The first fill level value specifies the percentage of queue fullness at which packets begin to drop, known as the drop start point. Until the queue reaches this level of fullness, no packets are dropped. The second fill level value specifies the percentage of queue fullness at which all packets are dropped, known as the drop end point.

The first drop probability value is always 0 (zero). This pairs with the drop start point and specifies that until the queue fullness level reaches the first fill level, no packets drop. When the queue fullness exceeds the drop start point, packets begin to drop until the queue exceeds the second fill level, when all packets drop. The second drop probability value, known as the maximum drop rate, specifies the likelihood of dropping packets.
when the queue fullness reaches the drop end point. As the queue fills from the drop start point to the drop end point, packets drop in a smooth, linear pattern (called an interpolated graph) as shown in Figure 25 on page 1879. After the drop end point, all packets drop.

**Figure 25: Tail-Drop Profile Packet Drop on EX4300 Switches**

The thick line in Figure 25 on page 1879 shows the packet drop characteristics for a sample tail drop profile. At the drop start point, the queue reaches a fill level of 30 percent. At the drop end point, the queue fill level reaches 50 percent, and the maximum drop rate is 80 percent.

No packets drop until the queue fill level reaches the drop start point of 30 percent. When the queue reaches the 30 percent fill level, packets begin to drop. As the queue fills, the percentage of packets dropped increases in a linear fashion. When the queue fills to the drop end point of 50 percent, the rate of packet drop has increased to the maximum drop rate of 80 percent. When the queue fill level exceeds the drop end point of 50 percent, all of the packets drop until the queue fill level drops below 50 percent.

**Drop Profile Parameters**

You can specify the following two values in drop profile configuration:

- **Fill level**—The queue fullness value, which represents a percentage of the memory used to store packets in relation to the total amount of memory allocated to the queue.
- **Drop probability**—The percentage value that corresponds to the likelihood that an individual packet is dropped.

**Related Documentation**

- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Example: Configuring CoS on EX Series Switches on page 1895
- Configuring CoS Congestion Management (CLI Procedure) on page 1935
Understanding CoS Schedulers

You use class-of-service (CoS) schedulers to define the properties of output queues on Juniper Networks EX Series Ethernet Switches. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the drop profiles associated with the queue.

You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the queues, packet schedulers, and tail drop processes that operate according to this mapping.

This topic describes:

- Default Schedulers on page 1880
- Excess Rate on page 1881
- Transmission Rate on page 1881
- Scheduler Buffer Size on page 1881
- Priority Scheduling on page 1882
- Scheduler Drop-Profile Maps on page 1883
- Scheduler Maps on page 1883

Default Schedulers

Each forwarding class has an associated scheduler priority. On EX Series switches other than Juniper Networks EX8200 and Juniper Networks EX4300 Ethernet Switches, only two forwarding classes—best-effort (queue 0) and network-control (queue 7)—are used in the default configuration. On EX8200 switches three forwarding classes—best-effort (queue 0), multicast best-effort (queue 2), and network-control (queue 7)—are used in the default configuration.

On EX Series switches other than EX8200 and EX4300 switches, by default, the best-effort forwarding class (queue 0) receives 95 percent of the bandwidth and the buffer space for the output link, and the network-control forwarding class (queue 7) receives 5 percent. The default drop profile causes the buffer to fill completely and then to discard all incoming packets until it has free space. On EX8200 switches, by default, the best-effort forwarding class (queue 0) receives 75 percent of the bandwidth, the multicast best-effort forwarding class (queue 2) receives 20 percent, and the network-control forwarding class (queue 7) receives 5 percent of the bandwidth and buffer space for the output link.

On EX4300 switches, four forwarding classes—best-effort (queue 0), multicast best-effort (queue 8), network-control (queue 3), and multicast network-control (queue 11)—are used in the default configuration. By default, all the multicast traffic flows through the multicast best-effort queue. EX4300 switches support 12 queues (0–11), and the default scheduler transmission rates for queues 0 through 11 are 75, 0, 0, 5, 0, 0, 0, 0, 15, 0, 0 and 5 percent, respectively, of the total available bandwidth.

On EX Series switches other than EX4300 switches, the expedited-forwarding (queue 5) and assured-forwarding (queue 1) classes have no scheduler because no resources are
assigned to queue 5 or queue 1, by default. However, you can manually configure resources
to be assigned to the expedited-forwarding and assured-forwarding classes. On EX4300
switches, the expedited-forwarding (queue 1) and assured-forwarding (queue 2) classes
have no scheduler because no resources are assigned to queue 1 or queue 2, by default.
However, you can manually configure resources to be assigned to the
expedited-forwarding and assured-forwarding classes.

Also by default, any queue can exceed the assigned bandwidth if additional bandwidth
is available from other queues. When a forwarding class does not fully use the allocated
transmission bandwidth, the remaining bandwidth can be used by other forwarding
classes if they have a traffic load that exceeds their allocated bandwidth.

**Excess Rate**

Excess rate traffic determines the percentage of the excess bandwidth to share when a
queue receives traffic in excess of its bandwidth allocation. By default, the excess
bandwidth is shared in the ratio of the transmit rates. You can control this distribution
by configuring the `excess-rate` statement at the [edit class-of-service schedulers
scheduler-name] hierarchy. You can specify the excess rate sharing in percentage.

**Transmission Rate**

Transmission-rate control determines the actual traffic bandwidth for each forwarding
class you configure. The transmission rate is specified in bits per second. Each queue is
allocated some portion of the bandwidth of the interface. This bandwidth can be a fixed
value, such as 1 megabit per second (Mbps), a percentage of the total available bandwidth,
or the rest of the available bandwidth. In case of congestion, the configured transmission
rate is guaranteed for the queue. Transmission-rate control allows you to ensure that
each queue receives the bandwidth appropriate for its level of service.

**Scheduler Buffer Size**

To control congestion at the output stage, you can configure the delay-buffer bandwidth
by using the `buffer-size` configuration statement. The delay-buffer bandwidth provides
packet buffer space to absorb burst traffic up to the specified duration of delay. When
the specified delay buffer becomes full, packets with 100 percent drop probability are
dropped from the tail of the buffer.

On EX Series switches other than EX8200 and EX4300 switches, the default scheduler
transmission rates for queues 0 through 7 are 95, 0, 0, 0, 0, 0, 0, and 5 percent,
respectively, of the total available bandwidth. The default buffer-size percentages for
queues 0 through 7 are 95, 0, 0, 0, 0, 0, 0, and 5 percent, respectively, of the total available
buffer. On EX8200 switches, the default scheduler transmission rates for queues 0
through 7 are 75, 0, 20, 0, 0, 0, 0, and 5 percent, respectively, of the total available
bandwidth, and the default buffer-size percentages for queues 0 through 7 are 75, 0, 20,
0, 0, 0, 0, and 5 percent, respectively, of the total available buffer. On EX4300 switches,
the default scheduler transmission rates for queues 0 through 11 are 75, 0, 0, 5, 0, 0, 0,
0, 15, 0, 0 and 5 percent, respectively, of the total available buffer. On EX4300 switches,
the default buffer-size percentages for queues 0 through 11 are 75, 0, 0, 5, 0, 0, 0, 0, 15,
0, 0 and 5 percent, respectively, of the total available buffer.
For each scheduler on EX Series switches other than EX8200 switches, you can configure the buffer size as one of the following:

- The exact buffer size.
- A percentage of the total buffer.
- The remaining buffer available. The remainder is the buffer percentage that is not assigned to other queues. For example, if you assign 40 percent of the delay buffer to queue 0, allow queue 2 to keep the default allotment of 20 percent, allow queue 7 to keep the default allotment of 5 percent, and assign the remainder to queue 3, then queue 3 uses 35 percent of the delay buffer.

On EX8200 switches, you can configure the buffer size as a temporal value (in microseconds), percentage of the total buffer, or the remaining buffer available. You can configure the buffer size as a temporal value on Juniper Networks EX4200 and EX4300 Ethernet Switches also.

When you configure buffer size as a temporal value on EX4200 switches, if sufficient buffer size is not available in the shared pool, an error message is logged in the system log (syslog) file and the default profile is applied to the interface. After the temporal buffer space is allocated successfully, if the shared buffer size is less than the current value (which was set using the `set class-of-service shared-buffer percent value` command), the new reduced value must be greater than a sum of the existing reserved temporal buffer size and the required minimum buffer size. Otherwise, the modification to the shared-buffer configuration fails and an error message is logged in the system log.

**Priority Scheduling**

Priority scheduling determines the order in which an interface transmits traffic from queues, thus ensuring that queues containing important traffic are provided faster access.

Priority scheduling is accomplished through a procedure in which the scheduler examines the priority of the queue. Juniper Networks Junos operating system (Junos OS) supports two levels of transmission priority:

- **Low**—The scheduler determines whether the individual queue is within its defined bandwidth profile or not. This binary decision, which is re-evaluated on a regular time cycle, involves comparing the amount of data transmitted by the queue against the bandwidth allocated to it by the scheduler. If the transmitted amount is less than the allocated amount, the queue is considered to be in profile. A queue is out of profile when the amount of traffic that it transmits is larger than the queue’s allocated limit. An out-of-profile queue is transmitted only if bandwidth is available. Otherwise, it is buffered.

- **Strict-high**—A strict-high priority queue receives preferential treatment over a low-priority queue. Unlimited bandwidth is assigned to a strict-high priority queue. On EX Series switches other than EX4300 switches, a queue from a set of queues is selected based on the shaped deficit weighted round robin (SDWRR) algorithm, which operates within the set. On EX4300 switches, the weighted deficit round-robin (WDRR) algorithm is used to select a queue from a set of queues.
the queue number, starting with the highest queue, 7, with decreasing priority down through queue 0. Traffic in higher-numbered queues is always scheduled prior to traffic in lower-numbered queues. In other words, if there are two high-priority queues, the queue with the higher queue number is processed first. On EX4300 switches, you can configure multiple strict-high priority queues on an interface and an EX4300 switch processes these queues in a round-robin method.

Packets in low-priority queues are transmitted only when strict-high priority queues are empty.

**Scheduler Drop-Profile Maps**

Drop-profile maps associate drop profiles with a scheduler. A drop-profile map sets the drop profile for a specific packet loss priority (PLP) and protocol type. The inputs for a drop-profile map are the PLP and the protocol type. The output is the drop profile.

**Scheduler Maps**

A scheduler map associates a specified forwarding class with a scheduler configuration. After configuring a scheduler, you must include it in a scheduler map and then associate the scheduler map with an output interface.

On EX Series switches, if you configure more than the supported number of scheduler maps on a switch or for a port group in a line card, an error is logged in the system log. On any interface in a port group on a line card or on a switch, if you configure a scheduler map that causes the number of scheduler maps for that port group to exceed the maximum number supported, the default scheduler map is bound to that interface. We recommend that you check the system log for errors after the commit operation to verify that you have not configured more than the maximum permitted number of scheduler maps.

**NOTE:** On EX Series switches, you cannot configure a scheduler map on an individual interface that is a member of a link aggregation group (LAG). Instead, you must configure the scheduler map on the LAG itself (that is, on the aggregated Ethernet (ae) interface).

Table 230 on page 1883 shows the number of scheduler maps supported for each port group in a switch or line card.

Table 230: Support for Scheduler Maps on Switches and Line Cards

<table>
<thead>
<tr>
<th>Switch/Line Card</th>
<th>Number of Port Groups</th>
<th>Port Grouping Details</th>
<th>Number of Scheduler Maps Supported for Each Port Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200-C-12T and EX2200-C-12P switches</td>
<td>1</td>
<td>Port 0–11 and 2 uplink ports form a port group.</td>
<td>6</td>
</tr>
<tr>
<td>EX2200-24T and EX2200-24P switches</td>
<td>1</td>
<td>Ports 0–23 and 4 SFP uplink ports form a port group.</td>
<td>5</td>
</tr>
</tbody>
</table>
## Table 230: Support for Scheduler Maps on Switches and Line Cards (continued)

<table>
<thead>
<tr>
<th>Switch/Line Card</th>
<th>Number of Port Groups</th>
<th>Port Grouping Details</th>
<th>Number of Scheduler Maps Supported for Each Port Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200-48T and EX2200-48P switches</td>
<td>2</td>
<td>• Ports 0–23 and SFP uplink ports 0 and 1 form a port group.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ports 24–47 and SFP uplink ports 2 and 3 form a port group.</td>
<td></td>
</tr>
<tr>
<td>EX3200-24T and EX3200-24P switches</td>
<td>1</td>
<td>• Ports 0–23 and the uplink ports form a port group.</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE</strong>: Uplink ports include 2 SFP+ or XFP uplink ports, or 4 SFP uplink ports.</td>
<td></td>
</tr>
<tr>
<td>EX3200-24T and EX3200-24P switches</td>
<td>1</td>
<td>• Ports 0–23 and the uplink ports form a port group.</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE</strong>: Uplink ports include 2 SFP+ or XFP uplink ports or 4 SFP uplink ports.</td>
<td></td>
</tr>
<tr>
<td>EX3200-48T and EX3200-48P switches</td>
<td>2</td>
<td>• Ports 0-23 and 1 SFP+ or XFP uplink port or 4 SFP uplink ports form a port group.</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ports 24–47 and 1 SFP+ or XFP uplink port form a port group.</td>
<td></td>
</tr>
<tr>
<td>EX4200-48T and EX4200-48P switches</td>
<td>3</td>
<td>• Ports 0–23 form a port group.</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ports 24–47 form a port group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 SFP+ or XFP uplink ports or 4 SFP uplink ports form a port group.</td>
<td></td>
</tr>
<tr>
<td>EX4200-24T and EX4200-24P switches</td>
<td>2</td>
<td>• Ports 0–23 form a port group.</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 SFP+ or XFP uplink ports or 4 SFP uplink ports form a port group.</td>
<td></td>
</tr>
<tr>
<td>EX4300-24T and EX4300-24P switches</td>
<td>1</td>
<td>• Ports 0–23 ports, 4 uplink ports, and 4 ports on the real panel form a port group.</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE</strong>: Uplink ports in the front panel contains SFP or SFP+ ports 0–3, and all uplink ports in the rear panel contains QSFP+ ports 0–3.</td>
<td></td>
</tr>
</tbody>
</table>
Table 230: Support for Scheduler Maps on Switches and Line Cards (continued)

<table>
<thead>
<tr>
<th>Switch/Line Card</th>
<th>Number of Port Groups</th>
<th>Port Grouping Details</th>
<th>Number of Scheduler Maps Supported for Each Port Group</th>
</tr>
</thead>
</table>
| EX4300-48T and EX4300-48P switches | 1 | • Ports 0–47, 4 uplink ports, and 4 ports on the real panel form a port group.  
**NOTE:** Uplink ports in the front panel contains SFP or SFP+ ports 0–3, and uplink ports in the rear panel contains QSFP+ ports 0–3. | 64 |
| EX4500-40F switch | 2 | • SFP or SFP+ ports 0–19 and the first SFP or SFP+ port 0–4 form a port group.  
• SFP or SFP+ ports 20–39 and the second SFP or SFP+ uplink port 0–4 form a port group. | 4 |
| EX4550-32F switch | 1 | • SFP or SFP+ ports 0–31 and the uplink ports in the front and rear panels form a port group.  
**NOTE:** Uplink ports in the front panel contains SFP, SFP+, or RJ-45 ports 0–7, and uplink ports in the rear panel contains SFP, SFP+, or RJ-45 ports 0–7. | 5 |
| EX6200-48T (48-port RJ-45) and EX6200-48P (48-port PoE+) line cards | 2 | • Ports 0–23 form a port group.  
• Ports 24–47 form a port group. | 5 |
| EX6200-SRE64-4XS | 1 | SFP+ ports 0–3 form a port group. | 4 |
| EX8200-8XS (8-port SFP+) line card | 4 | • SFP+ ports 0 and 1 form a port group.  
• SFP+ ports 2 and 3 form a port group.  
• SFP+ ports 4 and 5 form a port group.  
• SFP+ ports 6 and 7 form a port group. | 6 |
## Table 230: Support for Scheduler Maps on Switches and Line Cards (continued)

<table>
<thead>
<tr>
<th>Switch/Line Card</th>
<th>Number of Port Groups</th>
<th>Port Grouping Details</th>
<th>Number of Scheduler Maps Supported for Each Port Group</th>
</tr>
</thead>
</table>
| EX8200-40XS (40-port SFP+) line card | 8 | • SFP+ ports 0–4 form a port group.  
• SFP+ ports 5–9 form a port group.  
• SFP+ ports 10–14 form a port group.  
• SFP+ ports 15–19 form a port group.  
• SFP+ ports 20–24 form a port group.  
• SFP+ ports 25–29 form a port group.  
• SFP+ ports 30–34 form a port group.  
• SFP+ ports 35–39 form a port group. | 6 |
| EX8200-48F (48-port SFP) and EX8200-48T (48-port RJ-45) line cards | 2 | • SFP or RJ-45 ports 0–23 form a port group.  
• SFP or RJ-45 ports 24–47 form a port group. | 6 |
| EX8200-2XS-40P (40-port PoE+ with 4-port SFP and 2-port SFP+) line card | 3 | • Ports 0–19 and SFP ports 0 and 1 form a port group.  
• Ports 20–39 and SFP ports 2 and 3 form a port group.  
• 2 SFP+ ports form a port group. | 5 |
| EX8200-2XS-40T (40-port RJ-45 with 4-port SFP and 2-port SFP+) line card | 3 | • Ports 0–19, and SFP ports 0 and 1 form a port group.  
• Ports 20–39 and SFP ports 2 and 3 form a port group.  
• 2 SFP+ ports form a port group. | 5 |
| EX8200-48PL (48-port PoE+ 20 Gbps) and EX8200-48TL (48-port RJ-45 20 Gbps) line cards | 2 | • PoE+ or RJ-45 ports 0–23 form a port group.  
• PoE+ or RJ-45 ports 24–47 form a port group. | 5 |

### Related Documentation
- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929
Understanding CoS Two-Color Marking

Networks police traffic by limiting the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Policing traffic allows you to control the maximum rate of traffic sent or received on an interface and to partition a network into multiple priority levels or classes of service.

Policers require you to apply limits to the traffic flow and set a consequence for packets that exceed these limits—usually a higher loss priority, so that packets exceeding the policer limits are discarded first.

Juniper Networks EX Series Ethernet Switches support a single-rate two-color marking type of policer, which is a simplified version of Single-Rate-Three-Color marking, defined in RFC 2697, A Single Rate Three Color Marker. This type of policer meters traffic based on the configured committed information rate (CIR) and committed burst size (CBS).

The single-rate two-color marker meters traffic and marks incoming packets depending on whether they are smaller than the committed burst size (CBS)—marked green—or exceed it—marked red.

The single-rate two-color marking policer operates in color-blind mode. In this mode, the policer's actions are not affected by any previous marking or metering of the examined packets. In other words, the policer is “blind” to any previous coloring a packet might have had.

Understanding CoS Rewrite Rules

As packets enter or exit a network, edge switches might be required to alter the class-of-service (CoS) settings of the packets. This topic describes how to use rewrite rules to alter the CoS settings. It covers:

This topic covers:

- How Rewrite Rules Work on page 1887
- Default Rewrite Rule on page 1888

How Rewrite Rules Work

Rewrite rules set the value of the CoS bits within a packet's header. Each rewrite rule reads the current forwarding class and loss priority associated with the packet, locates the chosen CoS value from a table, and writes this CoS value into the packet header. For rewrites to occur, rewrite rules must be explicitly assigned to an interface.
NOTE: On EX4300 switches, you cannot configure a rewrite rule for logical interfaces. Each physical interface in a switch can be logically divided into multiple logical interfaces for moving traffic between those logical interfaces.

On EX Series switches except EX4300 switches, you can define rewrite rules for IPv4 and IPv6 traffic to network interfaces, aggregated Ethernet interfaces (also known as link aggregation groups (LAGs)), routed VLAN interfaces (RVIs), Layer 3 interfaces, and Layer 3 VLAN-tagged sub-interfaces. Multiple rewrite rules of different types can be assigned to a single interface.

On EX4300 switches, you can define rewrite rules for IPv4 and IPv6 traffic only to network interfaces, aggregated Ethernet interfaces, and Layer 3 interfaces. You cannot define rewrite rules for IPv4 and IPv6 traffic on integrated routing and bridging (IRB) interfaces, Layer 3 logical interfaces, and Layer 3 VLAN-tagged logical interfaces. Multiple rewrite rules of different types cannot be assigned to a single interface. Therefore, you cannot configure DSCP IPv4 and DSCP IPv6 rewrite rules on the same interface. If you configure a DSCP IPv4 rewrite rule on an interface to rewrite IPv4 traffic, then the same rewrite rule is applied to IPv6 traffic also on that interface, and vice versa.

In effect, the rewrite rule performs the reverse function of the behavior aggregate (BA) classifier, which is used when the packet enters the switch. As the packet leaves the switch, the final CoS action is generally the application of a rewrite rule.

You configure rewrite rules to alter CoS values in outgoing packets on the outbound interfaces of an edge switch to meet the policies of a targeted peer. This allows the downstream switch in a neighboring network to classify each packet into the appropriate service group.

NOTE: When an IP precedence rewrite rule is active, bits 3, 4, and 5 of the type-of-service (ToS) byte are always reset to zero when code points are rewritten.

Default Rewrite Rule

To define a rewrite rule on an interface, you can either create your own rewrite rule and enable it on the interface or enable a default rewrite rule. See “Defining CoS Rewrite Rules (CLI Procedure)” on page 1939.

Table 231 on page 1889 shows the default rewrite-rule mappings. These are based on the default bit definitions of Differentiated Services code point (DSCP), IEEE 802.1p, and IP precedence values and the default forwarding classes. You can configure multiple CoS rewrite rules for DSCP, IP precedence and IEEE 802.1p.

NOTE: By default, rewrite rules are not assigned to an interface. You must explicitly assign a user-defined or system-defined rewrite rule to an interface for the rewrites to occur.
When the CoS values of a packet match the forwarding class and packet-loss-priority (PLP) values, the switch rewrites markings on the packet based on the rewrite table.

### Table 231: Default Packet Header Rewrite Mappings

<table>
<thead>
<tr>
<th>Map from Forwarding Class</th>
<th>PLP Value</th>
<th>Map to DSCP/IEEE 802.1p/IP Precedence Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>ef</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>high</td>
<td>ef</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>low</td>
<td>af11</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>high</td>
<td>af12 (DSCP)</td>
</tr>
<tr>
<td>best-effort</td>
<td>low</td>
<td>be</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>be</td>
</tr>
<tr>
<td>network-control</td>
<td>low</td>
<td>nc1/cs6</td>
</tr>
<tr>
<td>network-control</td>
<td>high</td>
<td>nc2/cs7</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Rewrite Rules (CLI Procedure) on page 1939
- Defining CoS Rewrite Rules (J-Web Procedure) on page 1940

### Understanding Port Shaping and Queue Shaping for CoS on EX Series Switches

When the amount of traffic on a switch's network exceeds the maximum bandwidth, packets are lost because of congestion in the network. The excess traffic in the network must be handled carefully to ensure minimum or no data loss in the network. A class-of-service (CoS) configuration includes several parameters that classify traffic into different queues and also define packet loss priorities (PLPs) to ensure smooth transmission of data in the network. You can use these configuration parameters to control or shape traffic for a specific port on a switch or for a specific CoS queue. While port shaping defines the maximum bandwidth allocated to an interface, queue shaping defines a limit on excess-bandwidth usage for each queue.

This topic covers:
- Port Shaping on page 1890
- Queue Shaping on page 1890
Port Shaping

Port shaping enables you to shape the aggregate traffic through a port or channel to a rate that is less than the line rate. You can configure interfaces to shape traffic based on the rate-limited bandwidth of the total interface bandwidth. This allows you to shape the output of the interface so that the interface transmits less traffic than it is capable of transmitting. For port shaping, you can specify shaping rate as the peak rate at which traffic can pass through the interface. You can specify rate as a value in bits per second (bps) either as a decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000) and the value can range from 1000 through 160,000,000,000 bps.

By default, shaping is not configured on an interface. If you do not configure a shaping rate on an interface, the default shaping rate is 100 percent, which is the equivalent to no shaping configured for that interface.

On EX Series switches except EX4300 switches, when you configure a shaping rate on an aggregated Ethernet (ae) interface, all members of the ae interface are shaped at the configured shaping rate. For example, consider an interface ae0 that consists of three interfaces: ge-0/0/0, ge-0/0/1, and ge-0/0/2. If a shaping rate of X Mpbs is configured on ae0, traffic at the rate of X Mpbs flows through each of the three interfaces. Therefore, the total traffic flowing through ae0 would be at the rate of 3X Mbps. On EX4300 switches, when you configure a shaping rate on an ae interface, the traffic is equally divided among the members of the ae interface.

Queue Shaping

Queue shaping throttles the rate at which queues transmit packets. For example, using queue shaping, you can rate-limit a strict-priority queue so that the strict-priority queue does not lock out (or starve) low-priority queues. Similarly, for any queue, you can configure queue shaping.

You can specify queue shaping as the maximum rate at which traffic can pass through the queue or as a percentage of the available bandwidth. On EX Series switches except EX4300 switches, you can specify the rate as a value between 3200 and 160,000,000,000 bps and the percentage as a value from 0 to 100 percent. On EX4300 switches, you can specify the rate as a value between 8000 and 160,000,000,000 bps and the percentage as a value from 0 to 100 percent.

Related Documentation

- Understanding CoS Schedulers on page 1880
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929

Understanding Junos OS EZQoS for CoS Configurations on EX Series Switches

Junos operating system (Junos OS) EZQoS on Juniper Networks EX Series Ethernet Switches eliminates the complexities involved in configuring class of service (CoS) across the network. EZQoS offers templates for key traffic classes.

Junos OS CoS allows you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. You can use CoS to ensure that different types
of traffic (voice, video, and data) get the bandwidth and consideration they need to meet user expectations and business objectives.

Configuring CoS requires careful consideration of your service needs and thorough planning and design to ensure consistency across all switches in a CoS domain. To configure CoS manually, you must define and fine-tune all CoS components such as classifiers, rewrite rules, forwarding classes, schedulers, and scheduler-maps and then apply these components to the interfaces. Therefore, configuring CoS can be a fairly complex and time-consuming task.

EZQoS works by automatically assigning preconfigured values to all CoS parameters based on the typical application requirements. These preconfigured values are stored in a template with a unique name. You can change the preconfigured values of these parameters to suit your particular application needs.

For using EZQoS, you must identify which switch ports are being used for a specific application (such as VoIP, video, and data) and manually apply the corresponding application-specific EZQoS template to these switch ports.

**NOTE:** Currently, we provide an EZQoS template for configuring CoS for VoIP.

**NOTE:** We recommend that you do not use the term EZQoS for defining a classifier.

**Related Documentation**

- Junos OS CoS for EX Series Switches Overview on page 1862
- Configuring Junos OS EZQoS for CoS (CLI Procedure) on page 1944

**Understanding CoS Queues on EX8200 Line Cards That Include Oversubscribed Ports**

Some line cards available for Juniper Networks EX8200 Ethernet Switches include oversubscribed ports that are combined in logical port groups that share bandwidth. These oversubscribed ports handle traffic differently than ports that provide continuous line-rate bandwidth. You might need to configure CoS queues differently for oversubscribed ports than for line-rate ports.

This topic describes:

- Oversubscribed Ports on Line Cards on page 1891
- EX8200 Line Cards That Include Oversubscribed Ports on page 1892
- Ingress Queueing on page 1892
- Egress Queues on page 1894

**Oversubscribed Ports on Line Cards**

Oversubscribed ports on a line card are grouped into logical port groups. A port group collectively supports a certain bandwidth.
An EX8200 switch supports different line cards that provide line-rate and oversubscribed ports. Based on your requirement, you can choose the appropriate line card for an EX8200 switch. Line cards are field-replaceable units (FRUs) that can be installed in the line card slots in an EX8200 switch. In a line-rate EX8200 line card, each port in the line card supports the same amount of bandwidth and a single port can utilize that complete bandwidth. In an oversubscribed line card, a group of ports collectively support a certain total bandwidth and each port in that group can use either a portion or all of the available bandwidth. However, the total utilization of bandwidth by the ports in the group cannot exceed the bandwidth available for that group.

Because the port groups share bandwidth, class-of-service (CoS) ingress and egress queues are handled differently for these shared-bandwidth ports in logical port groups than they are for ports that individually support line-rate bandwidth. Some EX8200 line cards combine both port types, those that share bandwidth across port groups and those that individually support line-rate bandwidth.

**EX8200 Line Cards That Include Oversubscribed Ports**

Table 232 on page 1892 lists EX8200 line cards that include oversubscribed ports in logical port groups.

### Table 232: EX8200 Line Cards That Include Oversubscribed Ports

<table>
<thead>
<tr>
<th>Line Card Model</th>
<th>Name</th>
<th>Number of Oversubscribed Ports/Port Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX8200-40XS</td>
<td>40-port SFP+</td>
<td>40 oversubscribed 10-gigabit SFP+ ports</td>
</tr>
<tr>
<td>EX8200-2XS-40P</td>
<td>40-port PoE+ with 4-port SFP and 2-port SFP+</td>
<td>40 oversubscribed 10/100/1000 Gigabit Ethernet ports with RJ-45 connectors, four small form-factor pluggable (SFP) ports (in which you can install 1-gigabit SFP transceivers) and two SFP+ ports</td>
</tr>
<tr>
<td>EX8200-2XS-40T</td>
<td>40-port RJ-45 with 4-port SFP and 2-port SFP+</td>
<td>40 oversubscribed 10/100/1000 Gigabit Ethernet ports with RJ-45 connectors, four SFP ports (in which you can install 1-gigabit small form-factor pluggable (SFP) transceivers) and two SFP+ ports</td>
</tr>
<tr>
<td>EX8200-48PL</td>
<td>48-port PoE+ 20 Gbps</td>
<td>48 oversubscribed 10/100/1000 Gigabit Ethernet ports with RJ-45 connectors</td>
</tr>
<tr>
<td>EX8200-48TL</td>
<td>48-port RJ-45 20 Gbps</td>
<td>48 oversubscribed 10/100/1000 Gigabit Ethernet ports with RJ-45 connectors</td>
</tr>
</tbody>
</table>

**Ingress Queueing**

Classification of packets occurs in two phases for the oversubscribed ports in the port groups.

- Preclassification of Packets and Port Ingress Queueing on page 1893
- Full Classification of Packets and Fabric Ingress Queueing on page 1893
**Preclassification of Packets and Port Ingress Queuing**

Packets entering ports are forwarded to one of the ingress queues. The ingress queues schedule traffic from ports into the Packet Forwarding Engine.

The ingress queues are:

- **Low-priority queue**—Each interface in the line card has one low-priority queue. Traffic on these queues is scheduled using the shaped deficit weighted round-robin (SDWRR) algorithm, with each interface's queue having equal weight. On EX4300 switches, traffic is queued using the weighted deficit round-robin (WDRR) algorithm.

- **High-priority queue**—A set of interfaces in the line card shares a single high-priority queue. Traffic on this queue is scheduled by strict-high priority. The switch always sends critical network control packets on the high-priority queue.

- **Line-rate priority queue**—The packets entering line-rate ports are forwarded to this queue. Traffic on this queue is scheduled by strict priority and is always given higher priority than the traffic on the high-priority queue. This queue is used only in the following oversubscribed lines cards for an EX8200 switch:
  - EX8200-2XS-40P
  - EX8200-2XS-40T

For the purpose of port ingress queuing on oversubscribed ports, packets are classified only by behavior aggregate (BA) classification. To control the ingress queue (high priority or low priority) to which packets are sent, configure a BA classifier on the physical port and specify switch fabric priorities for the forwarding classes. On EX8200 switches, fabric priority determines the priority of packets ingressing the switch fabric. For the EX8200-40XS line card, fabric priority also determines the priority of packets ingressing the port group.

By default, the fabric priority for all forwarding classes is low. To direct packets belonging to a forwarding class to the high-priority ingress queue, set the fabric priority to high for that class.

Critical network-control packets and line-rate packets are handled differently from other packets. Instead of using the BA classifier to classify critical network-control packets, the switch always sends critical network packets to the high-priority queue. The line-rate packets are always sent to the line-rate priority queue. This difference in handling of network-control packets and line-rate packets ensures that these packets are not dropped because of congestion on the shared-bandwidth ports.

**Full Classification of Packets and Fabric Ingress Queuing**

When packets (apart from line-rate and critical network-control packets) from an oversubscribed port reach the Packet Forwarding Engine, it performs full packet classification, along with other actions, such as multifield (MF) classification, traffic policing, and storm control. It then schedules and queues the packets for ingressing the fabric. The fabric priority associated with the forwarding class determines whether packets are sent to the low priority or high-priority ingress queues.
Egress Queues

On EX Series switches except EX4300 switches, each interface supports eight egress CoS queues. You can map up to 16 forwarding classes to these queues. An EX4300 switch interface supports 12 egress CoS queues.

In the EX8200–40XS line card, all interfaces in a port group share a single set of eight egress queues at the Packet Forwarding Engine. Egress traffic is fanned out from the Packet Forwarding Engine queues to the corresponding queues for the individual ports. For this reason, the interfaces in a port group must share the same scheduler map configuration. If you configure different scheduler map configurations for the different interfaces in a port group, an error is logged in the system log and the default scheduler map is used for all ports in the port group.

Related Documentation
- Understanding Junos OS CoS Components for EX Series Switches on page 1863
- Understanding CoS Schedulers on page 1880
- Understanding CoS Forwarding Classes
- Example: Configuring CoS on EX Series Switches on page 1895
- Configuring CoS Traffic Classification for Ingress Queuing on Oversubscribed Ports on EX8200 Line Cards (CLI Procedure) on page 1945
CHAPTER 32

Configuration

- Configuration Examples on page 1895
- Configuration Tasks on page 1919
- Configuration Statements on page 1946

Configuration Examples

- Example: Configuring CoS on EX Series Switches on page 1895

Example: Configuring CoS on EX Series Switches

Configure class of service (CoS) on your switch to manage traffic so that when the network experiences congestion and delay, critical applications are protected. Using CoS, you can divide traffic on your switch into classes and provide various levels of throughput and packet loss. This is especially important for traffic that is sensitive to jitter and delay, such as voice traffic.

This example shows how to configure CoS on a single EX Series switch in the network.

- Requirements on page 1895
- Overview and Topology on page 1895
- Configuration on page 1898
- Verification on page 1908

Requirements

This example uses the following hardware and software components:

- EX3200, EX4200, or EX4300 switches
- Junos OS Release 9.0 or later for EX Series switches

Overview and Topology

This example uses the topology shown in Figure 26 on page 1896.
The topology for this configuration example consists of EX3200 and EX4200 switches at the access layer.

The EX Series access switch is configured to support VLAN membership. Interfaces ge-0/0/0 and ge-0/0/1 are assigned to the voice VLAN (voice-vlan) for two VoIP phones. Switch port ge-0/0/2 is assigned to the camera VLAN (camera-vlan) for the surveillance camera. Switch ports ge-0/0/3, ge-0/0/4, ge-0/0/5, and ge-0/0/6 are assigned to the server VLAN (server-vlan) for the servers hosting various applications such as those provided by Citrix, Microsoft, Oracle, and SAP.

Table 233 on page 1897 shows the VLAN configuration components.
Table 233: Configuration Components: VLANs

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>VLAN ID</th>
<th>VLAN Subnet and Available IP Addresses</th>
<th>VLAN Description</th>
</tr>
</thead>
</table>
| voice-vlan | 10      | 192.168.1.0/32
192.168.1.1 through 192.168.1.11
192.168.1.12 is the subnet’s broadcast address. | Voice VLAN used for employee VoIP communication. |
| camera-vlan| 20      | 192.168.1.13/32
192.168.1.14 through 192.168.1.20
192.168.1.21 is the subnet’s broadcast address. | VLAN for the surveillance cameras. |
| server-vlan| 30      | 192.168.1.22/32
192.168.1.23 through 192.168.1.35
192.168.1.36 is the subnet’s broadcast address. | VLAN for the servers hosting enterprise applications. |

PoE-capable ports on EX Series switches support Power over Ethernet (PoE) to provide both network connectivity and power for VoIP telephones connecting to the ports. Table 234 on page 1897 shows the switch interfaces that are assigned to the VLANs and the IP addresses for devices connected to the switch ports on a 48-port switch, all ports of which are PoE-capable.

Table 234: Configuration Components: Switch Ports on a 48-Port All-PoE Switch

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>VLAN Membership</th>
<th>IP Addresses</th>
<th>Port Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0, ge-0/0/1</td>
<td>voice-vlan</td>
<td>192.168.1.1 through 192.168.1.2</td>
<td>Two VoIP telephones.</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>camera-vlan</td>
<td>192.168.1.14</td>
<td>Surveillance camera.</td>
</tr>
<tr>
<td>ge-0/0/3, ge-0/0/4, ge-0/0/5, ge-0/0/6</td>
<td>server-vlan</td>
<td>192.168.1.23 through 192.168.1.26</td>
<td>Four servers hosting applications such as those provided by Citrix, Microsoft, Oracle, and SAP.</td>
</tr>
</tbody>
</table>

**NOTE:** This example shows how to configure CoS on a standalone EX Series switch. This example does not consider across-the-network applications of CoS in which you might implement different configurations on ingress and egress switches to provide differentiated treatment to different classes across a set of nodes in a network.
To quickly configure CoS, copy the following commands and paste them into the switch terminal window:

```
[edit]
set class-of-service forwarding-classes class app queue-num 5
set class-of-service forwarding-classes class mail queue-num 1
set class-of-service forwarding-classes class db queue-num 2
set class-of-service forwarding-classes class erp queue-num 3
set class-of-service forwarding-classes class video queue-num 4
set class-of-service forwarding-classes class best-effort queue-num 0
set class-of-service forwarding-classes class voice queue-num 6
set class-of-service forwarding-classes class network-control queue-num 7
set firewall family ethernet-switching filter voip_class term voip from source-address 192.168.1.1/32
set firewall family ethernet-switching filter voip_class term voip from source-address 192.168.1.2/32
set firewall family ethernet-switching filter voip_class term voip from protocol udp
set firewall family ethernet-switching filter voip_class term voip from source-port 2698
set firewall family ethernet-switching filter voip_class term voip then forwarding-class voice
loss-priority low
set firewall family ethernet-switching filter voip_class term network_control from precedence
[net-control internet-control]
set firewall family ethernet-switching filter voip_class term network_control then forwarding-class
network-control loss-priority low
set firewall family ethernet-switching filter voip_class term best_effort_traffic then
forwarding-class best-effort loss-priority low
set interfaces ge-0/0/0 description phone1–voip-ingress-port
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input voip_class
set class-of-service interfaces ge-0/0/0 shaping-rate 100m
set interfaces ge-0/0/0/1 description phone2–voip-ingress-port
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input voip_class
set firewall family ethernet-switching filter video_class term video from source-address
192.168.1.14/32
set firewall family ethernet-switching filter video_class term video from protocol udp
set firewall family ethernet-switching filter video_class term video from source-port 2979
set firewall family ethernet-switching filter video_class term video then forwarding-class video
loss-priority low
set firewall family ethernet-switching filter video_class term network_control from precedence
[net-control internet-control]
set firewall family ethernet-switching filter video_class term network_control then forwarding-class
network-control loss-priority low
set firewall family ethernet-switching filter video_class term best_effort_traffic then
forwarding-class best-effort loss-priority low
set interfaces ge-0/0/2 description video-ingress-port
set interfaces ge-0/0/2 unit 0 family ethernet-switching filter input video_class
set firewall family ethernet-switching filter app_class term app from source-address
192.168.1.23/32
set firewall family ethernet-switching filter app_class term app from protocol tcp
set firewall family ethernet-switching filter app_class term app from source-port [1494 2512 2513
2598 2897]
set firewall family ethernet-switching filter app_class term app then forwarding-class app
loss-priority low
set firewall family ethernet-switching filter app_class term mail from source-address
192.168.1.24/32
set firewall family ethernet-switching filter app_class term mail from protocol tcp
set firewall family ethernet-switching filter app_class term mail from source-port [25143 389
691 993 3268 3269]
set firewall family ethernet-switching filter app_class term mail then forwarding-class mail
loss-priority low
```
set firewall family ethernet-switching filter app_class term db from source-address 192.168.1.25/32
set firewall family ethernet-switching filter app_class term db from protocol tcp
set firewall family ethernet-switching filter app_class term db from source-port [1521 1525 1527
1571 1810 2481]
set firewall family ethernet-switching filter app_class term db then forwarding-class db loss-priority
low
set firewall family ethernet-switching filter app_class term erp from source-address 192.168.1.26/32
set firewall family ethernet-switching filter app_class term erp from protocol tcp
set firewall family ethernet-switching filter app_class term erp from source-port [3200 3300
3301 3600]
set firewall family ethernet-switching filter app_class term erp then forwarding-class erp
loss-priority low
set firewall family ethernet-switching filter app_class term network_control from precedence
[net-control internet-control]
set firewall family ethernet-switching filter app_class term network_control then forwarding-class
network-control loss-priority low
set firewall family ethernet-switching filter app_class term best_effort_traffic then forwarding-class
best-effort loss-priority low
set interfaces ge-0/0/3 unit 0 family ethernet-switching filter input app_class
set interfaces ge-0/0/4 unit 0 family ethernet-switching filter input app_class
set interfaces ge-0/0/5 unit 0 family ethernet-switching filter input app_class
set interfaces ge-0/0/6 unit 0 family ethernet-switching filter input app_class
set class-of-service schedulers voice-sched buffer-size percent 10
set class-of-service schedulers voice-sched transmit-rate percent 10
set class-of-service schedulers video-sched buffer-size percent 15
set class-of-service schedulers video-sched transmit-rate percent 10
set class-of-service schedulers app-sched buffer-size percent 10
set class-of-service schedulers app-sched priority low
set class-of-service schedulers app-sched transmit-rate percent 10
set class-of-service schedulers mail-sched buffer-size percent 5
set class-of-service schedulers mail-sched priority low
set class-of-service schedulers mail-sched transmit-rate percent 5
set class-of-service schedulers db-sched buffer-size percent 10
set class-of-service schedulers db-sched priority low
set class-of-service schedulers db-sched transmit-rate percent 10
set class-of-service schedulers erp-sched buffer-size percent 10
set class-of-service schedulers erp-sched priority low
set class-of-service schedulers erp-sched transmit-rate percent 10
set class-of-service schedulers nc-sched buffer-size percent 5
set class-of-service schedulers nc-sched priority strict-high
set class-of-service schedulers nc-sched transmit-rate percent 5
set class-of-service schedulers be-sched buffer-size percent 35
set class-of-service schedulers be-sched priority low
set class-of-service schedulers be-sched transmit-rate percent 35
set class-of-service scheduler-maps ethernet-cos-map forwarding-class voice scheduler
voice-sched
set class-of-service scheduler-maps ethernet-cos-map forwarding-class video scheduler
video-sched
set class-of-service scheduler-maps ethernet-cos-map forwarding-class app scheduler app-sched
set class-of-service scheduler-maps ethernet-cos-map forwarding-class mail scheduler mail-sched
set class-of-service scheduler-maps ethernet-cos-map forwarding-class db scheduler db-sched
set class-of-service scheduler-maps ethernet-cos-map forwarding-class erp scheduler erp-sched
set class-of-service scheduler-maps ethernet-cos-map forwarding-class network-control
scheduler nc-sched
set class-of-service scheduler-maps ethernet-cos-map forwarding-class best-effort scheduler
be-sched
set class-of-service interfaces ge-0/0/20 scheduler-map ethernet-cos-map
set class-of-service schedulers voice-sched-queue-shap shaping-rate 30m
Step-by-Step Procedure

To configure and apply CoS:

1. Configure one-to-one mappings between eight forwarding classes and eight queues:

   ```
   [edit class-of-service]
   user@switch# set forwarding-classes class app queue-num 5
   user@switch# set forwarding-classes class mail queue-num 1
   user@switch# set forwarding-classes class db queue-num 2
   user@switch# set forwarding-classes class erp queue-num 3
   user@switch# set forwarding-classes class video queue-num 4
   user@switch# set forwarding-classes class best-effort queue-num 0
   user@switch# set forwarding-classes class voice queue-num 6
   user@switch# set forwarding-classes class network-control queue-num 7
   ```

2. Define the firewall filter `voip_class` to classify the VoIP traffic:

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter voip_class
   ```

3. Define the term `voip`:

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter voip_class term voip from source-address 192.168.1.1/32
   user@switch# set family ethernet-switching filter voip_class term voip from source-address 192.168.1.2/32
   ```

4. Define the term `network_control` (for the `voip_class` filter):

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter voip_class term network_control from precedence [net-control internet-control]
   user@switch# set family ethernet-switching filter voip_class term network_control then forwarding-class network-control loss-priority low
   ```

5. Define the term `best_effort_traffic` with no match conditions (for the `voip_class` filter):

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter voip_class term best_effort_traffic then forwarding-class best-effort loss-priority low
   ```

6. Apply the firewall filter `voip_class` as an input filter to the interfaces for the VoIP phones:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/0 description phone1-voip-ingress-port
   user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input voip_class
   user@switch# set ge-0/0/1 description phone2-voip-ingress-port
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input voip_class
   ```

7. Apply port shaping on the interface ge-0/0/0:

   ```
   [edit]
   user@switch# set class-of-service interfaces ge-0/0/0 shaping-rate 100m
   ```

8. Define the firewall filter `video_class` to classify the video traffic:

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter video_class
   ```
9. Define the term video:

```
[edit firewall]
user@switch# set family ethernet-switching filter video_class term video from source-address 192.168.1.14/32
user@switch# set family ethernet-switching filter video_class term video protocol udp
user@switch# set family ethernet-switching filter video_class term video source-port 2979
user@switch# set family ethernet-switching filter video_class term video then forwarding-class video loss-priority low
```

10. Define the term network_control (for the video_class filter):

```
[edit firewall]
user@switch# set family ethernet-switching filter video_class term network_control from precedence [net-control internet-control]
user@switch# set family ethernet-switching filter video_class term network_control then forwarding-class network-control loss-priority low
```

11. Define the term best_effort_traffic with no match conditions (for the video_class filter):

```
[edit firewall]
user@switch# set family ethernet-switching filter video_class term best_effort_traffic then forwarding-class best-effort loss-priority low
```

12. Apply the firewall filter video_class as an input filter to the interface for the surveillance camera:

```
[edit interfaces]
user@switch# set ge-0/0/2 description video-ingress-port
user@switch# set ge-0/0/2 unit 0 family ethernet-switching filter input video_class
```

13. Define the firewall filter app_class to classify the application server traffic:

```
[edit firewall]
user@switch# set family ethernet-switching filter app_class
```

14. Define the term app (for the app_class filter):

```
[edit firewall]
user@switch# set family ethernet-switching filter app_class term app from source-address 192.168.1.23/32
user@switch# set family ethernet-switching filter app_class term app protocol tcp
user@switch# set family ethernet-switching filter app_class term app source-port [1494 2512 2513 2598 2897]
user@switch# set family ethernet-switching filter app_class term app then forwarding-class app loss-priority low
```

15. Define the term mail (for the app_class filter):

```
[edit firewall]
user@switch# set family ethernet-switching filter app_class term mail from source-address 192.168.1.24/32
user@switch# set family ethernet-switching filter app_class term mail protocol tcp
user@switch# set family ethernet-switching filter app_class term mail source-port [25 143 389 691 993 3268 3269]
user@switch# set family ethernet-switching filter app_class term mail then forwarding-class mail loss-priority low
```

16. Define the term db (for the app_class filter):

```
[edit firewall]
user@switch# set family ethernet-switching filter app_class term db from source-address 192.168.1.25/32
user@switch# set family ethernet-switching filter app_class term db protocol tcp
user@switch# set family ethernet-switching filter app_class term db source-port [1521 1525 1527 1571 1810 2481]
```
17. Define the term **erp** (for the **app_class** filter):

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter app_class term erp from source-address 192.168.1.26/32
   user@switch# set family ethernet-switching filter app_class term erp protocol tcp
   user@switch# set family ethernet-switching filter app_class term erp source-port [3200 3300 3301 3600]
   user@switch# set family ethernet-switching filter app_class term erp then forwarding-class erp loss-priority low
   ```

18. Define the term **network_control** (for the **app_class** filter):

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter app_class term network_control from precedence [net-control internet-control]
   user@switch# set family ethernet-switching filter app_class term network_control then forwarding-class network-control loss-priority low
   ```

19. Define the term **best_effort_traffic** (for the **app_class** filter):

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter app_class term best_effort_traffic then forwarding-class best-effort loss-priority low
   ```

20. Apply the firewall filter **app_class** as an input filter to the interfaces for the servers hosting applications:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/3 unit 0 family ethernet-switching filter input app_class
   user@switch# set ge-0/0/4 unit 0 family ethernet-switching filter input app_class
   user@switch# set ge-0/0/5 unit 0 family ethernet-switching filter input app_class
   user@switch# set ge-0/0/6 unit 0 family ethernet-switching filter input app_class
   ```

21. Configure schedulers:

   ```
   [edit class-of-service]
   user@switch# set schedulers voice-sched buffer-size percent 10
   user@switch# set schedulers voice-sched priority strict-high
   user@switch# set schedulers voice-sched transmit-rate percent 10
   user@switch# set schedulers video-sched buffer-size percent 15
   user@switch# set schedulers video-sched priority low
   user@switch# set schedulers video-sched transmit-rate percent 15
   user@switch# set schedulers app-sched buffer-size percent 10
   user@switch# set schedulers app-sched priority low
   user@switch# set schedulers app-sched transmit-rate percent 10
   user@switch# set schedulers mail-sched buffer-size percent 5
   user@switch# set schedulers mail-sched priority low
   user@switch# set schedulers mail-sched transmit-rate percent 5
   user@switch# set schedulers db-sched buffer-size percent 10
   user@switch# set schedulers db-sched priority low
   user@switch# set schedulers db-sched transmit-rate percent 10
   user@switch# set schedulers erp-sched buffer-size percent 10
   user@switch# set schedulers erp-sched priority low
   user@switch# set schedulers erp-sched transmit-rate percent 10
   user@switch# set schedulers nc-sched buffer-size percent 5
   user@switch# set schedulers nc-sched priority strict-high
   user@switch# set schedulers nc-sched transmit-rate percent 5
   user@switch# set schedulers be-sched buffer-size percent 35
   user@switch# set schedulers be-sched priority low
   user@switch# set schedulers be-sched transmit-rate percent 35
   ```
22. Assign the forwarding classes to schedulers with the scheduler map ethernet-cos-map:

```
[edit class-of-service]
user@switch# set scheduler-map ethernet-cos-map forwarding-class voice scheduler voice-sched
user@switch# set scheduler-map ethernet-cos-map forwarding-class video scheduler video-sched
user@switch# set scheduler-map ethernet-cos-map forwarding-class app scheduler app-sched
user@switch# set scheduler-map ethernet-cos-map forwarding-class mail scheduler mail-sched
user@switch# set scheduler-map ethernet-cos-map forwarding-class db scheduler db-sched
user@switch# set scheduler-map ethernet-cos-map forwarding-class erp scheduler erp-sched
user@switch# set scheduler-map ethernet-cos-map forwarding-class network-control scheduler nc-sched
user@switch# set scheduler-map ethernet-cos-map forwarding-class best-effort scheduler be-sched
```

23. Associate the scheduler map with the outgoing interface:

```
[edit class-of-service interfaces]
user@switch# set ge-0/0/20 scheduler-map ethernet-cos-map
```

24. Apply queue shaping for the best-effort queue:

```
[edit]
user@switch# set class-of-service schedulers voice-sched queue-shap shap shaping-rate 30m
user@switch# set class-of-service scheduler-maps sched-map be forwarding-class
user@switch# set class-of-service interfaces ge-0/0/2 scheduler-map sched-map be
```

**Results**

Display the results of the configuration:

```
user@switch> show firewall
firewall family ethernet-switching {
  filter voip_class {
    term voip {
      from {
        source-address {
          192.168.1.1/32;
          192.168.1.2/32;
        }
        protocol udp;
        source-port 2698;
      }
      then {
        forwarding-class voice;
        loss-priority low;
      }
    }
    term network control {
      from {
        precedence [net-control internet-control];
      }
      then {
        forwarding-class network-control;
        loss-priority low;
      }
    }
  }
}
```
term best_effort_traffic {
  then {
    forwarding-class best-effort;
    loss-priority low;
  }
}

filter video_class {
  term video {
    from {
      source-address { 192.168.1.14/32; }
      protocol udp;
      source-port 2979;
    }
    then {
      forwarding-class video;
      loss-priority low;
    }
  }
  term network_control {
    from {
      precedence [net-control internet-control];
    }
    then {
      forwarding-class network-control;
      loss-priority low;
    }
  }
  term best_effort_traffic {
    then {
      forwarding-class best-effort;
      loss-priority low;
    }
  }
}

filter app_class {
  term app {
    from {
      source-address { 192.168.1.23/32; }
      protocol tcp;
      source-port [1491 2512 2513 2598 2897];
    }
    then {
      forwarding-class app;
      loss-priority low;
    }
  }
  term mail {
    from {
      source-address {
192.168.1.24/32;
} protocol tcp;
source-port [25143389 691993 32683269];
} then {
    forwarding-class mail;
    loss-priority low;
} term db {
    from {
        source-address {
            192.168.1.25/32;
        } protocol tcp;
        source-port [152115251527157118102481];
    } then {
        forwarding-class db;
        loss-priority low;
    } term erp {
    from {
        source-address {
            192.168.1.26/32;
        } protocol tcp;
        source-port [3200 3300 3301 3600];
    } then {
        forwarding-class erp;
        loss-priority low;
    } term network control {
    from {
        precedence [net-control internet-control];
    } then {
        forwarding-class network-control;
        loss-priority low;
    } term best_effort_traffic {
    then {
        forwarding-class best-effort;
        loss-priority low;
    } user@switch# show class-of-service
forwarding-classes {
class app queue-num 5;
class mail queue-num 1;
class db queue-num 2;
class erp queue-num 3;
class video queue-num 4;
class best-effort queue-num 0;
class voice queue-num 6;
class network-control queue-num 7;
}

interfaces {
  ge-0/0/0 {
    shaping-rate 100m;
  }
}

interfaces {
  ge-0/0/2 {
    scheduler-map sched-map-be;
  }
}

schedulers {
  voice-sched-queue-shap {
    shaping-rate 30m;
  }
  voice-sched {
    buffer-size percent 10;
    priority strict-high;
    transmit-rate percent 10;
  }
  video-sched {
    buffer-size percent 15;
    priority low;
    transmit-rate percent 15;
  }
  app-sched {
    buffer-size percent 10;
    priority low;
    transmit-rate percent 10;
  }
  mail-sched {
    buffer-size percent 5;
    priority low;
    transmit-rate percent 5;
  }
  db-sched {
    buffer-size percent 10;
    priority low;
    transmit-rate percent 10;
  }
  erp-sched {
    buffer-size percent 10;
    priority low;
    transmit-rate percent 10;
  }
  nc-sched {
    buffer-size percent 5;
    priority strict-high;
  }
}
transmit-rate percent 5;

be-sched {
    buffer-size percent 35;
    priority low;
    transmit-rate percent 35;
}
}
}
scheduler-maps {
    ethernet-cos-map {
        forwarding-class voice scheduler voice-sched;
        forwarding-class video scheduler video-sched;
        forwarding-class app scheduler app-sched;
        forwarding-class mail scheduler mail-sched;
        forwarding-class db scheduler db-sched;
        forwarding-class erp scheduler erp-sched;
        forwarding-class network-control scheduler nc-sched;
        forwarding-class best-effort scheduler be-sched;
    }
    sched-map-be {
        forwarding-class best-effort scheduler voice-sched-queue-shap;
    }
}
}

user@switch# show interfaces

ge-0/0/0 {
    unit 0 {
        family ethernet {
            filter {
                input voip_class;
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family ethernet {
            filter {
                input voip_class;
            }
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family ethernet {
            filter {
                input video_class;
            }
        }
    }
}
ge-0/0/3 {
    unit 0 {
        family ethernet {
            filter {
Verifying That the Defined Forwarding Classes Exist and Are Mapped to Queues

Purpose

Verify that the forwarding classes **app**, **best-effort**, **db**, **erp**, **mail**, **network-control**, **video**, and **voice** have been defined and mapped to queues.
### Action

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>ID</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>db</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>erp</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>best-effort</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>mail</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>voice</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>video</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>network-control</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

### Meaning

This output shows that the forwarding classes have been defined and mapped to appropriate queues.

### Verifying That the Forwarding Classes Have Been Assigned to Schedulers

### Purpose

Verify that the forwarding classes have been assigned to schedulers.
Action 

user@switch> show class-of-service scheduler-map
Scheduler map: ethernet-cos-map, Index: 2
Scheduler: voice-sched, Forwarding class: voice, Index: 22
  Transmit rate: 5 percent, Rate Limit: none, Buffer size: 15 percent,
  Priority: Strict-high
  Drop profiles:
    Loss priority Protocol  Index    Name
    High          non-TCP      1    <default-drop-profile>
    High          TCP          1    <default-drop-profile>
Scheduler: video-sched, Forwarding class: video, Index: 22
  Transmit rate: 10 percent, Rate Limit: none, Buffer size: 10 percent,
  Priority: low
  Drop profiles:
    Loss priority Protocol  Index    Name
    High          non-TCP      1    <default-drop-profile>
    High          TCP          1    <default-drop-profile>
Scheduler: app-sched, Forwarding class: app, Index: 22
  Transmit rate: 10 percent, Rate Limit: none, Buffer size: 10 percent,
  Priority: low
  Drop profiles:
    Loss priority Protocol  Index    Name
    High          non-TCP      1    <default-drop-profile>
    High          TCP          1    <default-drop-profile>
Scheduler: mail-sched, Forwarding class: mail, Index: 22
  Transmit rate: 5 percent, Rate Limit: none, Buffer size: 5 percent,
  Priority: low
  Drop profiles:
    Loss priority Protocol  Index    Name
    High          non-TCP      1    <default-drop-profile>
    High          TCP          1    <default-drop-profile>
Scheduler: db-sched, Forwarding class: db, Index: 22
  Transmit rate: 10 percent, Rate Limit: none, Buffer size: 10 percent,
  Priority: low
  Drop profiles:
    Loss priority Protocol  Index    Name
    High          non-TCP      1    <default-drop-profile>
    High          TCP          1    <default-drop-profile>
Scheduler: erp-sched, Forwarding class: erp, Index: 22
  Transmit rate: 10 percent, Rate Limit: none, Buffer size: 10 percent,
  Priority: low
  Drop profiles:
    Loss priority Protocol  Index    Name
    High          non-TCP      1    <default-drop-profile>
    High          TCP          1    <default-drop-profile>
Scheduler: be-sched, Forwarding class: best-effort, Index: 20
  Transmit rate: 35 percent, Rate Limit: none, Buffer size: 35 percent,
  Priority: low
  Drop profiles:
    Loss priority Protocol  Index    Name
    High          non-TCP      1    <default-drop-profile>
    High          TCP          1    <default-drop-profile>
Scheduler: nc-sched, Forwarding class: network-control, Index: 22
  Transmit rate: 5 percent, Rate Limit: none, Buffer size: 5 percent,
Meaning  This output shows that the forwarding classes have been assigned to schedulers.

Verifying That the Scheduler Map Has Been Applied to the Interface

Purpose  Verify that the scheduler map has been applied to the interface.

Action  
user@switch> show class-of-service interface
...  
Physical interface: ge-0/0/20, Index: 149
Queues supported: 8, Queues in use: 8
  Scheduler map: ethernet-cos-map, Index: 43366
  Input scheduler map: <default>, Index: 3
...

Meaning  This output shows that the scheduler map (ethernet-cos-map) has been applied to the interface (ge-0/0/20).

Verifying That Port Shaping Has Been Applied

Purpose  Verify that the port shaping has been applied to an interface.

Action  Following is the output before port shaping is applied to the interface ge-0/0/0, when there is egress traffic of 400 Mpbps exiting on that interface:

user@switch> show interfaces ge-0/0/0 extensive
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 239, SNMP ifIndex: 548, Generation: 242
  Device flags  : Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags    : None
  CoS queues    : 8 supported, 8 maximum usable queues
  Hold-times    : Up 0 ms, Down 0 ms
  Current address: 00:23:9c:0b:ae:8d, Hardware address: 00:23:9c:0b:ae:8d
  Last flapped  : 2012-07-07 03:21:52 UTC (1d 18:02 ago)

Traffic statistics:
  Input bytes  : 0 0 bps
  Output bytes : 2299853696 345934816 bps
  Input packets: 0 0pps
  Output packets: 17967609 337827 pps

IPv6 transit statistics:
  Input bytes  : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Input errors:
   Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3
   incompatibles: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0,
   Resource errors: 0
Output errors:
   Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
   FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 0 18302337 0
1 assured-forwarding 0 0 0
5 expedited-forwarding 0 0 0
7 network-control 0 0 0
Queue number: Mapped forwarding classes
0 best-effort
1 assured-forwarding
5 expedited-forwarding
7 network-control
Active alarms : None
Active defects : None
MAC statistics: Receive Transmit
Total octets 0 2299853696
Total packets 0 17967609
Unicast packets 0 17967609
Broadcast packets 0 0
Multicast packets 0 0
CRC/Align errors 0 0
FIFO errors 0 0
MAC control frames 0 0
MAC pause frames 0 0
Oversized frames 0 0
Jabber frames 0 0
Fragment frames 0 0
Code violations 0 0
Autonegotiation information:
   Negotiation status: Complete
   Link partner:
      Link mode: Full-duplex, Flow control: Symmetric, Remote fault: OK, Link
      partner Speed: 1000 Mbps
   Local resolution:
      Flow control: Symmetric, Remote fault: Link OK
   Packet Forwarding Engine configuration:
      Destination slot: 1
   CoS information:
      Direction : Output
      CoS transmit queue Bandwidth Buffer Priority Limit
      % bps % usec
0 best-effort 95 950000000 95 NA low none
7 network-control 5 50000000 5 NA low none
Interface transmit statistics: Disabled
Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 638) (Generation 138)
   Flags: SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

Local statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

Transit statistics:
- Input bytes: 0 (0 bps)
- Output bytes: 0 (0 bps)
- Input packets: 0 (0 pps)
- Output packets: 0 (0 pps)

Protocol eth-switch, Generation: 163, Route table: 0
Flags: Trunk-Mode

The Traffic statistics: field in this output shows that egress traffic is ~400 Mbps (345,934,816 bps). When a port shaping of 100 Mbps is applied to the ge-0/0/0 interface, you see the following outputs for the show interfaces ge-0/0/0 statistics and the show class-of-service interface ge-0/0/0 commands:

user@switch> show interfaces ge-0/0/0 statistics
Physical interface: ge-0/0/0, Enabled, Physical link is Up
  Interface index: 239, SNMP ifIndex: 548, Generation: 242
  Device flags : Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags : None
  CoS queues : 8 supported, 8 maximum usable queues
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:23:9c:0b:ae:8d, Hardware address: 00:23:9c:0b:ae:8d
  Last flapped : 2012-07-07 03:21:52 UTC (1d 18:10 ago)
  Traffic statistics:
    Input bytes: 0 (0 bps)
    Output bytes: 15779512832 (100223104 bps)
    Input packets: 0 (0 pps)
    Output packets: 123277444 (97874 pps)
  IPv6 transit statistics:
    Input bytes: 0
    Output bytes: 0
    Input packets: 0
    Output packets: 0
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters: Queued packets Transmitted packets Dropped packets
    0 best-effort 0 123350092 57012484
    1 assured-forward 0 0 0
Queue number: Mapped forwarding classes
0  best-effort
1  assured-forwarding
5  expedited-forwarding
7  network-control
Active alarms: None
Active defects: None
MAC statistics:

<table>
<thead>
<tr>
<th></th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>15779512832</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>123277444</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>123277444</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Autonegotiation information:
Negotiation status: Complete
Link partner:
Link mode: Full-duplex, Flow control: Symmetric, Remote fault: OK, Link partner Speed: 1000 Mbps
Local resolution:
Flow control: Symmetric, Remote fault: Link OK
Packet Forwarding Engine configuration:
Destination slot: 1
CoS information:
Direction: Output

<table>
<thead>
<tr>
<th>Limit</th>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>%</td>
<td>bps</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>95000000</td>
<td>95</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 network-control</td>
<td>5</td>
<td>50000000</td>
<td>5</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Interface transmit statistics: Disabled

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 638) (Generation 138)
Flags: SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0
Output bytes : 0
          0 bps
Meaning

In the output for the `show interfaces ge-0/0/0 statistics` command, the Traffic statistics: field shows that egress traffic is ~100 Mbps (100,223,104 bps). The output for the `show class-of-service interface ge-0/0/0` command shows that the shaping rate is 100,000,000 bps, which indicates that a port shaping of 100 Mbps is applied to the ge-0/0/0 interface.

**Verifying That Queue Shaping Has Been Applied**

**Purpose**

Verify that the queue shaping has been applied to the best-effort queue.

**Action**

Following is the output before queue shaping is applied to the best-effort queue when there is egress traffic of 400 Mbps exiting on that interface:

```bash
user@switch> show interfaces ge-0/0/2 extensive
Physical interface: ge-0/0/2, Enabled, Physical link is Up
   Interface index: 239, SNMP ifIndex: 548, Generation: 242
   Media type: Copper
   Device flags   : Present Running
   Interface flags: SNMP-Traps Internal: 0x0
   Link flags     : None
   CoS queues     : 8 supported, 8 maximum usable queues
   Hold-times     : Up 0 ms, Down 0 ms
   Current address: 00:23:9c:0b:ae:8d, Hardware address: 00:23:9c:0b:ae:8d
   Last flapped   : 2012-07-07 03:21:52 UTC (1d 18:02 ago)
   Traffic statistics:
      Input  bytes  :                    0                    0 bps
      Output bytes :  2299853696            345934816 bps
      Input  packets:                    0                    0 pps
      Output packets:  0                  0 ppss
   IPv6 transit statistics:
      Input  bytes  :                    0                    0 bps
      Output bytes :                    0                    0 bps
      Input  packets:                    0                    0 pps
      Output packets:                    0                    0 pps
   Input errors:
      Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
   Output errors:
      Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
   Egress queues: 8 supported, 4 in use
   Queue counters:
```
0 best-effort                    0             18302337                    0
1 assured-forwarding           0                    0                    0
5 expedited-forwarding         0                    0                    0
7 network-control              0                    0                    0

Queue number: Mapped forwarding classes
    0                   best-effort
    1                   assured-forwarding
    5                   expedited-forwarding
    7                   network-control

Active alarms: None
Active defects: None

MAC statistics:

<table>
<thead>
<tr>
<th>Total octets</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total packets</td>
<td>2299853696</td>
<td>17967609</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Auto-negotiation information:
Negotiation status: Complete
Link partner:
    Link mode: Full-duplex, Flow control: Symmetric, Remote fault: OK, Link partner Speed: 1000 Mbps
Local resolution:
    Flow control: Symmetric, Remote fault: Link OK
Packet Forwarding Engine configuration:
    Destination slot: 1
CoS information:
    Direction: Output
    CoS transmit queue Limit
    Bandwidth Buffer Priority
    %     bps     %     usec
    0    95   950000000    95   NA   low
    none
    5 500000000   5   NA   low

Interface transmit statistics: Disabled

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 638) (Generation 138)
Flags: SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0pps
Output packets: 0 0pps
Protocol eth-switch, Generation: 163, Route table: 0
Flags: Trunk-Mode

The Traffic statistics: field in this output shows that the egress traffic is ~400 Mbps (345,934,816 bps). When a queue shaping of 30 Mbps is applied to the best-effort queue, you see the following output for the show interfaces ge-0/0/2 statistics and show class-of-service scheduler-map sched-map-be commands:

user@switch> show interfaces ge-0/0/2 statistics
Physical interface: ge-0/0/2, Enabled, Physical link is Up
   Interface index: 239, SNMP ifIndex: 548, Generation: 242
Device flags : Present Running
   Interface flags: SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:23:9c:0b:ae:8d, Hardware address: 00:23:9c:0b:ae:8d
Last flapped : 2012-07-07 03:21:52 UTC (1d 18:29 ago)
Statistics last cleared: 2012-07-08 21:46:22 UTC (00:04:56 ago)
Traffic statistics:
   Input bytes : 0 0 bps
   Output bytes : 537612896 30097712 bps
   Input packets: 0 0pps
   Output packets: 42001003 29392 pps
IPv6 transit statistics:
   Input bytes : 0
   Output bytes : 0
   Input packets: 0
   Output packets: 0
Input errors:
   Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0
Output errors:
   Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 0 41986978 57813642
1 assured-forward 0 0 0
5 expedited-forward 0 0 0
7 network-continue 0 0 0
Queue number: Mapped forwarding classes
0 best-effort
1 assured-forwarding
5 expedited-forwarding
Active alarms : None
Active defects : None

MAC statistics:          Receive      Transmit
Total octets             0           5376128896
Total packets            0           42001003
Unicast packets          0           42001003
Broadcast packets        0           0
Multicast packets        0           0
CRC/Align errors         0           0
FIFO errors              0           0
MAC control frames       0           0
MAC pause frames         0           0
Oversized frames         0
Jabber frames            0
Fragment frames          0
Code violations          0

Autonegotiation information:
   Negotiation status: Complete
   Link partner:
      Link mode: Full-duplex, Flow control: Symmetric, Remote fault: OK, Link
   partner Speed: 1000 Mbps
   Flow control: Symmetric, Remote fault: Link OK
Packet Forwarding Engine configuration:
   Destination slot: 1
CoS information:
   Direction : Output
   CoS transmit queue | Bandwidth | Buffer Priority
   Limit        %  bps | %      usec | Limit
   0 best-effort r  r  r  | NA low

Interface transmit statistics: Disabled

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 638) (Generation 138)
   Flags: SNMP-Traps 0x0 Encapsulation: ENET2
   Traffic statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   Local statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   Transit statistics:
      Input bytes : 0 0 bps
      Output bytes : 0 0 bps
      Input packets: 0 0 pps
      Output packets: 0 0 pps
   Protocol eth-switch, Generation: 163, Route table: 0
   Flags: Trunk-Mode

user@switch> show class-of-service scheduler-map sched-map-be

Scheduler map: sched-map-be, Index: 31271

Scheduler: voice-sched-queue-shap, Forwarding class: best-effort, Index: 64106
Transmit rate: remainder, Rate Limit: none, Buffer size: remainder, Buffer Limit: none, Priority: low
Excess Priority: unspecified
Shaping rate: 30000000 bps
Drop profiles:

<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
</tbody>
</table>

**Meaning**

In the output for the `show interfaces ge-0/0/2 statistics` command, the Traffic statistics: field shows that the egress traffic is ~30 Mbps (30,097,712 bps). The output for the `show class-of-service scheduler-map sched-map-be` command, shows that a shaping rate of 30,000,000 bps (that is 30 Mbps) is applied to the best-effort queue.

**Related Documentation**

- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921
- Defining CoS Classifiers (CLI Procedure) on page 1923
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929
- Configuring CoS Tail Drop Profiles (CLI Procedure)
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942
- Configuring Firewall Filters (CLI Procedure) on page 4192

**Configuration Tasks**

- Configuring CoS (J-Web Procedure) on page 1920
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921
- Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Defining CoS Classifiers (CLI Procedure) on page 1923
- Defining CoS Classifiers (J-Web Procedure) on page 1925
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927
- Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929
- Defining CoS Schedulers (J-Web Procedure) on page 1931
- Defining CoS Scheduler Maps (J-Web Procedure) on page 1934
- Configuring CoS Congestion Management (CLI Procedure) on page 1935
- Defining CoS Drop Profiles (J-Web Procedure) on page 1938
- Defining CoS Rewrite Rules (CLI Procedure) on page 1939
- Defining CoS Rewrite Rules (J-Web Procedure) on page 1940
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942
- Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942
Configuring CoS (J-Web Procedure)

The Class of Service Configuration pages allow you to configure the Junos CoS components. You can configure forwarding classes for transmitting packets, define which packets are placed into each output queue, and schedule the transmission service level for each queue. After defining the CoS components you must assign classifiers to the required physical and logical interfaces.

Using the Class of Service Configuration pages, you can configure various CoS components individually or in combination to define particular CoS services.

To configure CoS components:

1. In the J-Web interface, select **Configure>Class of Service**.
2. On the Class of Service Configuration page, select one of the following options depending on the CoS component that you want to define. Enter information into the pages as described in the respective table:
   - To define or edit CoS value aliases, select **CoS Value Aliases**.
   - To define or edit forwarding classes and assign queues, select **Forwarding Classes**.
   - To define or edit classifiers, select **Classifiers**.
   - To define or edit rewrite rules, select **Rewrite Rules**.
   - To define or edit schedulers, select **Schedulers**.
   - To define or edit virtual channel groups, select **Interface Associations**.
3. Click **Apply** after completing configuration on any Configuration page.

Related Documentation

- Defining CoS Classifiers (J-Web Procedure) on page 1925
- Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
- Defining CoS Rewrite Rules (J-Web Procedure) on page 1940
- Defining CoS Schedulers (J-Web Procedure) on page 1931
- Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942
You can use code-point aliases to streamline the process of configuring CoS features on your EX Series switch. A code-point alias assigns a name to a pattern of code-point bits. You can use this name instead of the bit pattern when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules.

You can configure code-point aliases for the following CoS marker types:

- **dscp** and **dscp-ipv6**—Handles incoming IPv4 and IPv6 packets, respectively.
- **ieee-802.1**—Handles Layer 2 CoS.
- **inet-precedence**—Handles incoming IPv4 packets. IP precedence mapping requires only the higher order three bits of the DSCP field.

To configure a code-point alias for a specified CoS marker type (**dscp**), assign an alias (**my1**) to the code-point (**110001**):

```
[edit class-of-service code-point-aliases]
user@switch# set dscp my1 110001
```

The **my1** alias will be applicable for incoming IPv4 packets.

### Related Documentation
- Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Example: Configuring CoS on EX Series Switches on page 1895
- Monitoring CoS Value Aliases on page 1881
- Understanding CoS Code-Point Aliases on page 1866

### Defining CoS Code-Point Aliases (J-Web Procedure)

You can use the J-Web interface to define CoS code-point aliases on an EX Series switch. By defining aliases you can assign meaningful names to a particular set of bit values and refer to them when configuring CoS components.

To define CoS code-point aliases:

1. Select **Configure > Class of Service > CoS Value Aliases**.

```
NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.
```

2. Click one of the following options:

   - **Add**—Adds a code-point alias. Enter information into the code point alias page as described in Table 235 on page 1922.
- **Edit**—Modifies an existing code-point alias. Enter information into the code point alias page as described in Table 235 on page 1922.
- **Delete**—Deletes an existing code-point alias.

Table 235 on page 1922 describes the related fields.

### Table 235: CoS Value Aliases Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code point name</td>
<td>Specifies the name for a code-point—for example, af11 or be.</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>Code point type</td>
<td>Specifies a code-point type. The code-point type can be DSCP or IP precedence.</td>
<td>Select a value.</td>
</tr>
</tbody>
</table>
| Code point value bits | Specifies the CoS value for which an alias is defined. Changing this value alters the behavior of all classifiers that refer to this alias. | To specify a CoS value, type it in the appropriate format:

- For DSCP CoS values, use the format xxxxxx, where x is 1 or 0—for example, 101110.
- For IP precedence CoS values, use the format xxx, where x is 1 or 0—for example, 111.

### Related Documentation
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921
- Example: Configuring CoS on EX Series Switches on page 1895
Defining CoS Classifiers (CLI Procedure)

Packet classification associates incoming packets with a particular CoS servicing level. Classifiers associate packets with a forwarding class and loss priority and assign packets to output queues based on the associated forwarding class. Junos OS supports two general types of classifiers:

- **Behavior aggregate (BA) classifier**—Examine the CoS value in the packet header. The value in this single field determines the CoS settings applied to the packet. BA classifiers allow you to set the forwarding class and loss priority of a packet based on the Differentiated Services code point (DSCP) value, IP precedence value, or IEEE 802.1p value. EX Series switches except EX4300 switches support two types of loss priorities: high and low. EX4300 switches support four types of loss priorities: high, medium-high, low, and medium-low.

You can configure BA classifiers for the following CoS marker types:

- **dscp** and **dscp-ipv6**—Handles incoming IPv4 and IPv6 packets, respectively.
- **ieee-802.1**—Handles Layer 2 CoS.
- **inet-precedence**—Handles incoming IPv4 packets. IP precedence mapping requires only the higher order three bits of the DSCP field.

- **Multifield (MF) classifier**—Examine multiple fields in the packet such as source and destination addresses and source and destination port numbers of the packet. With MF classifiers, you set the forwarding class and loss priority of a packet based on firewall filter rules.

**NOTE:** Juniper Networks EX8200 Ethernet Switches implement the on-demand ternary content addressable memory (TCAM) allocation of memory so that when additional TCAM space is required for CoS, the space is allocated from the free TCAM space or from the unused TCAM space. An error log message is generated when you configure CoS classifiers beyond the available TCAM space that includes both the free and unused space.

The following example describes how to configure a BA classifier (**ba-classifier**) as the default DSCP map for handling IPv4 traffic and to apply the BA classifier to either a specific Gigabit Ethernet interface or to all the Gigabit Ethernet interfaces on the switch. The BA classifier assigns loss priorities, as shown in Table 236 on page 1923, to incoming packets in the four forwarding classes.

You can use the same procedure to set MF classifiers (except that you would use firewall filter rules).

**Table 236: BA-classifier Loss Priority Assignments**

<table>
<thead>
<tr>
<th>Forwarding Class</th>
<th>For CoS Traffic Type</th>
<th>ba-classifier Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>be</td>
<td>Best-effort traffic</td>
<td>High-priority code point: 000001</td>
</tr>
</tbody>
</table>
### Table 236: BA-classifier Loss Priority Assignments (continued)

<table>
<thead>
<tr>
<th>Code Point</th>
<th>Traffic Type</th>
<th>High-priority Code Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>ef</td>
<td>Expedited-forwarding traffic</td>
<td>101110</td>
</tr>
<tr>
<td>af</td>
<td>Assured-forwarding traffic</td>
<td>001100</td>
</tr>
<tr>
<td>nc</td>
<td>Network-control traffic</td>
<td>110001</td>
</tr>
</tbody>
</table>

To configure a DSCP BA classifier named `ba-classifier` as the default DSCP map:

- Associate code point `000001` with forwarding class `be` and loss priority `high`:

  ```
  [edit class-of-service classifiers]
  user@switch# set dscp ba-classifier import default forwarding-class be loss-priority high code-points 000001
  ```

- Associate code point `101110` with forwarding class `ef` and loss priority `high`:

  ```
  [edit class-of-service classifiers]
  user@switch# set dscp ba-classifier forwarding-class ef loss-priority high code-points 101110
  ```

- Associate code point `001100` with forwarding class `af` and loss priority `high`:

  ```
  [edit class-of-service classifiers]
  user@switch# set dscp ba-classifier forwarding-class af loss-priority high code-points 001100
  ```

- Associate code point `110001` with forwarding class `nc` and loss priority `high`:

  ```
  [edit class-of-service classifiers]
  user@switch# set dscp ba-classifier forwarding-class nc loss-priority high code-points 110001
  ```

- Apply the classifier to a specific interface or to all Gigabit Ethernet interfaces on the switch.

  ```
  To apply the classifier to a specific interface:
  ```

  ```
  [edit class-of-service interfaces]
  user@switch# set ge-0/0/0 unit 0 classifiers dscp ba-classifier
  ```

  ```
  To apply the classifier to all Gigabit Ethernet interfaces on the switch, use wildcards for the interface name and the logical-interface (unit) number:
  ```

  ```
  [edit class-of-service interfaces]
  user@switch# set ge-* unit * classifiers dscp ba-classifier
  ```

---

**NOTE:** On EX8200 switches, it can take a long time to install code-point classifiers on multiple interfaces (for example, approximately 25 minutes to install 64 code-point classifiers on multiple interfaces in the order of 280 or more).
Defining CoS Classifiers (J-Web Procedure)

You can use the J-Web interface to define CoS classifiers on an EX Series switch. Classifiers examine the CoS value or alias of an incoming packet and assign the packet a level of service by setting its forwarding class and loss priority.

To define CoS classifiers:

1. Select **Configure > Class of Service > Classifiers**.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Adds a classifier. Enter information into the classifier page as described in Table 237 on page 1925.
   - **Edit**—Modifies an existing classifier. Enter information into the classifier page as described in Table 237 on page 1925.
   - **Delete**—Deletes an existing classifier.

### Table 237: Classifiers Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifier Name</td>
<td>Specifies the name for a classifier.</td>
<td>To name a classifier, type the name—for example, <em>ba-classifier</em>.</td>
</tr>
<tr>
<td>Classifier Type</td>
<td>Specifies the type of classifier: <em>dscp</em>, <em>ieee-802.1</em>, or <em>inet-precedence</em>.</td>
<td>Select a value from the list.</td>
</tr>
</tbody>
</table>
### Table 237: Classifiers Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Code Point Mapping     | Sets the forwarding classes and the packet loss priorities (PLPs) for specific CoS values and aliases. | To add a code point mapping:  
1. Click **Add**.  
2. Select the code point.  
3. Select a forwarding class from the following list:  
   - **expedited-forwarding**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. Packets can be forwarded out of sequence or dropped.  
   - **best-effort**—Provides no special CoS handling of packets. Typically, RED drop profile is aggressive and no loss priority is defined.  
   - **assured-forwarding**—Provides high assurance for packets within the specified service profile. Excess packets are dropped.  
   - **network-control**—Packets can be delayed but not dropped.  
4. Select the loss priority.  
   To assign a loss priority, select one:  
   - **high**—Packet has a high loss priority.  
   - **low**—Packet has a low loss priority. |

### Related Documentation
- Defining CoS Classifiers (CLI Procedure) on page 1923  
- Example: Configuring CoS on EX Series Switches on page 1895  
- Monitoring CoS Classifiers on page 1975  
- Understanding CoS Classifiers
Defining CoS Forwarding Classes (CLI Procedure)

Forwarding classes allow you to group packets for transmission. Based on forwarding classes, you assign packets to output queues.

By default, four categories of forwarding classes are defined: best effort, assured forwarding, expedited forwarding, and network control. EX Series switches support up to 16 forwarding classes.

You can configure forwarding classes in one of the following ways:

- Using `class` statement—You can configure up to 16 forwarding classes and you can map multiple forwarding classes to single queue.
- Using `queue` statement—You can configure up to 8 forwarding classes and you can map one forwarding class to one queue.

This example uses the `class` statement to configure forwarding classes.

To configure CoS forwarding classes, map the forwarding classes to queues:

```
[edit class-of-service forwarding-classes]
user@switch# set class be queue=num 0
user@switch# set class ef queue=num 1
user@switch# set class af queue=num 2
user@switch# set class nc queue=num 3
user@switch# set class efi queue=num 4
user@switch# set class ef2 queue=num 5
user@switch# set class af1 queue=num 6
user@switch# set class nc1 queue=num 7
```

Related Documentation

- Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
- Example: Configuring CoS on EX Series Switches on page 1895
- **Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic**
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942
- Monitoring CoS Forwarding Classes on page 1976
- Understanding CoS Forwarding Classes

Defining CoS Forwarding Classes (J-Web Procedure)

You can define CoS forwarding classes on an EX Series switch using the J-Web interface. Assigning a forwarding class to a queue number affects the scheduling and marking of a packet as it transits a switch.

To define forwarding classes:

1. Select **Configure > Class of Service > Forwarding Classes.**
NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Adds a forwarding class. Enter information into the forwarding class page as described in Table 238 on page 1928.
   - **Edit**—Modifies an existing forwarding class. Enter information into the forwarding class page as described in Table 238 on page 1928.
   - **Delete**—Deletes an existing forwarding class.

Table 238: Forwarding Classes Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forwarding Class Summary</strong></td>
<td>Specifications the internal queue numbers to which forwarding classes are assigned.</td>
<td>To specify an internal queue number, select an integer from 0 through 7, appropriate for your platform. <strong>NOTE:</strong> For EX4300 switches, to specify an internal queue number, select an integer from 0 through 11.</td>
</tr>
<tr>
<td><strong>Queue #</strong></td>
<td>Specifies the forwarding class names assigned to specific internal queue numbers.</td>
<td>Type the name—for example, be-class.</td>
</tr>
<tr>
<td></td>
<td>By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can have more than one forwarding class to a queue number.</td>
<td><strong>NOTE:</strong> For EX4300 switches, by default the forwarding classes are assigned to queue numbers 0 (best-effort), 1 (assured-forwarding), 5 (expedited-forwarding), and 7 (network-connect).</td>
</tr>
<tr>
<td></td>
<td>By default, four forwarding classes are assigned to queue numbers 0 (best-effort), 1 (assured-forwarding), 5 (expedited-forwarding), and 7 (network-connect).</td>
<td><strong>NOTE:</strong> For EX4300 switches, by default the forwarding classes are assigned to queue numbers 0 (best-effort), 1 (expedited-forwarding), 2 (assured-forwarding), 3 (network-connect), 8 (mcast-be), 9 (mcast-af), 10 (mcast-af), and 11 (mcast-nc).</td>
</tr>
</tbody>
</table>

Related Documentation
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927
- Example: Configuring CoS on EX Series Switches on page 1895
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic
- Monitoring CoS Forwarding Classes on page 1976
- Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942
Understanding CoS Forwarding Classes

Defining CoS Schedulers and Scheduler Maps (CLI Procedure)

You use schedulers to define the class-of-service (CoS) properties of output queues. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the drop profiles associated with the queue.

You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the queues and packet schedulers that operate according to this mapping.

NOTE: On EX Series switches, you cannot configure a scheduler map on an individual interface that is a member of a link aggregation group (LAG). Instead, you must configure the scheduler map on the LAG itself (that is, on the aggregated Ethernet (ae) interface).

You can associate up to four user-defined scheduler maps with an interface.

This topic describes:

- Configuring a Scheduler and a Scheduler Map on page 1929
- Assigning a Scheduler Map to Interfaces on page 1930
- Assigning Scheduler Maps to Interfaces on EX8200 Line Cards That Include Oversubscribed Ports on page 1930

Configuring a Scheduler and a Scheduler Map

You can define the properties for an output queue by configuring a scheduler. You can then define a scheduler map to associate a forwarding class with a scheduler.

To configure a scheduler and a scheduler map:

1. Create a scheduler, and assign one or more output queue properties to it:

```
[edit class-of-service]
user@switch# set schedulers scheduler-name output-queue-properties
```

For various properties that you can define for an output queue, see the schedulers hierarchy.

2. Configure a scheduler map that associates the scheduler with the forwarding class:

```
[edit class-of-service]
user@switch# set scheduler-maps map-name forwarding-class class-name scheduler scheduler-name
```
Assigning a Scheduler Map to Interfaces

After defining a scheduler map, you can assign the scheduler map to one or more interfaces. You can also assign the scheduler map to multiple interfaces by using a wildcard representation of the interface or Virtual Chassis Ports (VCPs).

Following are sample syntaxes and examples for assigning a scheduler map to a single or to multiple interfaces:

- To assign the scheduler map to one interface:

  ```
  [edit class-of-service interfaces]
  user@switch# set interface-name scheduler-map map-name
  ```

- To assign the scheduler map to more than one interface, you can use a wildcard representation of the interface:

  ```
  [edit class-of-service interfaces]
  user@switch# set wild-card-representation-of-interface-name scheduler-map map-name
  ```

  For example, following is the configuration to assign the be-map scheduler map to all Gigabit Ethernet interfaces (ge-*):

  ```
  [edit class-of-service interfaces]
  user@switch# set ge-* scheduler-map be-map
  ```

- To assign the scheduler map to all VCPs:

  ```
  [edit class-of-service interfaces]
  user@switch# set wild-card-representation-of-vcp scheduler-map map-name
  ```

  **NOTE:** You can assign a scheduler map to a VCP only on EX4200, EX4300 or EX4500 switches that are members of Virtual Chassis composed exclusively either of EX4200 switches, EX4300 switches or of EX4500 switches, or that are members of a mixed Virtual Chassis composed of EX4200, EX4300, and EX4500 switches.

  For example, following is the configuration to assign the be-map scheduler map to all VCPs:

  ```
  [edit class-of-service interfaces]
  user@switch# set vcp-* scheduler-map be-map
  ```

Assigning Scheduler Maps to Interfaces on EX8200 Line Cards That Include Oversubscribed Ports

Some line cards available for Juniper Networks EX8200 Ethernet Switches include oversubscribed ports that are combined in logical port groups that share bandwidth. These oversubscribed ports handle traffic differently than ports that provide continuous line-rate bandwidth. You might need to configure CoS queues differently for oversubscribed ports than for line-rate ports. For more information about EX8200 line cards that include oversubscribed ports, see “Understanding CoS Queues on EX8200 Line Cards That Include Oversubscribed Ports” on page 1891.

For interfaces on oversubscribed EX8200 line cards, you use the same procedure to configure CoS schedulers as you do for other interfaces. However, you must assign the
same scheduler map to all the interfaces in a port group. When you assign a scheduler map to one interface in a port group, you do not need to assign the scheduler map to the remaining interfaces in the port group. The switch automatically uses that scheduler map for all the interfaces in the port group when you bring the interfaces up. Therefore, you do not need to assign the scheduler map to the remaining interfaces in that port group.

If you assign different scheduler maps to different interfaces in a port group, you do not receive an error when you commit the configuration. Instead, an error is logged in the system log. When you bring an interface in the port group up, the default scheduler map is assigned to all interfaces in the port group. If you assign a scheduler map to an interface that is down and if that scheduler map is different from the scheduler map being used by the currently operating interfaces in the port group, then the default scheduler map is used by all interfaces in the port group, even the currently operating ones, when you bring the interface up.

To assign a scheduler map to a port group, assign a scheduler map to at least one interface in the port group:

```
[edit class-of-service interfaces]
user@switch# set interface-name scheduler-map map-name
```

Considering that the xe-0/0/2 interface is part of a port group, following is the configuration to assign a scheduler map named `ef-map` to a port group that contains xe-0/0/2:

```
[edit class-of-service interfaces]
user@switch# set xe-0/0/2 scheduler-map ef-map
```

### Related Documentation

- Defining CoS Schedulers (J-Web Procedure) on page 1931
- Example: Configuring CoS on EX Series Switches on page 1895
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942
- Monitoring CoS Scheduler Maps on page 1980
- Understanding CoS Schedulers on page 1880

### Defining CoS Schedulers (J-Web Procedure)

You can use the J-Web interface to define CoS schedulers on an EX Series switch. Using schedulers, you can assign attributes to queues and thereby provide congestion control for a particular class of traffic. These attributes include the amount of interface bandwidth, memory buffer size, transmit rate, and schedule priority.

To configure schedulers:

1. Select `Configure > Class of Service > Schedulers`. 
NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Adds a scheduler. Enter information into the Schedulers page as described in Table 239 on page 1932.
   - **Edit**—Modifies an existing scheduler. Enter information into the Schedulers page as described in Table 239 on page 1932.
   - **Delete**—Deletes an existing scheduler.

### Table 239: Schedulers Configuration Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler name</td>
<td>Specifies the name for a scheduler.</td>
<td>To name a scheduler, type the name—for example, <code>be-scheduler</code>.</td>
</tr>
</tbody>
</table>
| Scheduling priority | Sets the transmission priority of the scheduler, which determines the order in which an output interface transmits traffic from the queues. | You can set the scheduling priority at different levels in the order of increasing priority from low to high. A high-priority queue with a high transmission rate might lock out lower-priority traffic. To set a priority, select one:  
  - **low**—Packets in this queue are transmitted last.  
  - **strict-high**—Packets in this queue are transmitted first.  
  - To specify no scheduling priority, select the blank check box. |
Table 239: Schedulers Configuration Page *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer size</td>
<td>Defines the size of the delay buffer.</td>
<td>To define a delay buffer size for a scheduler, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td>By default, queues 0 through 11 are allotted the following percentages of the total available buffer space:</td>
<td>• To specify no buffer size, select the blank check box.</td>
</tr>
<tr>
<td></td>
<td>• Queue 0—75 percent</td>
<td>• To specify buffer size as a percentage of the total buffer, select <strong>Percent</strong> and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>• Queue 1—0 percent</td>
<td>• To specify buffer size as the remaining available buffer, select <strong>Remainder</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Queue 2—0 percent</td>
<td><strong>NOTE:</strong> On EX8200 and EX4300 switches, you can specify the buffer size as a temporal value. The queuing algorithm will then drop packets after it has queued a computed number of bytes. This number is the product of the logical interface speed and the configured temporal value.</td>
</tr>
<tr>
<td></td>
<td>• Queue 3—5 percent</td>
<td>• To specify no buffer size, select the blank check box.</td>
</tr>
<tr>
<td></td>
<td>• Queue 4—0 percent</td>
<td>• To specify buffer size as a percentage of the total buffer, select <strong>Percent</strong> and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>• Queue 5—0 percent</td>
<td>• To specify buffer size as the remaining available buffer, select <strong>Remainder</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Queue 6—0 percent</td>
<td><strong>NOTE:</strong> A large buffer size value correlates with a greater possibility of packet delays. Such a value might not be practical for sensitive traffic such as voice or video.</td>
</tr>
<tr>
<td></td>
<td>• Queue 7—0 percent</td>
<td>• To specify no buffer size, select the blank check box.</td>
</tr>
<tr>
<td></td>
<td>• Queue 8—15 percent</td>
<td>• To specify buffer size as a percentage of the total buffer, select <strong>Percent</strong> and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td>• Queue 9—0 percent</td>
<td>• To specify buffer size as the remaining available buffer, select <strong>Remainder</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Queue 10—0 percent</td>
<td>• To specify no buffer size, select the blank check box.</td>
</tr>
<tr>
<td></td>
<td>• Queue 11—5 percent</td>
<td>• To specify no buffer size, select the blank check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To specify buffer size as a percentage of the total buffer, select <strong>Percent</strong> and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To specify buffer size as the remaining available buffer, select <strong>Remainder</strong>.</td>
</tr>
</tbody>
</table>

Shaping rate | Specifies the rate at which queues transmit packets. | To specify shaping rate as a percentage, select **Percent** and type an integer from 1 through 100. |
|-------------|-----------------------------------------------------|• To specify shaping rate as a number, select **Rate** and enter a value. |
|-------------|-----------------------------------------------------|• To specify no shaping rate, select the blank check box. |
Table 239: Schedulers Configuration Page *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit rate</td>
<td>Defines the transmission rate of a scheduler.</td>
<td>To define a transmit rate, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td>The transmit rate determines the traffic bandwidth from each forwarding class you configure.</td>
<td>• To enforce the exact transmission rate, select Rate and enter a value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To specify the remaining transmission capacity, select Remainder Available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To specify a percentage of transmission capacity, select Percent and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To specify no transmit rate, select the blank check box.</td>
</tr>
<tr>
<td>Excess rate</td>
<td>Defines the excess rate of a scheduler.</td>
<td>To define the excess rate, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To specify a percentage of the excess rate, select Percent and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To specify no excess rate, select the blank check box.</td>
</tr>
</tbody>
</table>

**Note:** This option is supported only on EX4300 switches.

Related Documentation

- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929
- Example: Configuring CoS on EX Series Switches on page 1895
- Monitoring CoS Scheduler Maps on page 1980

**Defining CoS Scheduler Maps (J-Web Procedure)**

You can use the J-Web interface to configure CoS scheduler maps on an EX Series switch.

**Note:** On EX Series switches, you cannot configure a scheduler map on an individual interface that is a member of a link aggregation group (LAG). Instead, you must configure the scheduler map on the LAG itself (that is, on the aggregated Ethernet (ae) interface).

To configure scheduler maps:
1. Select Configure > Class of Service > Scheduler Maps.

**NOTE:** After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Adds a scheduler map. Enter information into the scheduler map page as described in Table 240 on page 1935.
   - **Edit**—Modifies an existing scheduler map. Enter information into the scheduler map page as described in Table 240 on page 1935.
   - **Delete**—Deletes an existing scheduler map.

### Table 240: Scheduler Maps Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler Map Name</td>
<td>Specifies the name for a scheduler map.</td>
<td>To name a map, type the name—for example, be-scheduler-map.</td>
</tr>
<tr>
<td>Scheduler Mapping</td>
<td>Allows you to associate a preconfigured scheduler with a forwarding class.</td>
<td>To associate a scheduler with a forwarding class, locate the forwarding class and select the scheduler in the box next to it. For example, for the best-effort forwarding class, select the configured scheduler from the list.</td>
</tr>
<tr>
<td></td>
<td>After scheduler maps have been applied to an interface, they affect the hardware queues and packet schedulers.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- Defining CoS Schedulers (J-Web Procedure) on page 1931
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929
- Example: Configuring CoS on EX Series Switches on page 1895
- Monitoring CoS Scheduler Maps on page 1980

### Configuring CoS Congestion Management (CLI Procedure)

An effective congestion management mechanism is imperative to ensure smooth flow of traffic in a network and also to ensure minimum packet drops in the network. Class of service (CoS) provides congestion management methods that allow you to define parameters based on which packets can be dropped when the output queue is full. These parameters vary depending on the EX Series switch that you are using in a network.

You can specify parameters for dropping packets at the [edit class-of-service drop-profiles] hierarchy level and reference them in a scheduler configuration. The parameters that you can specify are `fill-level` and `drop-probability`. The first parameter defines the delay-buffer bandwidth, which provides packet buffer space to absorb burst traffic up
to the specified duration of delay. When the specified delay buffer becomes full, packets with 100 percent drop probability are dropped from the head of the buffer. The second parameter represents a percentage value that correlates to the likelihood that an individual packet is dropped from the network.

Depending on the switch on which you are configuring a drop profile, you can configure either a weighted tail drop (WTD) profile or a weighted random early detection (WRED) profile.

This topic describes:

- Configuring a Weighted Tail Drop Profile on page 1936
- Configuring a Weighted Random Early Detection Drop Profile on page 1936

### Configuring a Weighted Tail Drop Profile

A weighted tail drop (WTD) is a congestion management mechanism in which packets are dropped from the tail of the queue when the queue reaches a certain buffer capacity (that is, the fill level), and hence the name weighted tail drop. When that level is reached on EX2200, EX3200, or EX4200 Switches, packets marked with a packet loss priority (PLP) of high are prevented from entering the queue (that is, they are discarded).

To configure a WTD profile, create a drop profile name and assign a fill level:

```
[edit class-of-service drop-profiles]
user@switch# set profile-name fill-level percentage
```

Following is a sample WTD profile in which the fill level is set to 80 percent:

```
[edit class-of-service drop-profiles]
user@switch# set wtd-profile fill-level 80
```

### Configuring a Weighted Random Early Detection Drop Profile

A WRED drop profile enables you to define multiple data points for fill level and drop probability so that packets are dropped at various levels of queue fullness, and for various drop probabilities. Unlike the WTD drop profile that can be defined only for packets with a PLP of high, WRED can be defined for packets with a PLP of high and also for packets with a PLP of low.

**NOTE:** The WRED drop profile is supported only on EX4300 standalone switches, EX4300 Virtual Chassis, EX8200 standalone switches and EX8200 Virtual Chassis.

WRED has two implementations: segmented and interpolated. From a high level, segmented is a stair-step-like drop profile, whereas interpolated is a smother (curve) drop profile. For a graphical representation of both these implementations, see “Understanding CoS Congestion Management” on page 1875. Although the formation of graph lines is different for both these implementations, the application of the profile is the same. On EX Series switches except EX4300 switches, when a packet reaches the head of the queue, a random number between 0 and 100 is calculated. This random number is plotted against the drop profile using the current queue fullness of that
particular queue. When the random number falls above the graph line, the packet is transmitted. When the number falls below the graph line, the packet is dropped from the network.

For information about congestion management on EX4300 switches, see “Understanding CoS Congestion Management” on page 1875.

NOTE: On EX4300 switches, you cannot enable WRED on multidestination (multicast) queues. You can enable WRED only on unicast queues.

Following is the procedure to define a segmented and an interpolated drop profiles:

- To configure a segmented drop profile, specify multiple data points for fill level (l) and drop probability (p) as follows:

  ```
  [edit class-of-service drop-profiles]
  user@switch# set profile-name fill-level percentage-l1 drop-probability percentage-p1
  user@switch# set profile-name fill-level percentage-l2 drop-probability percentage-p2
  user@switch# set profile-name fill-level percentage-l3 drop-probability percentage-p3
  user@switch# set profile-name fill-level percentage-l4 drop-probability percentage-p4
  ```

  Following is a sample segmented drop profile:

  ```
  [edit class-of-service drop-profiles]
  user@switch# set seg-prof fill-level 20 drop-probability 25
  user@switch# set seg-prof fill-level 40 drop-probability 50
  user@switch# set seg-prof fill-level 60 drop-probability 75
  user@switch# set seg-prof fill-level 80 drop-probability 100
  ```

- To configure an interpolated drop profile on EX Series switches except EX4300 switches, specify multiple data points for fill level (l) and drop probability (p) using the `interpolate` statement as follows:

  ```
  [edit class-of-service drop-profiles]
  user@switch# set profile-name interpolate fill-level percentage-l1 drop-probability percentage-p1
  user@switch# set profile-name interpolate fill-level percentage-l2 drop-probability percentage-p2
  user@switch# set profile-name interpolate fill-level percentage-l3 drop-probability percentage-p3
  user@switch# set profile-name interpolate fill-level percentage-l4 drop-probability percentage-p4
  ```

  Following is a sample interpolated drop profile:

  ```
  [edit class-of-service drop-profiles]
  user@switch# set inter-prof interpolate fill-level 20 drop-probability 25
  user@switch# set inter-prof interpolate fill-level 40 drop-probability 50
  user@switch# set inter-prof interpolate fill-level 60 drop-probability 75
  user@switch# set inter-prof interpolate fill-level 80 drop-probability 100
  ```

- To configure an interpolated drop profile EX4300 switches, specify two data points for fill level (l) and drop probability (p) by using the `interpolate` statement as follows:

  ```
  [edit class-of-service drop-profiles]
  user@switch# set profile-name interpolate fill-level percentage-l1 fill-level percentage-l2 drop-probability percentage-l1 percentage-l2
  ```

  Following is a sample interpolated drop profile:
[edit class-of-service drop-profiles]
user@switch#  set inter-prof interpolate fill-level 20 fill-level 80 drop-probability 25
       drop-probability 100

Related Documentation
• Example: Configuring CoS on EX Series Switches on page 1895
• Understanding CoS Congestion Management on page 1875

Defining CoS Drop Profiles (J-Web Procedure)

You can use the J-Web interface to define CoS drop profiles on EX4500 and EX8200 switches.

To configure CoS drop profiles:
1. Select Configure > Class of Service > Drop Profile.

NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Optionsto Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   • Add—Adds a drop profile. Enter information into the drop profiles page as described in Table 241 on page 1938.
   • Edit—Modifies an existing drop file. Enter information into the drop profiles page as described in Table 241 on page 1938.
   • Delete—Deletes an existing drop profile.

Table 241: Drop Profiles Configuration parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop Profile Name</td>
<td>Specifies the name for a drop profile.</td>
<td>Type the name.</td>
</tr>
<tr>
<td>Drop profile graph</td>
<td>Specifies the drop profile graph type</td>
<td>Select one: Segmented or Interpolated.</td>
</tr>
</tbody>
</table>
| Drop profile values        | Specifies values for the following two parameters of the drop profile: the queue fill level and the drop probability. | To add new values:
|                            | The queue fill level represents a percentage of the memory used to store packets in relation to the total amount that has been allocated for that specific queue. | 1. Click Add. |
|                            | The drop probability is a percentage value that correlates to the likelihood that an individual packet is dropped from the network. | 2. Enter the fill level. |
|                            | To edit an existing value, click Edit and modify the fill level and drop probability. | 3. Enter the drop probability. |
|                            | To delete a value, select it and click Delete. | 4. Click OK. |
Related Documentation

- Monitoring CoS Drop Profiles on page 1982
- Example: Configuring CoS on EX Series Switches on page 1895

Defining CoS Rewrite Rules (CLI Procedure)

You configure rewrite rules to alter CoS values in outgoing packets on the outbound interfaces of an EX Series switch to match the policies of a targeted peer. Policy matching allows the downstream routing platform or switch in a neighboring network to classify each packet into the appropriate service group.

To configure a CoS rewrite rule, create the rule by giving it a name and associating it with a forwarding class, loss priority, and a code point, thus creating a rewrite table, and you can enable the rewrite rule on an interface. On EX Series switches except EX4300 switches, you can also enable a rewrite rule on routed VLAN interfaces (RVIs). On EX4300 switches, you can also enable rewrite rules on integrated routing and bridging (IRB) interfaces. If you need to customize a rewrite rule, you can create a customized rewrite rule using a firewall filter configuration. You can configure CoS rewrite rules for DSCP, IP precedence and IEEE 802.1p.

You can configure rewrite rules for the following CoS marker types:

- **dscp** and **dscp-ipv6**—Handles incoming IPv4 and IPv6 packets, respectively. On EX4300 switches, you cannot configure DSCP IPv4 and DSCP IPv6 rewrite rules on the same interface. If you configure a DSCP IPv4 rewrite rule on an interface to rewrite IPv4 traffic, then the same rewrite rule is applied to IPv6 traffic also on that interface, and vice versa.

- **ieee-802.1**—Handles Layer 2 CoS.

- **inet-precedence**—Handles incoming IPv4 packets. IP precedence mapping requires only the higher order three bits of the DSCP field.

**NOTE:** To replace an existing rewrite rule on the interface with a new rewrite rule of the same type, first explicitly remove the rewrite rule and then apply the new rule.

To create IEEE 802.1p rewrite rules and enable them on Layer 2 interfaces:

To create an IEEE 802.1p rewrite rule named customup-rw in the rewrite table for all Layer 2 interfaces:

```plaintext
[edit class-of-service rewrite-rules]
user@switch# set ieee-802.1 customup-rw forwarding-class be loss-priority low code-point 000
user@switch# set ieee-802.1 customup-rw forwarding-class be loss-priority high code-point 001
user@switch# set ieee-802.1 customup-rw forwarding-class af loss-priority low code-point 010
user@switch# set ieee-802.1 customup-rw forwarding-class af loss-priority high code-point 011
```
user@switch# set ieee-802.1 custom-up-rw forwarding-class ef loss-priority low code-point 100
user@switch# set ieee-802.1 custom-up-rw forwarding-class ef loss-priority high code-point 101
user@switch# set ieee-802.1 custom-up-rw forwarding-class nc loss-priority low code-point 110
user@switch# set ieee-802.1 custom-up-rw forwarding-class nc loss-priority high code-point 111

- To enable an IEEE 802.1p rewrite rule named custom-up-rw on a Layer 2 interface:

  [edit]
  user@switch# set class-of-service interfaces ge-0/0/0 unit 0 rewrite-rules ieee-802.1 custom-up-rw

  (On EX4300 switches) To enable an IEEE 802.1p rewrite rule named custom-up-rw on a Layer 2 interface:

  [edit]
  user@switch# set class-of-service interfaces ge-0/0/0 rewrite-rules ieee-802.1 custom-up-rw

- To enable an IEEE 802.1p rewrite rule named custom-up-rw on all Gigabit Ethernet interfaces on the switch, use wildcards for the interface name and logical-interface (unit) number:

  [edit]
  user@switch# set class-of-service interfaces ge-* unit * rewrite-rules custom-up-rw

  (On EX4300 switches) To enable an IEEE 802.1p rewrite rule named custom-up-rw on all Gigabit Ethernet interfaces on the switch, use wildcards for the interface name:

  [edit]
  user@switch# set class-of-service interfaces ge-* rewrite-rules custom-up-rw

Related Documentation
- Defining CoS Rewrite Rules (J-Web Procedure) on page 1940
- Example: Configuring CoS on EX Series Switches on page 1895
- Monitoring CoS Rewrite Rules on page 1979
- Understanding CoS Rewrite Rules on page 1887

Defining CoS Rewrite Rules (J-Web Procedure)

You can use the J-Web interface to define CoS rewrite rules. Use the rewrite rules to alter the CoS values in outgoing packets to meet the requirements of the targeted peer. A rewrite rule examines the forwarding class and loss priority of a packet and sets its bits to a corresponding value specified in the rule.

To define rewrite rules:

1. Select Configure > Class of Service > Rewrite Rules.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.
2. Click one of the following options:

- **Add**—Adds a rewrite rule. Enter information into the rewrite rule page as described in Table 242 on page 1941.

- **Edit**—Modifies an existing rewrite rule. Enter information into the rewrite rule page as described in Table 242 on page 1941.

- **Delete**—Deletes an existing rewrite rule.

Table 242: Rewrite Rules Configuration Page Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rewrite Rule Name</td>
<td>Specifies the name for the rewrite rule.</td>
<td>To name a rule, type the name—for example, rewrite-dscps.</td>
</tr>
<tr>
<td>Rewrite rule type</td>
<td>Specifies the type of rewrite rule: dscp, ieee-802.1, or inet-precedence.</td>
<td>Select a value from the list.</td>
</tr>
</tbody>
</table>
| Code Point Mapping  | Rewrites outgoing CoS values of a packet based on the forwarding class and loss priority. Allows you to remove a code point mapping entry. | To configure a CoS value assignment, follow these steps: 

1. Click **Add**.

2. Select the code point.

3. Select a forwarding class from the following list:

   - **expedited-forwarding**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. Packets can be forwarded out of sequence or dropped.
   - **best-effort**—Provides no special CoS handling of packets. Typically, RED drop profile is aggressive and no loss priority is defined.
   - **assured-forwarding**—Provides high assurance for packets within the specified service profile. Excess packets are dropped.
   - **network-control**—Packets can be delayed but not dropped.

4. Select the loss priority.

   To assign a loss priority, select one:

   - **high**—Packet has a high loss priority.
   - **low**—Packet has a low loss priority.

To edit an existing code point mapping, select it and click **Edit**.

To remove a code point mapping entry, select it and click **Remove**.
Assigning CoS Components to Interfaces (CLI Procedure)

After you have defined the following CoS components, you must assign them to logical or physical interfaces.

- Forwarding classes—Assign only to logical interfaces.
- Classifiers—Assign only to logical interfaces.
- Scheduler maps—Assign to either physical or logical interfaces.
- Rewrite rules—Assign to either physical or logical interfaces.

You can assign a CoS component to a single interface or to multiple interfaces using wild cards.

To assign CoS components to interfaces:

- To assign CoS components to a single interface, associate a CoS component (for example a scheduler map named `ethernet-cos-map`) with an interface:

  ```
  [edit class-of-service interfaces]
  user@switch# set ge-0/0/20 scheduler-map ethernet-cos-map
  ```

- To assign a CoS component to multiple interfaces, associate a CoS component (for example, a rewrite rule named `customup-rw`) to all Gigabit Ethernet interfaces on the switch, use wild characters for the interface name and logical-interface (unit) number:

  ```
  [edit class-of-service interfaces]
  user@switch# set ge-* unit* rewrite-rules ieee-802.1 customup-rw
  ```

Related Documentation

- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942
- Example: Configuring CoS on EX Series Switches on page 1895
- Monitoring Interfaces That Have CoS Components on page 1978
- Understanding Junos OS CoS Components for EX Series Switches on page 1863

Assigning CoS Components to Interfaces (J-Web Procedure)

After you have defined CoS components on an EX Series switch, you must assign them to logical or physical interfaces. You can use the J-Web interface to assign scheduler maps to physical or logical interfaces and to assign forwarding classes or classifiers to logical interfaces.

To assign CoS components to interfaces:
1. Select Configure > Class of Service > Assign to Interface.

**NOTE:** After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. To configure interface association, select an interface from the list and click Edit. For an EX8200 Virtual Chassis configuration, select the member, the FPC, and the interface from the list, and click Edit.

3. Select one of the following:
   - Associate system default scheduler map—Associates the interface with the default scheduler map.
   - Select the scheduler map—Associates the interface with a configured scheduler map. Select the scheduler map from the list.

**NOTE:** On the 40-port SFP+ line card for EX8200 switches, the J-Web interface does not allow you to commit your changes unless you assign the same scheduler map or the default scheduler map to all interfaces in a port group.

4. Click OK.

5. To manage a CoS service assignment on a logical interface, Click one of the following options:
   - Add—Adds a CoS service to a logical interface on a specified physical interface. Enter information as described in Table 243 on page 1943.
   - Edit—Modifies a CoS service assignment to a logical interface. Enter information as described in Table 243 on page 1943.
   - Delete—Deletes the CoS service assignment to a logical interface.

**Table 243: Assigning CoS Components to Logical Interfaces**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td>Specifies the name of a logical interface. Allows you to assign CoS components while configuring a logical interface on a physical interface at the same time.</td>
<td>Type the interface name. To assign CoS services to all logical interfaces configured on this physical interface, type the wildcard character (*).</td>
</tr>
<tr>
<td>Forwarding Class</td>
<td>Assigns a predefined forwarding class to incoming packets on a logical interface.</td>
<td>To assign a forwarding class to an interface, select the forwarding class.</td>
</tr>
</tbody>
</table>
Table 243: Assigning CoS Components to Logical Interfaces (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifiers</td>
<td>Allows you to apply classification maps to a logical interface.</td>
<td>To assign a classification map to an interface, select an appropriate classifier for each CoS value type used on the interface.</td>
</tr>
<tr>
<td></td>
<td>Classifiers assign a forwarding class and loss priority to an incoming packet based on its CoS value.</td>
<td></td>
</tr>
<tr>
<td>Rewrite Rules</td>
<td>Allows you to alter the CoS values in outgoing packets to meet the requirements of the targeted peer. A rewrite rule examines the forwarding class and loss priority of a packet and sets its bits to a corresponding value specified in the rule.</td>
<td>To assign rewrite rules to the interface, select the appropriate rewrite rule for each CoS value type used on the interface.</td>
</tr>
</tbody>
</table>

**NOTE:** In EX4300 switches, this option is available only when you click Edit button in the Configure Interface Association table.

**Related Documentation**
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942
- Example: Configuring CoS on EX Series Switches on page 1895
- Monitoring Interfaces That Have CoS Components on page 1978

**Configuring Junos OS EZQoS for CoS (CLI Procedure)**

You use Junos OS EZQoS on EX Series switches to eliminate the complexities involved in configuring class of service (CoS) across the network. EZQoS offers templates for key traffic classes.

When you configure EZQoS on EX Series switches, preconfigured values are assigned to all CoS parameters based on the typical application requirements. These preconfigured values are stored in a template with a unique name.

**NOTE:** Currently, we provide an EZQoS template for configuring CoS for VoIP applications. The EZQoS VoIP template is stored in /etc/config/ezqos-voip.conf.

To configure EZQoS using the CLI:

1. Load the EZQoS configuration file (/etc/config/ezqos-voip.conf):

   ```
   [edit]
   user@switch# load merge /etc/config/ezqos-voip.conf
   ```

2. Apply the EZQoS group (ezqos-voip):

   ```
   [edit]
   user@switch# set apply-groups ezqos-voip
   ```

3. Apply the DSCP classifier (ezqos-dscp-classifier) to a Gigabit Ethernet interface (ge-0/0/0):

   ```
   [edit class-of-service interfaces]
   ```
user@switch# set ge-0/0/0 unit 0 classifiers dscp ezqos-dscp-classifier

4. Apply the scheduler map (ezqos-voip-sched-maps) to a Gigabit Ethernet interface (ge-0/0/1):

[edit class-of-service interfaces]
user@switch# set ge-0/0/1 scheduler-map ezqos-voip-sched-maps

Related Documentation
• Example: Configuring CoS on EX Series Switches on page 1895
• Understanding Junos OS EZQoS for CoS Configurations on EX Series Switches on page 1890

Configuring CoS Traffic Classification for Ingress Queuing on Oversubscribed Ports on EX8200 Line Cards (CLI Procedure)

EX8200 switches provide certain line cards that include oversubscribed ports. These ports are logically grouped into a port group and each port group share a certain fixed bandwidth. Because oversubscribed ports handle traffic differently than ports that provide continuous line-rate bandwidth, configuring CoS queues is different for oversubscribed ports than for line-rate ports.

Packets arriving on an oversubscribed port in a line card are directed to a high-priority, low priority, or line-rate queue. These queues are used for scheduling traffic from the port into the Packet Forwarding Engine. The fabric priority associated with the packet’s forwarding class determines which queue the packet is sent to. The forwarding class of the packet in turn is determined by the behavior aggregate (BA) classifier assigned to the port. By default, the fabric priority of all forwarding classes is low. Thus all packets, with the exception of critical network packets and line-rate packets, are sent to the low-priority ingress queue by default. The critical network packets and line-rate packets do not need a BA classifier as they are always sent on the high-priority and line-rate queues, respectively.

This procedure describes how you can direct traffic into the high-priority ingress queue and thus avoid congestion at the port group.

To direct traffic to the high-priority ingress queue for a port group:

1. Create the BA classifier for the forwarding class:

   [edit class-of-service]
   user@switch# set classifiers classifier-type classifier-name
   forwarding-class class-name loss-priority level code-points code-point

2. Assign a queue number and fabric priority to the forwarding class:

   [edit class-of-service]
   user@switch# set forwarding-classes class class-name queue-num number
   priority level

3. Assign the BA classifier to the physical interface:

   [edit class-of-service]
   user@switch# set interfaces interface-name unit 0
   classifiers classifier-type classifier-name
For example, to direct voice traffic to the high-priority ingress queue for interface xe-1/0/2:

```
[edit class-of-service]
user@switch# set classifiers dscp dscp1 forwarding-class cos-voice
  loss-priority low code-points ef

[edit class-of-service]
user@switch# set forwarding-classes class cos-voice queue-num 5 priority high

[edit class-of-service]
user@switch# set interfaces xe-1/0/2 unit 0 classifiers dscp dscp1
```

**NOTE:** You must use a BA classifier to classify traffic for ingress queuing. Multifield (MF) classification and port classification (that is, assigning a forwarding class to the interface) are not supported for classifying traffic for ingress queuing. The BA classifier must be assigned to a physical interface, not a Layer 3 tagged interface or a routed VLAN interface (RVI).

---

**Related Documentation**

- Understanding CoS Queues on EX8200 Line Cards That Include Oversubscribed Ports on page 1891

---

**Configuration Statements**

- [edit class-of-service] Configuration Statement Hierarchy on EX Series Switches on page 1946

---

**[edit class-of-service] Configuration Statement Hierarchy on EX Series Switches**

This topic lists supported and unsupported configuration statements in the [edit class-of-service] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.

- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27

This topic lists:

- Supported Statements in the [edit class-of-service] Hierarchy Level on page 1946
- Unsupported Statements in the [edit class-of-service] Hierarchy Level on page 1948

---

**Supported Statements in the [edit class-of-service] Hierarchy Level**

The following hierarchy shows the [edit class-of-service] configuration statements supported on EX Series switches:

```
class-of-service {
```
classifiers {
    (dscp | dscp-ipv6 | ieee-802.1 | inet-precedence) classifier-name {
        forwarding-class class-name {
            loss-priority (high | low | medium-high | medium-low) {
                code-points [ aliases ] [ 6 bit-patterns ];
            }
        }
        import (classifier-name | default);
    }
}
code-point-aliases {
    (dscp | dscp-ipv6 | ieee-802.1 | inet-precedence) {
        alias-name bits;
    }
}
drop-profiles {
    profile-name {
        interpolate {
            drop-probability [values];
            fill-level [values]
        }
    }
}
forwarding-classes {
    class class-name
    queue queue-number;
}
interfaces interface-name {
    scheduler-map map-name;
    shaping-rate rate;
    unit (logical-unit-number | *) {
        classifiers {
            (dscp | dscp-ipv6 | ieee-802.1 | inet-precedence) (classifier-name | default);
        }
        forwarding-class class-name;
    }
}
rewrite-rules {
    (dscp | dscp-ipv6 | ieee-802.1 | inet-precedence) (rewrite-rule-name | default);
}
}
rewrite-rules {
    (dscp | dscp-ipv6 | ieee-802.1 | inet-precedence) rewrite-name {
        import (default | rewrite-name);
        forwarding-class class-name {
            loss-priority (high | low | medium-high | medium-low) code-point (alias | bits);
        }
    }
}
scheduler-maps {
    map-name {
        forwarding-class class-name {
            scheduler scheduler-name;
        }
    }
}
schedulers {
    scheduler-name {
        buffer-size (exact | percent percentage | remainder);
        drop-profile-map {
            loss-priority (any | high | medium-high | medium-low);
            protocol any;
            {
                drop-profile profile-name
            }
        }
        excess-rate {
            percent percentage;
        }
        priority (low | strict-high);
        shaping-rate (rate | percent percentage);
        transmit-rate (EX Series Switches) (rate | percent percentage | remainder);
    }
} shared-buffer {
    percent;
} traceoptions {
    file (file-name | files files | match match | no-world-readable | size size | world-readable);
    flag (all | asynch | chassis-scheduler | cos-adjustment | dynamic | hardware-database | init | parse | performance-monitor | process | restart | route-socket | show | snmp | util);
    no-remote-trace;
    tri-color;
}

Unsupported Statements in the [edit class-of-service] Hierarchy Level
All statements in the [edit class-of-service] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921 or Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927 or Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
- Configuring CoS Tail Drop Profiles (CLI Procedure)
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining CoS Schedulers (J-Web Procedure) on page 1931
### broadcast

**Syntax**  
`broadcast forwarding-class-name;`

**Hierarchy Level**  
`[edit class-of-service multi-destination family ethernet]`

**Release Information**  
Statement introduced in Junos OS Release 9.5 for EX Series switches.

**Description**  
Specify the forwarding class for the broadcast traffic belonging to the Ethernet family.

**Options**  
`forwarding-class-name` — Name of the forwarding class:
- `mcast-af` — Default forwarding class for assured forwarding of multicast traffic.
- `mcast-be` — Default best-effort forwarding class for multicast traffic.
- `mcast-ef` — Default forwarding class for expedited forwarding of multicast traffic.

**Required Privilege**  
`interface`—To view this statement in the configuration.
`interface-control`—To add this statement to the configuration.

**Related Documentation**
- Understanding CoS Schedulers on page 1880
- Understanding CoS Forwarding Classes
- Understanding CoS Classifiers
buffer-size

Syntax  buffer-size (exact | percent percentage | remainder | temporal);

Hierarchy Level  [edit class-of-service schedulers scheduler-name]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify buffer size in a scheduler configuration.

Default  On EX Series switches except EX4300 switches, the default scheduler transmission rate
and buffer size percentages for queues 0 through 7 are 95, 0, 0, 0, 0, 0, 0, and 5 percent,
respectively. On EX4300 switches, the default scheduler transmission rate and buffer
size for queues 0 through 11 are 75, 0, 5, 0, 0, 0, 0, 0, 15, 0, 0 and 5 percent, respectively,
of the total available buffer.

Options  exact—(Except on EX8200 standalone switches and EX8200 Virtual Chassis) Enforce
the exact buffer size. When this option is configured, sharing is disabled on the queue,
restricting the usage to guaranteed buffers only.

percent percentage—Buffer size as a percentage of the total buffer.

remainder—Remaining buffer available.

temporal—(EX4200 standalone switches, EX4200 Virtual Chassis, EX4300 standalone
switches, EX4300 Virtual Chassis, EX8200 standalone switches, and EX8200 Virtual
Chassis only) Buffer size as a temporal value.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring CoS on EX Series Switches on page 1895
• Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining
  CoS Schedulers (J-Web Procedure) on page 1931
• Understanding CoS Schedulers on page 1880
classifiers

Syntax  classifiers {
  (dscp | dscp-ipv6 | leee-802.1 | inet-precedence) classifier-name {
    import (classifier-name | default);
    forwarding-class class-name {
      loss-priority level {
        code-points [aliases] [6–bit-patterns];
      }
    }
  }
}

Hierarchy Level [edit class-of-service],
[edit class-of-service interfaces interface-name unit logical-unit-number]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.
Expanded to include EXP classifiers in Junos OS Release 10.1 for EX Series switches.

Description Apply a CoS aggregate behavior classifier to a logical interface. You can apply a default classifier or a custom classifier.

The remaining statements are explained separately.

Required Privilege level

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring CoS on EX Series Switches on page 1895
- Example: Combining CoS with MPLS on EX Series Switches
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942 or Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942
- Understanding CoS Classifiers
**code-point-aliases**

**Syntax**

```
code-point-aliases {
  (dscp | dscp-ipv6 | ieee-802.1 | inet-precedence) {{
    alias-name bits;
  }
}
```

**Hierarchy Level**

[edit class-of-service]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Define an alias for a CoS marker.

The remaining statement is explained separately.

**Required Privilege**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921 or Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Understanding CoS Code-Point Aliases on page 1866

---

**code-points**

**Syntax**

```
code-points [ aliases ] [ 6 bit-patterns ];
```

**Hierarchy Level**

[edit class-of-service classifiers (dscp | ieee-802.1 | inet-precedence) forwarding-class class-name loss-priority level]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Specify one or more DSCP code-point aliases or bit sets for association with a forwarding class.

**Options**

- **aliases** —Name of the DSCP alias.
- **6 bit-patterns** —Value of the code-point bits, in decimal form.

**Required Privilege**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Understanding CoS Classifiers
drop-profile-map

Syntax:  
drop-profile-map loss-priority loss-priority protocol protocol drop-profile profile-name;

Hierarchy Level:  
[edit class-of-service schedulers scheduler-name]

Release Information:  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description:  
Define the loss priority value for the specified drop profile.

Options:  
drop-profile profile-name —Name of the drop profile.

The remaining statements are explained separately.

Required Privilege Level:  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Related Documentation:  
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining CoS Schedulers (J-Web Procedure) on page 1931
- Understanding CoS Schedulers on page 1880
### dscp

**Syntax**

```
dscp classifier-name {
  import (classifier-name | default);
  forwarding-class class-name {
    loss-priority level {
      code-points [ aliases ] [ 6-bit-patterns ];
    }
  }
}
```

**Hierarchy Level**

- [edit class-of-service classifiers],
- [edit class-of-service code-point-aliases],
- [edit class-of-service interfaces interface-name unit logical-unit-number classifiers],
- [edit class-of-service rewrite-rules]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Define the Differentiated Services code point (DSCP) mapping that is applied to the packets.

**Options**

- `classifier-name`—Name of the classifier.

The remaining statements are explained separately.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921 or Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942 or Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942
- Understanding CoS Classifiers
**dscp-ipv6**

**Syntax**
```
dscp-ipv6 classifier-name {
    import (classifier-name | default);
    forwarding-class class-name {
        loss-priority level {
            code-points [aliases] [6–bit-patterns];
        }
    }
}
```

**Hierarchy Level**
```
[edit class-of-service classifiers],
[edit class-of-service code-point-aliases],
[edit class-of-service interfaces interface-name unit logical-unit-number classifiers]
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]
```

**Release Information**
Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**
Define the Differentiated Services code point (DSCP) mapping that is applied to the IPv6 packets.

**Options**
- `classifier-name`—Name of the classifier.

The remaining statements are explained separately.

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921 or Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942 or Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942
- Understanding CoS Classifiers
ethernet (CoS for Multidestination Traffic)

Syntax

```
ethernet {
  broadcast forwarding-class-name;
}
```

Hierarchy Level

[edit class-of-service multi-destination family]

Release Information

Statement introduced in Junos OS Release 9.5 for EX Series switches.

Description

Specify the Ethernet broadcast traffic family.

The remaining statement is explained separately.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Understanding CoS Schedulers on page 1880
- Understanding CoS Forwarding Classes
- Understanding CoS Classifiers

excess-rate (Schedulers)

Syntax

```
excess-rate {
  percent percentage;
}
```

Hierarchy Level

[edit class-of-service on page 1946 schedulers scheduler-name]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

(EX4300 switches only) Specify the percentage of excess bandwidth traffic to share.

Default

Excess bandwidth is shared in proportion to the configured transmit rate of each queue.

Options

- percent—Percentage of the excess bandwidth to share.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Understanding CoS Schedulers on page 1880
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining CoS Schedulers (J-Web Procedure) on page 1931
- Example: Configuring CoS on EX Series Switches on page 1895
**family**

**Syntax**

```plaintext
family {
  ethernet {
    broadcast forwarding-class-name;
  }
  inet {
    classifiers{
      (dscp | ieee-802.1 | inet-precedence) classifier-name;
    }
  }
}
```

**Hierarchy Level**
[edit class-of-service multi-destination]

**Release Information**
Statement introduced in Junos OS Release 9.5 for EX Series switches.

**Description**
Specify the multidestination traffic family.

The remaining statements are explained separately.

**Required Privilege Level**
interface—To view this statement in the configuration.interface-control—To add this statement to the configuration.

**Related Documentation**
- Understanding CoS Schedulers on page 1880
- Understanding CoS Forwarding Classes
- Understanding CoS Classifiers
forwarding-class

Syntax

```plaintext
forwarding-class class-name {
  loss-priority level {
    code-points [aliases] [6–bit-patterns];
  }
}
```

Hierarchy Level

- `[edit class-of-service classifiers (dscp | ieee-802.1 | inet-precedence) classifier-name]`
- `[edit class-of-service interfaces interface-name unit logical-unit-number]`
- `[edit class-of-service rewrite-rules] (dscp | ieee-802.1 | inet-precedence) rewrite-rule-name`
- `[edit class-of-service scheduler-maps map-name]`
- `[edit class-of-service host-outbound-traffic]`

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Define forwarding class name and option values.

Options

class-name — Name of the forwarding class.

The remaining statements are explained separately.

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927 or Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
- Understanding CoS Forwarding Classes
forwarding-classes

Syntax
forwarding-classes {
   class class-name queue-num queue-number priority (high | medium-high | low | medium-low);
}

Hierarchy Level  [edit class-of-service]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Associate the forwarding class with a queue name and number.

   The statement is explained separately.

Required Privilege Level
   interface—To view this statement in the configuration.
   interface-control—To add this statement to the configuration.

Related Documentation
   • Example: Configuring CoS on EX Series Switches on page 1895
   • Defining CoS Forwarding Classes (CLI Procedure) on page 1927 or Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
   • Understanding CoS Forwarding Classes
**IEEE-802.1**

**Syntax**
```
ieee-802.1 classifier-name {
    import (classifier-name | default);
    forwarding-class class-name {
        loss-priority level {
            code-points [ aliases ] [ 6 bit-patterns ];
        }
    }
}
```

**Hierarchy Level**
- [edit class-of-service classifiers],
- [edit class-of-service code-point-aliases],
- [edit class-of-service interfaces interface-name unit logical-unit-number classifiers],
- [edit class-of-service rewrite-rules]

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Apply an IEEE-802.1 rewrite rule.

**Options**
- `classifier-name` — Name of the classifier.

The remaining statements are explained separately.

**Required Privilege Level**
- interface — To view this statement in the configuration.
- interface-control — To add this statement to the configuration.

**Related Documentation**
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921 or Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Understanding CoS Classifiers
- Understanding CoS Rewrite Rules on page 1887
**Syntax**

```plaintext
import (classifier-name | default);
```

**Hierarchy Level**

```plaintext
[edit class-of-service classifiers (dscp | ieee-802.1 | inet-precedence) classifier-name].
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Specify a default or previously defined classifier.

**Options**

- `classifier-name` — Name of the classifier mapping configured at the [edit class-of-service classifiers] hierarchy level.
- `default` — Default classifier mapping.

**Required Privilege Level**

- `interface` — To view this statement in the configuration.
- `interface-control` — To add this statement to the configuration.

**Related Documentation**

- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- **Understanding CoS Classifiers**
- Understanding CoS Rewrite Rules on page 1887
inet-precedence

Syntax
inet-precedence classifier-name {
    import (classifier-name | default);
    forwarding-class class-name {
        loss-priority level {
            code-points [ aliases ] [ 6-bit-patterns ];
        }
    }
}

Hierarchy Level
[edit class-of-service classifiers],
[edit class-of-service code-point-aliases],
[edit class-of-service interfaces interface-name unit logical-unit-number classifiers],
[edit class-of-service rewrite-rules]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Apply an IPv4 precedence rewrite rule.

Options
classifier-name—Name of the classifier.

The remaining statements are explained separately.

Required Privilege
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921 or Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Understanding CoS Classifiers
- Understanding CoS Rewrite Rules on page 1887
interfaces

Syntax

```
interfaces {
  interface-name {
    congestion-notification-profile profile-name {
      input {
        ieee-802.1 {
          code-point up-bits pfc;
        }
      }
    }
  }
  scheduler-map map-name;
  unit logical-unit-number {
    forwarding-class class-name;
    classifiers {
      (dscp | ieee-802.1 | inet-precedence) (classifier-name | default);
    }
  }
}
```

Hierarchy Level
[edit class-of-service]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure interface-specific class-of-service (CoS) properties for incoming packets.

Options
- `interface-name`—Name of the interface.
  The remaining statements are explained separately.

Required Privilege Level
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

Related Documentation
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927 or Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining CoS Schedulers (J-Web Procedure) on page 1931
- Configuring Priority-Based Flow Control for an EX Series Switch (CLI Procedure)
**loss-priority (Classifiers and Rewrite Rules)**

**Syntax**

```
loss-priority level {
    code-points [aliases] [6-bit-patterns | 3-bit-patterns];
}
```

**Hierarchy Level**

```
[edit class-of-service classifiers (dscp | ieee-802.1 | inet-precedence | exp) classifier-name
    forwarding-class class-name],
[edit class-of-service rewrite-rules (dscp | ieee-802.1 | inet-precedence | exp)
    rewrite-rule-name forwarding-class class-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement expanded to apply to EXP classifiers in Junos OS Release 10.1 for EX Series switches.

**Description**

Specify packet loss priority value for a specific set of code-point aliases and bit patterns.

**Options**

`level` — Can be one of the following:

- **high** — Packet has high loss priority.
- **medium-high** — (On EX3200, EX4200, EX4300, and EX4500 switches only) Code points to classify to loss priority medium-high.
- **low** — Packet has low loss priority.
- **medium-low** — (On EX3200, EX4200, EX4300, and EX4500 switches only) Code points to classify to loss priority medium-low.

The remaining statement is explained separately.

**Required Privilege**

- **interface** — To view this statement in the configuration.
- **interface-control** — To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring CoS on EX Series Switches on page 1895](#)
- [Defining CoS Classifiers (CLI Procedure) on page 1923 or Defining CoS Classifiers (J-Web Procedure) on page 1925](#)
- [Understanding CoS Classifiers](#)
- [Understanding CoS Rewrite Rules on page 1887](#)
## policing

**Syntax**  
```plaintext```
policing (filter filter-name | no-automatic-policing);
```

**Hierarchy Level**  
- [edit protocols mpls label-switched-path lsp-name]
- [edit interfaces interface-id unit number-of-logical-unit family inet address ip-address]

**Release Information**  
Statement introduced in Junos OS Release 10.1 for EX Series switches.

**Description**  
Apply a rate-limiting policer as the specified policing filter:
- To the LSP for MPLS over CCC.
- To the customer-edge interface for IP over MPLS.

**Options**  
- `filter filter-name`—Specify the name of the policing filter.
- `no-automatic-policing`—Disable automatic policing on this LSP.

**Required Privilege Level**  
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**  
- [policer on page 4246](#)
- [Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206](#)
- [Configuring CoS on an MPLS Provider Edge Switch Using Circuit Cross-Connect (CLI Procedure)](#)
- [Configuring CoS on an MPLS Provider Edge Switch Using IP Over MPLS (CLI Procedure)](#)
priority (Schedulers)

Syntax

priority priority;

Hierarchy Level

[edit class-of-service schedulers scheduler-name]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify packet-scheduling priority value.

Options

priority — It can be one of the following:

- low—Scheduler has low priority.
- strict-high—Scheduler has strictly high priority.

Required Privilege

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining CoS Schedulers (J-Web Procedure) on page 1931
- Understanding CoS Schedulers on page 1880

protocol (Drop Profiles)

Syntax

protocol protocol drop-profile profile-name;

Hierarchy Level

[edit class-of-service schedulers scheduler-name]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Specify the protocol type for the specified drop profile.

Options

drop-profile profile-name — Name of the drop profile.

protocol — Type of protocol. It can be:

- any—Accept any protocol type.

Required Privilege

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring CoS on EX Series Switches on page 1895
- Configuring CoS Tail Drop Profiles (CLI Procedure)
- Understanding CoS Tail Drop Profiles
**rewrite-rules**

**Syntax**

```
rewrite-rules {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) rewrite-name {
    import (default | rewrite-name);
    forwarding-class class-name {
      loss-priority level code-point (alias | bits);
    }
  }
}
```

**Hierarchy Level**

[edit class-of-service]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement expanded for use with global EXP classifiers in Junos OS Release 10.1 for EX Series switches.

**Description**

Specify a rewrite-rules mapping for the traffic that passes through all queues on the interface.

The remaining statements are explained separately.

**Required Privilege**

- **Level**
  - interface—To view this statement in the configuration.
  - interface-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring CoS on EX Series Switches on page 1895
- Understanding CoS Rewrite Rules on page 1887
- Understanding Using CoS with MPLS Networks on EX Series Switches
**scheduler-map**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>scheduler-map <code>map-name</code>;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit class-of-service <code>interfaces</code>], [edit class-of-service multi-destination]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 9.0 for EX Series switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Associate a scheduler map name with an interface or with a multidestination traffic configuration.</td>
</tr>
<tr>
<td>Options</td>
<td><code>map-name</code> — Name of the scheduler map.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td></td>
</tr>
<tr>
<td>interface — To view this statement in the configuration.</td>
<td></td>
</tr>
<tr>
<td>interface-control — To add this statement to the configuration.</td>
<td></td>
</tr>
<tr>
<td>Related Documentation</td>
<td></td>
</tr>
<tr>
<td>Example: Configuring CoS on EX Series Switches on page 1895</td>
<td></td>
</tr>
<tr>
<td>Assigning CoS Components to Interfaces (CLI Procedure) on page 1942 or Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942</td>
<td></td>
</tr>
<tr>
<td>Understanding CoS Schedulers on page 1880</td>
<td></td>
</tr>
<tr>
<td>Understanding CoS Classifiers</td>
<td></td>
</tr>
</tbody>
</table>
scheduler-maps

Syntax

scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}

Hierarchy Level  [edit class-of-service]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify a scheduler map name and associate it with the scheduler configuration and forwarding class.

Options  map-name —Name of the scheduler map.

The remaining statement is explained separately.

Required Privilege

Level  interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring CoS on EX Series Switches on page 1895
• Defining CoS Forwarding Classes (CLI Procedure) on page 1927 or Defining CoS Forwarding Classes (J-Web Procedure) on page 1927
• Understanding CoS Schedulers on page 1880
• Understanding CoS Forwarding Classes
**schedulers (CoS)**

**Syntax**

```
schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder);
        drop-profile-map loss-priority protocol drop-profile profile-name;
        excess-rate (percent percentage);
        priority priority;
        shaping-rate (rate | percent percentage);
        transmit-rate (EX Series Switches) (rate | percent percentage | remainder);
    }
}
```

**Hierarchy Level**  
[edit class-of-service]

**Release Information**  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Specify scheduler name and parameter values.

**Options**  
`scheduler-name` — Name of the scheduler.

The remaining statements are explained separately.

**Required Privilege**

`interface`—To view this statement in the configuration.  
`interface-control`—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining CoS Schedulers (J-Web Procedure) on page 1931
- Understanding CoS Schedulers on page 1880
shaping-rate

Syntax:  
```
shaping-rate (percent percentage | rate);
```

Hierarchy Level:  
```
[edit class-of-service schedulers (CoS) scheduler-name]
```

Release Information:  
Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description:  
Configure shaping rate to throttle the rate at which queues transmit packets.
We recommend that you configure the shaping rate as an absolute maximum usage and not as additional usage beyond the configured transmit rate.

Default:  
If you do not include this statement, the default shaping rate is 100 percent, which is the same as no shaping at all.

Options:  
- `percentpercentage` — Shaping rate as a percentage of the available interface bandwidth.  
  Range: 0 through 100 percent
- `rate` — Peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).  
  Range: 3200 through 32,000,000,000 bps  
  (EX4300 switches only) 8000 through 160,000,000,000 bps

Required Privilege:  
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

Related Documentation:  
- Example: Configuring CoS on EX Series Switches on page 1895
- Understanding Junos OS CoS Components for EX Series Switches on page 1863
transmit-rate (EX Series Switches)

Syntax: transmit-rate (rate | percent percentage | remainder);

Hierarchy Level: [edit class-of-service schedulers scheduler-name]

Release Information: Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description: Specify the transmit rate or percentage for a scheduler.

Default: If you do not include this statement, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 0, 0, 0, 0, and 5 percent.

Options:
- **rate** —Transmission rate, in bps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).
  - Range: 3200 through 160,000,000,000 bps
    - (EX4300 switches only) 8000 through 160,000,000,000 bps
- **percent percentage** —Percentage of transmission capacity. A percentage of zero drops all packets in the queue.
  - Range: 0 through 100 percent
- **remainder** —Remaining rate available

Required Privilege Level:
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

Related Documentation:
- Example: Configuring CoS on EX Series Switches on page 1895
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929 or Defining CoS Schedulers (J-Web Procedure) on page 1931
- Understanding CoS Schedulers on page 1880
unit

Syntax  
unit *logical-unit-number* {  
  forwarding-class *class-name*;  
  classifiers {  
    (dscp | ieee-802.1 | inet-precedence) (*classifier-name* | default);  
  }  
}

Hierarchy Level  
[edit class-of-service interfaces *interface-name*]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options  
*logical-unit-number*—Number of the logical unit.  
**Range:** 0 through 16,385

The remaining statements are explained separately.

Required Privilege
**Level**  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  
- Example: Configuring CoS on EX Series Switches on page 1895  
- Assigning CoS Components to Interfaces (CLI Procedure) on page 1942 or Assigning CoS Components to Interfaces (J-Web Procedure) on page 1942
CHAPTER 33

Administration

- Routine Monitoring on page 1975
- Operational Commands on page 1983

Routine Monitoring

- Monitoring CoS Classifiers on page 1975
- Monitoring CoS Forwarding Classes on page 1976
- Monitoring Interfaces That Have CoS Components on page 1978
- Monitoring CoS Rewrite Rules on page 1979
- Monitoring CoS Scheduler Maps on page 1980
- Monitoring CoS Drop Profiles on page 1982

Monitoring CoS Classifiers

**Purpose**
Use the monitoring functionality to display the mapping of incoming CoS values to forwarding class and loss priority for each classifier.

**Action**
To monitor CoS classifiers in the J-Web interface, select Monitor > Class of Service > Classifiers.

To monitor CoS classifiers in the CLI, enter the following CLI command:

```
show class-of-service classifier
```

**Meaning**
Table 244 on page 1975 summarizes key output fields for CoS classifiers.

### Table 244: Summary of Key CoS Classifier Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifier Name</td>
<td>Name of a classifier.</td>
<td>To display classifier assignments, click the plus sign (+).</td>
</tr>
</tbody>
</table>
### Table 244: Summary of Key CoS Classifier Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS Value Type</td>
<td>The classifiers are displayed by type:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• dscp—All classifiers of the DSCP type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ieee-802.1—All classifiers of the IEEE 802.1 type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• inet-precedence—All classifiers of the IP precedence type.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Internal index of the classifier.</td>
<td></td>
</tr>
<tr>
<td>Incoming CoS Value</td>
<td>CoS value of the incoming packets, in bits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>These values are used for classification.</td>
<td></td>
</tr>
<tr>
<td>Assign to Forwarding Class</td>
<td>Forwarding class that the classifier assigns to an incoming packet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This class affects the forwarding and scheduling policies that are applied to the packet as it transits the switch.</td>
<td></td>
</tr>
<tr>
<td>Assign to Loss Priority</td>
<td>Loss priority value that the classifier assigns to the incoming packet based on its CoS value.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- Defining CoS Classifiers (CLI Procedure) on page 1923
- Defining CoS Classifiers (J-Web Procedure) on page 1925
- Example: Configuring CoS on EX Series Switches on page 1895

**Monitoring CoS Forwarding Classes**

**Purpose**
View the current assignment of class-of-service (CoS) forwarding classes to queues on the switch.

**Action**
To monitor CoS forwarding classes in the J-Web interface, select Monitor > Class of Service > Forwarding Classes.

To monitor CoS forwarding classes in the CLI, enter the following CLI command:

```
show class-of-service forwarding-class
```

**Meaning**
Table 245 on page 1977 summarizes key output fields for CoS forwarding classes.
Names of forwarding classes assigned to queue numbers. The following are the default forwarding classes:

- **best-effort**—Provides no special CoS handling of packets. Loss priority is typically not carried in a CoS value.
- **expedited-forwarding**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service.
- **assured-forwarding**—Provides high assurance for packets within the specified service profile. Excess packets are dropped.
- **network-control**—Packets can be delayed but not dropped.

EX8200 switches have the following additional default forwarding classes:

- **mcast-be**—Provides no special CoS handling of packets.
- **mcast-ef**—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service.
- **mcast-af**—Provides high assurance for packets within the specified service profile. Excess packets are dropped.

EX4300 switches supports all the forwarding classes mentioned above and the one mentioned in this section:

- **mcast-nc**—Provides multicast network-control traffic.

Queue number corresponding to the forwarding class name. The default forwarding classes are assigned as follows:

- **best-effort**—0
- **expedited-forwarding**—5
- **assured-forwarding**—1
- **network-control**—7
- **mcast-be**—2
- **mcast-ef**—4
- **mcast-af**—6

EX4300 switches have the following queue numbers for the forwarding classes:

- **best-effort**—0
- **expedited-forwarding**—1
- **assured-forwarding**—2
- **network-control**—3
- **mcast-be**—8
- **mcast-ef**—9
- **mcast-af**—10
- **mcast-nc**—11

(EX8200 switches only) Fabric priority for the forwarding class, either high or low. The fabric priority determines the priority of packets entering the switch fabric.
Monitoring Interfaces That Have CoS Components

**Purpose**  Use the monitoring functionality to display details about the physical and logical interfaces and the CoS components assigned to them.

**Action**  To monitor interfaces that have CoS components in the J-Web interface, select Monitor > Class of Service > Interface Association.

To monitor interfaces that have CoS components in the CLI, enter the following command:

```
show class-of-service interface
```

**Meaning**  Table 246 on page 1978 summarizes key output fields for CoS interfaces.

### Table 246: Summary of Key CoS Interfaces Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of a physical interface to which CoS components are assigned.</td>
<td>To display names of logical interfaces configured on this physical interface, click the plus sign (+).</td>
</tr>
<tr>
<td>Scheduler Map</td>
<td>Name of the scheduler map associated with this interface.</td>
<td></td>
</tr>
<tr>
<td>Queues Supported</td>
<td>Number of queues you can configure on the interface.</td>
<td></td>
</tr>
<tr>
<td>Queues in Use</td>
<td>Number of queues currently configured.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface</td>
<td>Name of a logical interface on the physical interface to which CoS components are assigned.</td>
<td></td>
</tr>
<tr>
<td>Object</td>
<td>Category of an object—for example, classifier, scheduler-map, or rewrite.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name that you have given to an object—for example, ba-classifier.</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Type of an object—for example, dscp for a classifier.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Index of this interface or the internal index of a specific object.</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring CoS Rewrite Rules

**Purpose**
Use the monitoring functionality to display information about CoS value rewrite rules, which are based on the forwarding class and loss priority.

**Action**
To monitor CoS rewrite rules in the J-Web interface, select **Monitor > Class of Service > Rewrite Rules**.

To monitor CoS rewrite rules in the CLI, enter the following command:

```
show class-of-service rewrite-rules
```

**Meaning**
Table 247 on page 1979 summarizes key output fields for CoS rewrite rules.

### Table 247: Summary of Key CoS Rewrite Rules Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rewrite Rule Name</td>
<td>Names of rewrite rules.</td>
<td></td>
</tr>
<tr>
<td>CoS Value Type</td>
<td>Rewrite rule type:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- dscp—For IPv4 DiffServ traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- exp—For MPLS traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ieee-802.1—For Layer 2 traffic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- inet-precedence—For IPv4 traffic.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Internal index for this particular rewrite rule.</td>
<td></td>
</tr>
<tr>
<td>Forwarding Class</td>
<td>Forwarding class that is used to determine CoS values for rewriting in combination with loss priority.</td>
<td>Rewrite rules are applied to CoS values in outgoing packets based on forwarding class and loss priority setting.</td>
</tr>
<tr>
<td>Loss Priority</td>
<td>Loss priority that is used to determine CoS values for rewriting in combination with forwarding class.</td>
<td></td>
</tr>
<tr>
<td>Rewrite CoS Value To</td>
<td>Value that the CoS value is rewritten to.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- Defining CoS Rewrite Rules (CLI Procedure) on page 1939
- Defining CoS Rewrite Rules (J-Web Procedure) on page 1940
- Example: Configuring CoS on EX Series Switches on page 1895
Monitoring CoS Scheduler Maps

**Purpose**
Use the monitoring functionality to display assignments of CoS forwarding classes to schedulers.

**Action**
To monitor CoS scheduler maps in the J-Web interface, select **Monitor > Class of Service > Scheduler Maps**.

To monitor CoS scheduler maps in the CLI, enter the following CLI command:

`show class-of-service scheduler-map`

**Meaning**
Table 248 on page 1980 summarizes key output fields for CoS scheduler maps.

### Table 248: Summary of Key CoS Scheduler Maps Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler Map</td>
<td>Name of a scheduler map.</td>
<td>For details, click the plus sign (+).</td>
</tr>
<tr>
<td>Index</td>
<td>Index of a specific object—scheduler maps, schedulers, or drop profiles.</td>
<td></td>
</tr>
<tr>
<td>Scheduler Name</td>
<td>Name of a scheduler.</td>
<td></td>
</tr>
<tr>
<td>Forwarding Class</td>
<td>Forwarding classes this scheduler is assigned to.</td>
<td></td>
</tr>
<tr>
<td>Transmit Rate</td>
<td>Configured transmit rate of the scheduler in bits per second (bps). The rate value can be either of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A percentage—The scheduler receives the specified percentage of the total interface bandwidth.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• remainder—The scheduler receives the remaining bandwidth of the interface after bandwidth allocation to other schedulers.</td>
<td></td>
</tr>
<tr>
<td>Buffer Size</td>
<td>Delay buffer size in the queue or the amount of transmit delay (in milliseconds). The buffer size can be either of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• A percentage—The buffer is a percentage of the total buffer allocation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• remainder—The buffer is sized according to what remains after other scheduler buffer allocations.</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>Scheduling priority of a queue:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• strict-high—Packets in this queue are transmitted first.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• low—Packets in this queue are transmitted last.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 248: Summary of Key CoS Scheduler Maps Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Excess rate</td>
<td>The percentage of excess bandwidth traffic to share.</td>
<td></td>
</tr>
<tr>
<td>Drop Profiles</td>
<td>Name and index of a drop profile that is assigned to a specific loss priority and protocol pair.</td>
<td></td>
</tr>
<tr>
<td>Loss Priority</td>
<td>Packet loss priority corresponding to a drop profile.</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol corresponding to a drop profile.</td>
<td></td>
</tr>
<tr>
<td>Drop Profile Name</td>
<td>Name of the drop profile.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Index of a specific object—scheduler maps, schedulers, or drop profiles.</td>
<td></td>
</tr>
</tbody>
</table>

### Related Documentation
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929
- Defining CoS Schedulers (J-Web Procedure) on page 1931
- Example: Configuring CoS on EX Series Switches on page 1895

### Monitoring CoS Value Aliases

**Purpose**
Use the monitoring functionality to display information about the CoS value aliases that the system is currently using to represent DSCP, IEEE 802.1p, and IPv4 precedence bits.

**Action**
To monitor CoS value aliases in the J-Web interface, select Monitor > Class of Service > CoS Value Aliases.

To monitor CoS value aliases in the CLI, enter the following command:

```
show class-of-service code-point-aliases
```

**Meaning**
Table 249 on page 1982 summarizes key output fields for CoS value aliases.
### Table 249: Summary of Key CoS Value Alias Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS Value Type</td>
<td>Type of the CoS value:</td>
<td>To display aliases and bit patterns, click the plus sign (+).</td>
</tr>
<tr>
<td></td>
<td>• dscp—Examines Layer 3 packet headers for IP packet classification.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ieee-802.1—Examines Layer 2 packet headers for packet classification.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• inet-precedence—Examines Layer 3 packet headers for IP packet classification.</td>
<td></td>
</tr>
<tr>
<td>CoS Value Alias</td>
<td>Name given to a set of bits—for example, af11 is a name for 001010 bits.</td>
<td></td>
</tr>
<tr>
<td>CoS Value</td>
<td>Set of bits associated with an alias.</td>
<td></td>
</tr>
</tbody>
</table>

#### Related Documentation
- Defining CoS Code-Point Aliases (CLI Procedure) on page 1921
- Defining CoS Code-Point Aliases (J-Web Procedure) on page 1921
- Example: Configuring CoS on EX Series Switches on page 1895

### Monitoring CoS Drop Profiles

#### Purpose
Use the monitoring functionality to view data point information for each CoS random early detection (RED) drop profile on the EX8200 switch.

#### Action
- To monitor CoS RED drop profiles in the J-Web interface, select Monitor > Class of Service > RED Drop Profiles.
- To monitor CoS RED drop profiles in the CLI, enter the following CLI command: `show class-of-service drop-profile`

#### Meaning
Table 250 on page 1982 summarizes the key output fields for CoS RED drop profiles.

### Table 250: Summary of the Key Output Fields for CoS Red Drop Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED Drop Profile Name</td>
<td>Name of the RED drop profile. A drop profile consists of pairs of values between 0 and 100, one for queue buffer fill level and the other for drop probability, that determine the relationship between a buffer’s fullness and the likelihood it will drop packets.</td>
<td>To display profile values, click the plus sign (+).</td>
</tr>
<tr>
<td>Graph RED Profile</td>
<td>Links to a graph of a RED curve that the system uses to determine the drop probability based on queue buffer fullness.</td>
<td>The x axis represents the queue buffer fill level, and the y axis represents the drop probability.</td>
</tr>
</tbody>
</table>
### Table 250: Summary of the Key Output Fields for CoS Red Drop Profiles (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of a specific drop profile:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>interpolated</strong>—The two coordinates (x and y) of the graph are</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interpolated to produce a smooth profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>segmented</strong>—The two coordinates (x and y) of the graph are</td>
<td></td>
</tr>
<tr>
<td></td>
<td>represented by line fragments to produce a segmented</td>
<td></td>
</tr>
<tr>
<td></td>
<td>profile.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Internal index of this drop profile.</td>
<td></td>
</tr>
<tr>
<td>Fill Level</td>
<td>Percentage fullness of a buffer queue. This value is the x coordinate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of the RED drop profile graph.</td>
<td></td>
</tr>
<tr>
<td>Drop Probability</td>
<td>Drop probability of a packet corresponding to a specific queue buffer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>fill level. This value is the y coordinate of the RED drop profile graph.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- [Defining CoS Drop Profiles (J-Web Procedure) on page 1938](#)
- [Example: Configuring CoS on EX Series Switches on page 1895](#)

**Operational Commands**
show class-of-service

Syntax
show class-of-service

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.
EXP classifiers added in Junos OS Release 10.1 for EX Series switches.

Description
Display the class-of-service (CoS) information.

Required Privilege
view

Required Privilege Level
view

Related Documentation
• Example: Configuring CoS on EX Series Switches on page 1895
• Monitoring CoS Value Aliases on page 1981
• Monitoring CoS Classifiers on page 1975
• Monitoring CoS Forwarding Classes on page 1976
• Monitoring CoS Scheduler Maps on page 1980
• Monitoring CoS Rewrite Rules on page 1979

List of Sample Output
show class-of-service on page 1985
show class-of-service rewrite-rule on page 1988

Output Fields
Table 251 on page 1984 lists the output fields for the show class-of-service command.
Output fields are listed in the approximate order in which they appear.

Table 251: show class-of-service Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding class</td>
<td>The forwarding class configuration:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Forwarding class—Name of the forwarding class.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ID—Forwarding class ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Queue—Queue number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fabric Priority—(EX8200 switches only) Fabric priority: either high or low. The fabric priority determines which CoS ingress queues packets are sent to.</td>
<td></td>
</tr>
<tr>
<td>Code point type</td>
<td>The type of code-point alias:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• dscp—Aliases for DiffServ code point (DSCP) values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ieee–802.1—Aliases for IEEE 802.1p values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• inet-precedence—Aliases for IP precedence values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• exp—Aliases for experimental (EXP) values.</td>
<td></td>
</tr>
<tr>
<td>Alias</td>
<td>Names given to CoS values.</td>
<td>All levels</td>
</tr>
<tr>
<td>Bit pattern</td>
<td>Set of bits associated with an alias.</td>
<td>All levels</td>
</tr>
<tr>
<td>Classifier</td>
<td>Name of the classifier.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 251: show class-of-service Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code point</td>
<td>Code-point values.</td>
<td>All levels</td>
</tr>
<tr>
<td>Loss priority</td>
<td>Loss priority assigned to specific CoS values and aliases of the classifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rewrite rule</td>
<td>Name of the rewrite-rule.</td>
<td>All levels</td>
</tr>
<tr>
<td>Drop profile</td>
<td>Name of the drop profile.</td>
<td>All levels</td>
</tr>
<tr>
<td>Type</td>
<td>Type of drop profile. EX Series switches support only the discrete type of drop profile.</td>
<td>All levels</td>
</tr>
<tr>
<td>Fill level</td>
<td>Percentage of queue buffer fullness of high packets beyond which high packets are dropped.</td>
<td>All levels</td>
</tr>
<tr>
<td>Scheduler</td>
<td>Name of the scheduler.</td>
<td>All levels</td>
</tr>
<tr>
<td>Transmit rate</td>
<td>Transmission rate of the scheduler.</td>
<td>All levels</td>
</tr>
<tr>
<td>Excess rate</td>
<td>Percentage of excess bandwidth traffic to share.</td>
<td>All levels</td>
</tr>
<tr>
<td>Buffer size</td>
<td>Delay buffer size in the queue.</td>
<td>All levels</td>
</tr>
<tr>
<td>Drop profiles</td>
<td>Drop profiles configured for the specified scheduler.</td>
<td>All levels</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocol corresponding to the drop profile.</td>
<td>All levels</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the drop profile.</td>
<td>All levels</td>
</tr>
<tr>
<td>Queues supported</td>
<td>Number of queues that can be configured on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Queues in use</td>
<td>Number of queues currently configured.</td>
<td>All levels</td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Scheduler map</td>
<td>Name of the scheduler map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Internal index of a specific object.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output
show class-of-service

```
user@switch> show class-of-service
Forwarding class   ID  Queue
best-effort        0   0
expedited-forwarding 1   5
assured-forwarding 2   1
network-control    3   7
```
<table>
<thead>
<tr>
<th>Code point type: dscp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
</tr>
<tr>
<td>af11</td>
</tr>
<tr>
<td>af12</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code point type: ieee-802.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
</tr>
<tr>
<td>af11</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code point type: inet-precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
</tr>
<tr>
<td>af11</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>

**Classifier: dscp-default, Code point type: dscp, Index: 7**

<table>
<thead>
<tr>
<th>Code point</th>
<th>Forwarding class</th>
<th>Loss priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000001</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

**Classifier: ieee8021p-default, Code point type: ieee-802.1, Index: 11**

<table>
<thead>
<tr>
<th>Code point</th>
<th>Forwarding class</th>
<th>Loss priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>001</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>010</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>100</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>101</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>110</td>
<td>network-control</td>
<td>low</td>
</tr>
<tr>
<td>111</td>
<td>network-control</td>
<td>low</td>
</tr>
</tbody>
</table>

**Classifier: ipprec-default, Code point type: inet-precedence, Index: 12**

<table>
<thead>
<tr>
<th>Code point</th>
<th>Forwarding class</th>
<th>Loss priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>001</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>010</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>100</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>101</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>110</td>
<td>network-control</td>
<td>low</td>
</tr>
<tr>
<td>111</td>
<td>network-control</td>
<td>low</td>
</tr>
</tbody>
</table>

**Classifier: ieee8021p-untrust, Code point type: ieee-802.1, Index: 16**

<table>
<thead>
<tr>
<th>Code point</th>
<th>Forwarding class</th>
<th>Loss priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>001</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>010</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>100</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>101</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>110</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>111</td>
<td>best-effort</td>
<td>low</td>
</tr>
</tbody>
</table>

**Rewrite rule: dscp-default, Code point type: dscp, Index: 27**

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>Loss priority</th>
<th>Code point</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>low</td>
<td>000000</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>000000</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>101110</td>
</tr>
</tbody>
</table>
Rewrite rule: ieee8021p-default, Code point type: ieee-802.1, Index: 30
Forwarding class       Loss priority       Code point
best-effort            low                 000
best-effort            high                001
expedited-forwarding   low                 100
expedited-forwarding   high                101
assured-forwarding     low                 010
assured-forwarding     high                011
network-control        low                 110
network-control        high                111

Rewrite rule: ipprec-default, Code point type: inet-precedence, Index: 31
Forwarding class       Loss priority       Code point
best-effort            low                 000
best-effort            high                000
expedited-forwarding   low                 101
expedited-forwarding   high                101
assured-forwarding     low                 001
assured-forwarding     high                001
network-control        low                 110
network-control        high                111

Drop profile:<default-drop-profile>, Type: discrete, Index: 1
Fill level
100

Scheduler map: <default>, Index: 2

Scheduler: <default-be>, Forwarding class: best-effort, Index: 20
Transmit rate: 95 percent, Rate Limit: none, Buffer size: 95 percent,
Priority: low
Drop profiles:
  Loss priority   Protocol   Index   Name
High            non-TCP    1    <default-drop-profile>
High            TCP        1    <default-drop-profile>

Scheduler: <default-nc>, Forwarding class: network-control, Index: 22
Transmit rate: 5 percent, Rate Limit: none, Buffer size: 5 percent,
Priority: low
Drop profiles:
  Loss priority   Protocol   Index   Name
High            non-TCP    1    <default-drop-profile>
High            TCP        1    <default-drop-profile>

Physical interface: ge-0/0/0, Index: 129
Queues supported: 8, Queues in use: 4
Scheduler map: <default>, Index: 2

Physical interface: ge-0/0/1, Index: 130
Queues supported: 8, Queues in use: 4
Scheduler map: <default>, Index: 2

Fabric priority: low
Scheduler: <default-fabric>, Index: 23
Drop profiles:

<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
</tbody>
</table>

Fabric priority: high
Scheduler: <default-fabric>, Index: 23
Drop profiles:

<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
</tbody>
</table>

show class-of-service rewrite-rule

user@switch> show class-of-service rewrite-rule

Rewrite rule: dscp-default, Code point type: dscp, Index: 31

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>Loss priority</th>
<th>Code point</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>low</td>
<td>000000</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>000000</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>101110</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>high</td>
<td>101110</td>
</tr>
<tr>
<td>fw-class</td>
<td>low</td>
<td>001010</td>
</tr>
<tr>
<td>fw-class</td>
<td>high</td>
<td>001100</td>
</tr>
<tr>
<td>network-control</td>
<td>low</td>
<td>110000</td>
</tr>
<tr>
<td>network-control</td>
<td>high</td>
<td>111000</td>
</tr>
</tbody>
</table>

Rewrite rule: exp-default, Code point type: exp, Index: 33

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>Loss priority</th>
<th>Code point</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>low</td>
<td>00</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>001</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>010</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>high</td>
<td>011</td>
</tr>
<tr>
<td>fw-class</td>
<td>low</td>
<td>10</td>
</tr>
<tr>
<td>fw-class</td>
<td>high</td>
<td>101</td>
</tr>
<tr>
<td>network-control</td>
<td>low</td>
<td>110</td>
</tr>
<tr>
<td>network-control</td>
<td>high</td>
<td>111</td>
</tr>
</tbody>
</table>

Rewrite rule: ieee8021p-default, Code point type: ieee-802.1, Index: 34

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>Loss priority</th>
<th>Code point</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>low</td>
<td>00</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>001</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>010</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>high</td>
<td>011</td>
</tr>
<tr>
<td>fw-class</td>
<td>low</td>
<td>100</td>
</tr>
<tr>
<td>fw-class</td>
<td>high</td>
<td>101</td>
</tr>
<tr>
<td>network-control</td>
<td>low</td>
<td>110</td>
</tr>
<tr>
<td>network-control</td>
<td>high</td>
<td>111</td>
</tr>
</tbody>
</table>

Rewrite rule: ipprec-default, Code point type: inet-precedence, Index: 35

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>Loss priority</th>
<th>Code point</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>low</td>
<td>00</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>00</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>101</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>high</td>
<td>101</td>
</tr>
<tr>
<td>fw-class</td>
<td>low</td>
<td>001</td>
</tr>
<tr>
<td>fw-class</td>
<td>high</td>
<td>001</td>
</tr>
<tr>
<td>network-control</td>
<td>low</td>
<td>110</td>
</tr>
<tr>
<td>network-control</td>
<td>high</td>
<td>111</td>
</tr>
</tbody>
</table>
**show class-of-service classifier**

**Syntax**
```
show class-of-service classifier
<name name>
<type dscp | type dscp-ipv6 | type exp | type ieee-802.1 | type inet-precedence>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
For each class-of-service (CoS) classifier, display the mapping of code point value to forwarding class and loss priority.

**Options**
- `none`—Display all classifiers.
- `name name`—(Optional) Display named classifier.
- `type dscp`—(Optional) Display all classifiers of the Differentiated Services code point (DSCP) type.
- `type dscp-ipv6`—(Optional) Display all classifiers of the DSCP for IPv6 type.
- `type exp`—(Optional) Display all classifiers of the MPLS experimental (EXP) type.
- `type ieee-802.1`—(Optional) Display all classifiers of the ieee-802.1 type.
- `type inet-precedence`—(Optional) Display all classifiers of the inet-precedence type.

**Required Privilege**
- View

**List of Sample Output**
- `show class-of-service classifier type ieee-802.1` on page 1990
- `show class-of-service classifier type ieee-802.1 (QFX Series)` on page 1990

**Output Fields**
Table 252 on page 1989 describes the output fields for the `show class-of-service classifier` command. Output fields are listed in the approximate order in which they appear.

**Table 252: show class-of-service classifier Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifier</td>
<td>Name of the classifier.</td>
</tr>
<tr>
<td>Code point type</td>
<td>Type of the classifier: exp (not on EX Series switch), dscp, dscp-ipv6 (not on EX Series switch), ieee-802.1, or inet-precedence.</td>
</tr>
<tr>
<td>Index</td>
<td>Internal index of the classifier.</td>
</tr>
<tr>
<td>Code point</td>
<td>Code point value used for classification</td>
</tr>
<tr>
<td>Forwarding class</td>
<td>Classification of a packet affecting the forwarding, scheduling, and marking policies applied as the packet transits the router.</td>
</tr>
</tbody>
</table>
Table 252: show class-of-service classifier Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss priority</td>
<td>Loss priority value used for classification. For most platforms, the value is high or low. For some platforms, the value is high, medium-high, medium-low, or low.</td>
</tr>
</tbody>
</table>

Sample Output

show class-of-service classifier type ieee-802.1

```
user@host> show class-of-service classifier type ieee-802.1
Classifier: ieee802.1-default, Code point type: ieee-802.1, Index: 3
  Code Point Forwarding Class Loss priority
  000        best-effort      low
  001        best-effort      high
  010        expedited-forwarding low
  011        expedited-forwarding high
  100        assured-forwarding low
  101        assured-forwarding medium-high
  110        network-control  low
  111        network-control  high

Classifier: users-ieee802.1, Code point type: ieee-802.1
  Code point Forwarding class Loss priority
  100        expedited-forwarding low
```

show class-of-service classifier type ieee-802.1 (QFX Series)

```
user@switch> show class-of-service classifier type ieee-802.1
Classifier: ieee8021p-default, Code point type: ieee-802.1, Index: 11
  Code point Forwarding class Loss priority
  000        best-effort      low
  001        best-effort      low
  010        best-effort      low
  011        fcoe            low
  100        no-loss         low
  101        best-effort      low
  110        network-control  low
  111        network-control  low

Classifier: ieee-mcast, Code point type: ieee-802.1, Index: 46
  Code point Forwarding class Loss priority
  000        mcast            low
  001        mcast            low
  010        mcast            low
  011        mcast            low
  100        mcast            low
  101        mcast            low
  110        mcast            low
  111        mcast            low
```
show class-of-service code-point-aliases

**Syntax**

```
show class-of-service code-point-aliases
<dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display the mapping of class-of-service (CoS) code point aliases to corresponding bit patterns.

**Options**

- `none`—Display code point aliases of all code point types.
- `dscp`—(Optional) Display Differentiated Services code point (DSCP) aliases.
- `dscp-ipv6`—(Optional) Display IPv6 DSCP aliases.
- `exp`—(Optional) Display MPLS EXP code point aliases.
- `ieee-802.1`—(Optional) Display IEEE-802.1 code point aliases.
- `inet-precedence`—(Optional) Display IPv4 precedence code point aliases.

**Required Privilege**

- `view`

**List of Sample Output**

`show class-of-service code-point-aliases exp on page 1992`

**Output Fields**

Table 253 on page 1991 describes the output fields for the `show class-of-service code-point-aliases` command. Output fields are listed in the approximate order in which they appear.

**Table 253: show class-of-service code-point-aliases Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code point type</td>
<td>Type of the code points displayed: <code>dscp</code>, <code>dscp-ipv6</code> (not on EX Series switch), <code>exp</code> (not on EX Series switch or the QFX Series), <code>ieee-802.1</code>, or <code>inet-precedence</code> (not on the QFX Series).</td>
</tr>
<tr>
<td>Alias</td>
<td>Alias for a bit pattern.</td>
</tr>
<tr>
<td>Bit pattern</td>
<td>Bit pattern for which the alias is displayed.</td>
</tr>
</tbody>
</table>
Sample Output

show class-of-service code-point-aliases exp

```
user@host> show class-of-service code-point-aliases exp
Code point type: exp
       Alias  Bit pattern
       af11    100
       af12    101
        be     000
        be1    001
        cs6    110
        cs7    111
         ef    010
         ef1   011
        nc1    110
        nc2    111
```
show class-of-service drop-profile

**Syntax**
```
show class-of-service drop-profile
<profile-name profile-name>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Display data points for each class-of-service (CoS) random early detection (RED) drop profile.

**Options**
- `none`—Display all drop profiles.
- `profile-name profile-name`—(Optional) Display the specified profile only.

**Required Privilege Level**
`view`

**List of Sample Output**
- `show class-of-service drop-profile on page 1994`
- `show class-of-service drop-profile (EX4200 Switch) on page 1994`
- `show class-of-service drop-profile (EX8200 Switch) on page 1994`

**Output Fields**
Table 254 on page 1993 describes the output fields for the `show class-of-service drop-profile` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop profile</td>
<td>Name of a drop profile.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of drop profile:</td>
</tr>
<tr>
<td></td>
<td>• discrete (default)</td>
</tr>
<tr>
<td></td>
<td>• interpolated (EX8200 switches only)</td>
</tr>
<tr>
<td>Index</td>
<td>Internal index of this drop profile.</td>
</tr>
<tr>
<td>Fill Level</td>
<td>Percentage fullness of a queue.</td>
</tr>
<tr>
<td>Drop probability</td>
<td>Drop probability at this fill level.</td>
</tr>
</tbody>
</table>
Sample Output

**show class-of-service drop-profile**

```
user@host> show class-of-service drop-profile
Drop profile: <default-drop-profile>, Type: discrete, Index: 1
  Fill level  Drop probability
       100            100

Drop profile: user-drop-profile, Type: interpolated, Index: 2989
  Fill level  Drop probability
            0            0
            1            2
            2            4
            4            5
            6            6
            8            8
           10           10
           12           15
           14           20
           15           23
... 64 entries total
            90           96
            92           96
            94           97
            95           98
            96           98
            98           99
            99           99
           100         100
```

**show class-of-service drop-profile (EX4200 Switch)**

```
user@switch> show class-of-service drop-profile
Drop profile: <default-drop-profile>, Type: discrete, Index: 1
  Fill level
       100

Drop profile: dp1, Type: discrete, Index: 40496
  Fill level
       10
```

**show class-of-service drop-profile (EX8200 Switch)**

```
user@switch> show class-of-service drop-profile
Drop profile: <default-drop-profile>, Type: discrete, Index: 1
  Fill level  Drop probability
       100            100

Drop profile: dp1, Type: interpolated, Index: 40496
  Fill level  Drop probability
            0            0
            1            80
            2            90
            4            90
            5            90
            6            90
            8            90
           10           90
           12           91
           14           91
           15           91
           16           91
```
Drop profile: dp2, Type: discrete, Index: 40499

<table>
<thead>
<tr>
<th>Fill level</th>
<th>Drop probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>50</td>
<td>50</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
**show class-of-service forwarding-class**

**Syntax**
```
show class-of-service forwarding-class
```

**Release Information**

**Description**
Display information about forwarding classes, including the mapping of forwarding classes to queue numbers.

**Required Privilege**
view

**Related Documentation**
- Example: Configuring CoS on EX Series Switches on page 1895
- Monitoring CoS Forwarding Classes on page 1976
- Defining CoS Forwarding Classes (CLI Procedure) on page 1927
- Configuring CoS Traffic Classification for Ingress Queuing on Oversubscribed Ports on EX8200 Line Cards (CLI Procedure) on page 1945

**List of Sample Output**
- show class-of-service forwarding-class on page 1997
- show class-of-service forwarding-class (EX8200 Switch) on page 1997
- show class-of-service forwarding-class (QFX Series) on page 1997

**Output Fields**
Table 255 on page 1996 describes the output fields for the `show class-of-service forwarding-class` command. Output fields are listed in the approximate order in which they appear.

**Table 255: show class-of-service forwarding-class Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding class</td>
<td>Name of the forwarding class.</td>
</tr>
<tr>
<td>ID</td>
<td>Forwarding class identifier.</td>
</tr>
<tr>
<td>Queue</td>
<td>CoS queue mapped to the forwarding class.</td>
</tr>
<tr>
<td>Policing priority</td>
<td>Not supported on EX Series switches or the QFX Series and can be ignored.</td>
</tr>
<tr>
<td>Fabric priority</td>
<td>(EX8200 switches only) Fabric priority for the forwarding class, either high or low. Determines the priority of packets entering the switch fabric.</td>
</tr>
</tbody>
</table>
Table 255: show class-of-service forwarding-class Output
Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No-Loss</strong></td>
<td>(QFX Series only) Packet loss attribute to differentiate lossless forwarding classes from lossy forwarding classes:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—Lossless transport is not configured on the forwarding class (packet drop attribute is drop).</td>
</tr>
<tr>
<td></td>
<td>• Enabled—Lossless transport is configured on the forwarding class (packet drop attribute is no-loss).</td>
</tr>
</tbody>
</table>

---

**Sample Output**

*show class-of-service forwarding-class*

```
user@switch> show class-of-service forwarding-class
Forwarding class               ID                      Queue  Policing priority
best-effort                        0                       0           normal
expedited-forwarding               1                       5           normal
assured-forwarding                 2                       1           normal
network-control                    3                       7           normal
```

**Sample Output**

*show class-of-service forwarding-class (EX8200 Switch)*

```
user@switch> show class-of-service forwarding-class
Forwarding class               ID      Queue  Fabric priority
best-effort                           0       0      low
expedited-forwarding                  1       5      low
assured-forwarding                    2       1      low
network-control                       3       7      low
mcast-be                              4       2      low
mcast-ef                              5       4      low
mcast-af                              6       6      low
```

**Sample Output**

*show class-of-service forwarding-class (QFX Series)*

```
user@switch> show class-of-service forwarding-class
Forwarding class               ID      Queue  Policing priority  No-Loss
best-effort                          0         0         normal        Disabled
fcoe                                 1         3         normal        Enabled
no-loss                              2         4         normal        Enabled
network-control                      3         7         normal        Disabled
mcast                                8         8         normal        Disabled
```
show pfe statistics traffic cpu

Syntax

show pfe statistics traffic cpu <fpc  fpc-slot>

Release Information

Command introduced in Junos OS Release 9.5 for EX Series switches.

Description

(On EX8200 switches only) Display count of multidestination packets ingressing from the physical interface to the CPU.

NOTE: Multidestination packets include unknown unicast, broadcast, and multicast packets.

Options

none—Displays the count of packets ingressing from all the physical interfaces (line cards) to the CPU.

fpc  fpc-slot—(Optional) Displays the count of packets ingressing from the physical interface, referred to by the slot number, to the CPU.

On an EX8200 switch, the FPC slot number is the slot number for the line card. Possible values are 0 through 7 on the EX8208 switch and 0 through 15 on the EX8216 switch.

Required Privilege Level

view

Related Documentation

• show pfe statistics traffic multicast on page 2004
• show pfe statistics traffic egress-queues on page 2002
• show interfaces queue on page 2518
• Monitoring Interface Status and Traffic on page 2463
• Understanding Junos OS CoS Components for EX Series Switches on page 1863

List of Sample Output

show pfe statistics traffic cpu (EX8208 Switch) on page 1999

Output Fields

Table 256 on page 1998 lists the output fields for the show pfe statistics traffic cpu command. Output fields are listed in the approximate order in which they appear.

Table 256: show pfe statistics traffic cpu Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue</td>
<td>CoS queue number.</td>
</tr>
<tr>
<td>Forwarding classes</td>
<td>Forwarding class name.</td>
</tr>
<tr>
<td>Queued Packets</td>
<td>Number of packets queued to this queue.</td>
</tr>
</tbody>
</table>
### Table 256: show pfe statistics traffic cpu Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queued Bytes</td>
<td>Number of bytes queued to this queue.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets transmitted by this queue.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Number of bytes transmitted by this queue.</td>
</tr>
<tr>
<td>Tail-dropped packets</td>
<td>Count of packets dropped at the tail end of the queue because of lack of buffer space.</td>
</tr>
<tr>
<td>RED-dropped packets</td>
<td>Number of packets dropped because of Random Early Discard (RED):</td>
</tr>
<tr>
<td></td>
<td>• Low—Number of low-loss priority packets dropped because of RED.</td>
</tr>
<tr>
<td></td>
<td>• High—Number of high-loss priority packets dropped because of RED.</td>
</tr>
<tr>
<td>RED-dropped bytes</td>
<td>Number of bytes dropped because of Random Early Discard (RED):</td>
</tr>
<tr>
<td></td>
<td>• Low—Number of low-loss priority bytes dropped because of RED.</td>
</tr>
<tr>
<td></td>
<td>• High—Number of high-loss priority bytes dropped because of RED.</td>
</tr>
</tbody>
</table>

### Sample Output

**show pfe statistics traffic cpu (EX8208 Switch)**

```
user@switch> show pfe statistics traffic cpu

Queue: 0, Forwarding classes: best-effort
   Queued:
   Packets   : Not Available
   Bytes     : Not Available
   Packets   : 0  0 pps
   Bytes     : 0  0 bps
   Tail-dropped packets : 0
   RED-dropped bytes   : 0  0 bps
   Low                   : 0  0 bps
   High                  : 0  0 bps
   RED-dropped packets  : 0  0 pps
   Low                   : 0  0 pps
   High                  : 0  0 pps

Queue: 1, Forwarding classes: expedited-forwarding
   Queued:
   Packets   : Not Available
   Bytes     : Not Available
   Packets   : 0  0 pps
   Bytes     : 0  0 bps
   Tail-dropped packets : 0
   RED-dropped bytes   : 0  0 bps
   Low                   : 0  0 bps
   High                  : 0  0 bps
   RED-dropped packets  : 0  0 pps
   Low                   : 0  0 pps
   High                  : 0  0 pps

Queue: 2, Forwarding classes: assured-forwarding
   Queued:
   Packets   : Not Available
```
Bytes : Not Available
Packets : 0 0 pps
Bytes : 0 0 bps
Tail-dropped packets : 0
RED-dropped bytes : 0 0 bps
Low : 0 0 bps
High : 0 0 bps
RED-dropped packets : 0 0 pps
Low : 0 0 pps
High : 0 0 pps

Queue: 3, Forwarding classes: network-control
Queued:
  Packets : Not Available
  Bytes : Not Available
  Packets : 0 0 pps
  Bytes : 0 0 bps
  Tail-dropped packets : 0
  RED-dropped bytes : 0 0 bps
  Low : 0 0 bps
  High : 0 0 bps
  RED-dropped packets : 0 0 pps
  Low : 0 0 pps
  High : 0 0 pps

Queue: 4
  Packets : Not Available
  Bytes : Not Available
  Packets : 0 0 pps
  Bytes : 0 0 bps
  Tail-dropped packets : 0
  RED-dropped bytes : 0 0 bps
  Low : 0 0 bps
  High : 0 0 bps
  RED-dropped packets : 0 0 pps
  Low : 0 0 pps
  High : 0 0 pps

Queue: 5
  Packets : Not Available
  Bytes : Not Available
  Packets : 0 0 pps
  Bytes : 0 0 bps
  Tail-dropped packets : 0
  RED-dropped bytes : 0 0 bps
  Low : 0 0 bps
  High : 0 0 bps
  RED-dropped packets : 0 0 pps
  Low : 0 0 pps
  High : 0 0 pps

Queue: 6
  Packets : Not Available
  Bytes : Not Available
  Packets : 0 0 pps
  Bytes : 0 0 bps
  Tail-dropped packets : 0
  RED-dropped bytes : 0 0 bps
  Low : 0 0 bps
  High : 0 0 bps
  RED-dropped packets : 0 0 pps
  Low : 0 0 pps
  High : 0 0 pps

Queue: 7
  Packets : Not Available
<table>
<thead>
<tr>
<th>Metric</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>Not Available</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tail-dropped packets</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RED-dropped bytes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RED-dropped packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show pfe statistics traffic egress-queues

**Syntax**
```
show pfe statistics traffic egress-queues <fpc fpc-slot>
```

**Release Information**
Command introduced in Junos OS Release 9.5 for EX Series switches.

**Description**
(On EX8200 switches only) Display count of multidestination packets dropped on egress ports when the egress queues are oversubscribed due to multidestination traffic.

**Options**
- **none**—Displays count of packets dropped on egress ports of all physical interfaces (line cards) when egress queues are oversubscribed due to multidestination traffic.
- **fpc fpc-slot**—(Optional) Displays count of packets dropped on egress ports of the physical interface (line card) referred to by the slot number.

**NOTE:** Multidestination packets include unknown unicast, broadcast, and multicast packets.

**Required Privilege Level**
view

**Related Documentation**
- show pfe statistics traffic cpu on page 1998
- show pfe statistics traffic multicast on page 2004
- show interfaces queue on page 2518
- Monitoring Interface Status and Traffic on page 2463
- Understanding Junos OS CoS Components for EX Series Switches on page 1863

**List of Sample Output**
- show pfe statistics traffic egress-queues fpc 4 (EX8208 Switch) on page 2003

**Output Fields**
Table 257 on page 2002 lists the output fields for the `show pfe statistics traffic egress-queues` command. Output fields are listed in the approximate order in which they appear.

**Table 257: show pfe statistics traffic egress-queues Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tail-dropped packets</td>
<td>Number of arriving packets dropped because the output queue buffers are full.</td>
</tr>
</tbody>
</table>
Sample Output

show pfe statistics traffic egress-queues fpc 4 (EX8208 Switch)

    user@switch> show pfe statistics traffic egress-queues fpc 4
    Tail-dropped packets : 0
**show pfe statistics traffic multicast**

**Syntax**

```
show pfe statistics traffic multicast <fpc fpc-slot dev-number>
```

**Release Information**

Command introduced in Junos OS Release 9.5 for EX Series switches.

**Description**

(On EX8200 switches only) Display class-of-service (CoS) queue information for multidestination traffic on a physical interface (line card).

**Options**

- `fpc fpc-slot dev-number` — (Optional) Displays class-of-service (CoS) queue information for multidestination traffic on the physical interface (line card) referred to by the slot number and device number.

**Required Privilege Level**

view

**Related Documentation**

- show pfe statistics traffic cpu on page 1998
- show pfe statistics traffic egress-queues on page 2002
- show interfaces queue on page 2518
- Monitoring Interface Status and Traffic on page 2463
- Understanding Junos OS CoS Components for EX Series Switches on page 1863

**List of Sample Output**

show pfe statistics traffic multicast fpc 0 2 (EX8208 Switch) on page 2005

**Output Fields**

Table 258 on page 2005 lists the output fields for the `show pfe statistics traffic multicast` command. Output fields are listed in the approximate order in which they appear.

**NOTE:** Multidestination packets include unknown unicast, broadcast, and multicast packets.

**NOTE:** To view statistical information for unicast traffic, use the `show interfaces queue` command.

**NOTE:** On an EX8200 switch, the FPC slot number is the slot number for the line card. Possible values for the FPC slot number are 0 through 7 on the EX8208 switch and 0 through 15 on the EX8216 switch. The value for the device number ranges from 0–5, where 0–4 values correspond to the statistics only from that specific device and the value 5 corresponds to the combined statistics from all the devices in the FPC.
### Table 258: show pfe statistics traffic multicast Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue</td>
<td>CoS queue number.</td>
</tr>
<tr>
<td>Forwarding classes</td>
<td>Forwarding class name.</td>
</tr>
<tr>
<td>Queued Packets</td>
<td>Number of packets queued to this queue.</td>
</tr>
<tr>
<td>Queued Bytes</td>
<td>Number of bytes queued to this queue.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets transmitted by this queue.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Number of bytes transmitted by this queue.</td>
</tr>
<tr>
<td>Tail-dropped packets</td>
<td>Count of packets dropped at the tail end of the queue because of lack of buffer space.</td>
</tr>
<tr>
<td>RED-dropped packets</td>
<td>Number of packets dropped because of Random Early Discard (RED):</td>
</tr>
<tr>
<td></td>
<td>- Low—Number of low-loss priority packets dropped because of RED.</td>
</tr>
<tr>
<td></td>
<td>- High—Number of high-loss priority packets dropped because of RED.</td>
</tr>
<tr>
<td>RED-dropped bytes</td>
<td>Number of bytes dropped because of Random Early Discard (RED):</td>
</tr>
<tr>
<td></td>
<td>- Low—Number of low-loss priority bytes dropped because of RED.</td>
</tr>
<tr>
<td></td>
<td>- High—Number of high-loss priority bytes dropped because of RED.</td>
</tr>
</tbody>
</table>

### Sample Output

**show pfe statistics traffic multicast fpc 0 2(EX8208 Switch)**

```
user@switch> show pfe statistics traffic multicast fpc 0 2

Queue: 0, Forwarding classes: best-effort
Queued:
  Packets : Not Available
  Bytes  : Not Available
  Packets : 0
  Bytes  : 0
  Tail-dropped packets : 0
  RED-dropped bytes : 0
  Low : 0
  High : 0
  RED-dropped packets : 0
  Low : 0
  High : 0

Queue: 1, Forwarding classes: expedited-forwarding
Queued:
  Packets : Not Available
  Bytes  : Not Available
  Packets : 0
  Bytes  : 0
  Tail-dropped packets : 0
  RED-dropped bytes : 0
  Low : 0
  High : 0
```

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Queue</th>
<th>Forwarding classes:</th>
<th>Packets</th>
<th>Bytes</th>
<th>Tail-dropped packets</th>
<th>RED-dropped bytes</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>assured-forwarding</td>
<td>Not Available</td>
<td>Not Available</td>
<td>0</td>
<td>0 bps</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
<td>Not Available</td>
<td>Not Available</td>
<td>0</td>
<td>0 bps</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Not Available</td>
<td>Not Available</td>
<td>0</td>
<td>0 bps</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Not Available</td>
<td>Not Available</td>
<td>0</td>
<td>0 bps</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Not Available</td>
<td>Not Available</td>
<td>0</td>
<td>0 bps</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
<td>-----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0 bps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0 bps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RED-dropped packets</td>
<td>0</td>
<td>0 pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0 pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0 pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queue</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RED-dropped bytes</td>
<td>0</td>
<td>0 bps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0 bps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0 bps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RED-dropped packets</td>
<td>0</td>
<td>0 pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0 pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0 pps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Packets** : Not Available

**Bytes** : Not Available

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>Bytes</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>Tail-dropped packets</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RED-dropped bytes</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>RED-dropped packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
<td>0 pps</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0 pps</td>
</tr>
</tbody>
</table>
Troubleshooting Procedures

• Troubleshooting CoS Schedulers on a 40-port SFP+ Line Card in an EX8200 Switch on page 2009
• Troubleshooting a CoS Classifier Configuration for a TCAM Space Error on page 2010

Troubleshooting CoS Schedulers on a 40-port SFP+ Line Card in an EX8200 Switch

Problem
After you configure a scheduler map on an interface on the 40-port SFP+ line card, you notice one or both of the following:

• All packets are being dropped on a class-of-service queue configured on the interface.

• A message in the system log states that the interface is using the default scheduler map, not the scheduler map you configured. For example:

  Sep 19 21:26:50  hostname cosd[907]: COSD_SCHED_MAP_GROUP_CONFLICT: Interface xe-5/0/15 cannot be bound to scheduler-map m1. It will be bound to default scheduler-map

Cause
The ports in a 40-port SFP+ line card are divided into eight groups, each group comprising five ports. The ports in a port group share 10 gigabits of bandwidth. Because the port groups share bandwidth, only one scheduler map can be active at a time in a port group. If you configure different scheduler maps for different interfaces in a port group, you do not receive an error when you commit the configuration. Instead, default scheduler map becomes the active scheduler map for all interfaces in the port group, and messages in the system log report that the default scheduler map is in use for the affected interfaces. If the default scheduler map does not define a queue, all traffic is dropped on that queue.

Solution
Check your CoS configuration for the interfaces in the port group. If you have different scheduler maps assigned to different interfaces in the port group:

1. Delete the scheduler map configuration for all interfaces in the port group.
2. Determine the scheduler map that you want all interfaces in the port group to use.
3. Assign that scheduler map to at least one interface in the port group. The remaining interfaces in the port group will adopt this scheduler map.
BEST PRACTICE: To prevent confusion and future configuration conflicts, explicitly assign the scheduler map to each interface in the port group.

4. After you commit the configuration, verify that the scheduler map is the active scheduler map for the interfaces in the port group by using the `show class-of-service forwarding-table scheduler-map` command.

**Troubleshooting a CoS Classifier Configuration for a TCAM Space Error**

**Problem**
When a CoS classifier configuration exceeds the amount of available ternary content addressable memory (TCAM) space, the switch returns the following system log message:

```
<number_of_rules_being_added> rules for <filter_name> class <filter_class> will not be installed, key: <bind_point>. no space in tcam db(<shared_pool_information>)
```

The switch returns this message during the commit operation if the number of classifiers defined in the CoS configuration or the number of bind points (interfaces) to which classifiers are bound causes the CoS configuration to exceed the amount of available TCAM space. However, the commit operation for the CoS configuration is completed in the CLI module.

**Solution**
When a CoS configuration exceeds the amount of available TCAM table space, you must either define fewer classifiers or bind them to fewer interfaces, or both, so that the space requirements for the CoS configuration do not exceed the available space in TCAM.
To delete classifier definitions and bind points in a CoS configuration, and to apply a new CoS classifier definition to fewer bind points:

1. Delete either the CoS classifier definition or the bind points:
   - To delete the CoS classifier definition:
     - For behavioral classifiers:
       ```
       [edit class-of-service]
       user@switch# delete classifier dscp dl
       ```
     - For multifield classifiers:
       ```
       [edit]
       user@switch# delete interfaces ge-3/0/2 unit 0 family ethernet-switching filter input ipacl
       ```
     This command deletes a multifield classifier defined for a port. Similarly, you can delete a multifield classifier defined for a VLAN or router.
     You can also delete terms defined in a single multifield classifier:
     ```
     [edit]
     user@switch# delete firewall family inet filter f1 term t1
     ```
     In both these examples (for behavioral and multifield classifiers), the assumption is that too many classifier definitions resulted in the error message.
   - To delete the bind points:
     ```
     [edit class-of-service]
     user@switch# delete class-of-service interfaces ge-0/0/0
     user@switch# delete class-of-service interfaces ge-0/0/1
     user@switch# delete class-of-service interfaces ge-0/0/2
     user@switch# delete class-of-service interfaces ge-0/0/3
     user@switch# delete class-of-service interfaces ge-0/0/4
     user@switch# delete class-of-service interfaces ge-0/0/5
     user@switch# delete class-of-service interfaces ge-0/0/6
     user@switch# delete class-of-service interfaces ge-0/0/7
     user@switch# delete class-of-service interfaces ge-0/0/8
     ```
     Here the assumption is that too many bind points (nine) in the configuration resulted in the error message.

2. Commit the operation:
   ```
   [edit]
   user@switch# commit
   ```

3. Define fewer classifiers in the CoS configuration or bind classifiers to fewer interfaces, or both, so that the CoS classifier configuration does not exceed the amount of available TCAM space on the switch:
   - To define CoS classifiers:
     - For behavioral classifiers:
       ```
       [edit]
       user@switch# set class-of-service classifiers dscp d2 forwarding-class fc1 loss-priority low code-points 000001
       user@switch# set class-of-service classifiers dscp d2 forwarding-class fc2 loss-priority low code-points 000010
       user@switch# set class-of-service classifiers dscp d2 forwarding-class fc3 loss-priority low code-points 000011
       ```
user@switch# set class-of-service classifiers dscp d2 forwarding-class fc4 loss-priority low code-points 000100
user@switch# set class-of-service classifiers dscp d2 forwarding-class fc5 loss-priority low code-points 000101
user@switch# set class-of-service classifiers dscp d2 forwarding-class fc6 loss-priority low code-points 000110
user@switch# set class-of-service classifiers dscp d2 forwarding-class fc7 loss-priority low code-points 000111

- For multifield Classifiers:

  [edit]
  user@switch# set firewall family inet filter f1 term t1 from protocol tcp
  user@switch# set firewall family inet filter f1 term t1 then loss-priority high
  user@switch# set firewall family inet filter f1 term t1 then forwarding-class best-effort
  user@switch# set firewall family inet filter f1 term t2 from protocol udp
  user@switch# set firewall family inet filter f1 term t2 then loss-priority high
  user@switch# set firewall family inet filter f1 term t2 then forwarding-class assured-forwarding
  user@switch# set firewall family inet filter f1 term t3 from source-port ssh
  user@switch# set firewall family inet filter f1 term t3 then loss-priority low
  user@switch# set firewall family inet filter f1 term t3 then forwarding-class fc8
  user@switch# set class-of-service forwarding-classes best-effort, assured-forwarding, fc8

- To bind classifiers to fewer interfaces:

  [edit]
  user@switch# set class-of-service interfaces ge-0/0/0 unit 0 classifers dscp d2
  user@switch# set class-of-service interfaces ge-0/0/1 unit 0 classifers dscp d2
  user@switch# set class-of-service interfaces ge-0/0/2 unit 0 forwarding-class best-effort
  user@switch# set class-of-service interfaces ge-0/0/3 unit 0 forwarding-class assured-forwarding
  user@switch# set class-of-service interfaces ge-0/0/4 unit 0 forwarding-class fc8

4. Commit the operation:

  [edit]
  user@switch# commit

5. Check system log for an error message. If an error message is not logged, then your classifier configuration has not exceeded the TCAM space limit.

   If an error message is logged, then repeat this procedure by defining fewer classifiers or binding classifiers to fewer bind points.

Related Documentation

- Understanding CoS Classifiers
- Defining CoS Classifiers (CLI Procedure) on page 1923
PART 12

Device Security

- Overview on page 2015
- Configuration on page 2019
- Administration on page 2043
CHAPTER 35

Overview

- Storm Control Overview on page 2015
- Unknown Unicast Forwarding Overview on page 2017

Storm Control Overview

- Understanding Storm Control on EX Series Switches on page 2015

Understanding Storm Control on EX Series Switches

NOTE: This topic uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Understanding Storm Control on EX Series Switches. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

A traffic storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. Storm control enables the switch to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level—called the storm control level or storm control bandwidth—is exceeded, thus preventing packets from proliferating and degrading the LAN. As an alternative to having the switch drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces (see the action-shutdown statement and the recovery-timeout statement) when the storm control level is exceeded.

NOTE: On Juniper Networks EX4300 Ethernet Switches, the factory default configuration enables storm control on all Layer 2 interfaces, with the storm control level set to 80 percent of the combined broadcast, multicast, and unknown unicast traffic streams.

Storm control is not enabled by default on Juniper Networks EX9200 Ethernet Switches.
You can customize the storm control level for a specific interface by explicitly configuring either bandwidth level or bandwidth percentage.

- **Bandwidth level**—Configures the storm control level as the bandwidth in kilobits per second of the applicable traffic streams on that interface.

- **Bandwidth percentage**—Configures the storm control level as a percentage of the available bandwidth used by the combined applicable traffic streams that are subject to storm control on that interface.

**NOTE:** You cannot configure both bandwidth level and bandwidth percentage for the same interface.

You can disable storm control selectively for broadcast, multicast, or unknown unicast traffic, or any combination of traffic types. When disabling storm control for multicast traffic, you can specify the traffic to be either registered multicast or unregistered multicast.

The sending and receiving of broadcast, multicast, and unicast packets are part of normal LAN operation. Therefore, to recognize a storm, you must be able to identify when traffic has reached a level that is abnormal for your LAN. Suspect a storm when operations begin timing out and network response times slow down. As more packets flood the LAN, network users might be unable to access servers or e-mail.

Monitor the level of broadcast, multicast, and unknown unicast traffic in the LAN when it is operating normally. Use this data as a benchmark to determine when traffic levels are too high. Then configure storm control to set the level at which you want the switch to drop broadcast traffic, multicast traffic, unknown unicast traffic, or two or all three of those traffic types.

**NOTE:** When you configure storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth or level. For example, if you configure a storm control level of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined traffic streams. Traffic might include broadcast, multicast, and unknown unicast traffic, depending upon the configuration.

**Related Documentation**

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 2023
- Configuring or Disabling Storm Control (CLI Procedure) on page 2023
Unknown Unicast Forwarding Overview

- Understanding Unknown Unicast Forwarding on EX Series Switches on page 2017

Understanding Unknown Unicast Forwarding on EX Series Switches

Unknown unicast traffic consists of unicast packets with unknown destination MAC addresses. By default, the switch floods these unicast packets that are traveling in a VLAN to all interfaces that are members of the VLAN. Forwarding this type of traffic to interfaces on the switch can trigger a security issue. The LAN is suddenly flooded with packets, creating unnecessary traffic that leads to poor network performance or even a complete loss of network service. This is known as a traffic storm.

To prevent a storm, you can disable the flooding of unknown unicast packets to all interfaces by configuring one VLAN or all VLANs to forward all unknown unicast traffic to a specific Layer 2 interface. This channels the unknown unicast traffic to a single interface.

Related Documentation

- Configuring Unknown Unicast Forwarding (CLI Procedure)
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 2022
- Understanding Storm Control on EX Series Switches
- Understanding Storm Control on EX Series Switches on page 2015
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
CHAPTER 36

Configuration

- Configuration Examples on page 2019
- Configuration Tasks on page 2021
- Configuration Statements on page 2027

Configuration Examples

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019

Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches

**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Storm control enables you to prevent network outages caused by broadcast storms on the LAN. You can configure storm control on an EX Series switch to rate-limit broadcast traffic, multicast traffic, and unknown unicast traffic at a specified level and to have packets dropped when the specified traffic level is exceeded, thereby preventing packets from proliferating and degrading the LAN.

**NOTE:** On EX4300 switches, the factory default configuration enables storm control on all Layer 2 interfaces, with the storm control level set to 80 percent of the available bandwidth used by the applicable traffic streams on that interface.
This example shows how to configure storm control on an EX Series switch running Junos OS with ELS.

- Requirements on page 2020
- Overview and Topology on page 2020
- Configuration on page 2020

Requirements

This example uses the following hardware and software components:

- One EX Series switch running Junos OS with ELS
- Junos OS Release 13.2 or later for EX Series switches

Overview and Topology

A storm is generated when messages are broadcast on a network and each message prompts a receiving node to respond by broadcasting its own messages on the network. This, in turn, prompts further responses, creating a snowball effect and resulting in a broadcast storm that can cause network outages.

You can use storm control to prevent broadcast storms by specifying the amount, also known as the storm control level, of broadcast traffic, multicast traffic, and unknown unicast traffic to be allowed on an interface. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined applicable traffic streams or as the percentage of available bandwidth used by the combined applicable traffic streams.

Storm control monitors the level of applicable incoming traffic and compares it with the level that you specify. If the combined level of the applicable traffic exceeds the specified level, the switch drops packets for the controlled traffic types. As an alternative to having the switch drop packets, you can configure storm control to shut down interfaces or temporarily disable interfaces (see the action-shutdown statement or the recovery-timeout statement) when the storm control level is exceeded.

The topology used in this example consists of one switch connected to various network devices. This example shows how to configure the storm control level on interface ge-0/0/0 by setting the level to a traffic rate of 15,000 Kbps, based on the traffic rate of the combined applicable traffic streams. If the combined traffic exceeds this level, the switch drops packets for the controlled traffic types to prevent a network outage.

Configuration

To quickly configure storm control based on the traffic rate in kilobits per second of the combined traffic streams, copy the following command and paste it into the switch terminal window:

```
[edit]
set forwarding-options storm-control-profiles sc all bandwidth-level 15000
set interfaces ge-0/0/0 unit 0 family ethernet-switching storm-control sc
```
Step-by-Step Procedure

To configure storm control:

1. Configure a storm control profile, sc, and specify the traffic rate in kilobits per second of the combined traffic streams:

   [edit]
   user@switch> set forwarding-options storm-control-profiles sc all bandwidth-level 15000

2. Bind the storm control profile, sc, to a logical interface:

   [edit]
   user@switch> set interfaces ge-0/0/0 unit 0 family ethernet-switching storm-control sc

Results

Display the results of the configuration:

[edit forwarding-options]
user@switch> show storm-control-profiles sc
all {
   bandwidth 15000;
}

[edit]
user@switch> show interfaces ge-0/0/0
unit 0 {
   family ethernet-switching {
      vlan {
         members default;
      }
      storm-control sc;
   }
}

Related Documentation

- Configuring or Disabling Storm Control (CLI Procedure) on page 2023
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 2023
- Understanding Storm Control on EX Series Switches on page 2015

Configuration Tasks

- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 2022
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 2023
- Configuring or Disabling Storm Control (CLI Procedure) on page 2023
NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Unknown Unicast Forwarding (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Unknown unicast traffic consists of packets with unknown destination MAC addresses. By default, the switch floods these packets to all interfaces associated with a VLAN. Forwarding such traffic to interfaces on the switch can create a security issue.

To prevent flooding unknown unicast traffic across the switch, configure unknown unicast forwarding to direct all unknown unicast packets within a VLAN out to a specific Layer 2 interface. You can configure each VLAN to divert unknown unicast traffic to different interfaces or use one interface for multiple VLANs.

To configure unknown unicast forwarding options:

NOTE: Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.

- Configure unknown unicast forwarding for a specific VLAN (here, the VLAN name is employee), and specify the Layer 2 interface to which all unknown unicast traffic will be forwarded:

  [edit switch-options]
  user@switch# set unknown-unicast-forwarding vlan vlan-name interface ge-x/y/z.0

Related Documentation
- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 2043
- Understanding Unknown Unicast Forwarding on EX Series Switches on page 2017
Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

An Ethernet switching access interface on an EX Series switch might shut down or be disabled as a result of one of the following port-security or storm control configurations:

- MAC limiting—`mac-limit` statement is configured with the action `shutdown`.
- MAC move limiting—(Not supported on EX9200) `mac-move-limit` statement is configured with the action `shutdown`.
- Storm control—`storm-control` statement is configured with the action `shutdown`.

You can configure the switch to automatically restore the disabled interfaces to service after a specified period of time. The specified `recovery-timeout` applies to all the interfaces that have been disabled due to MAC limiting, MAC move limiting, or storm control errors.

NOTE: To enable autorecovery, specify the timeout value for the interfaces to recover automatically. There is no default recovery timeout. If you do not specify a timeout value, you need to use the `clear ethernet-switching recovery-timeout` command to clear the errors and restore the interfaces to service.

Specify the recovery timeout period for the interface:

```
[edit interfaces interface-name family ethernet-switching]
user@switch# set recovery-timeout seconds
```

Related Documentation

- Configuring MAC Limiting (CLI Procedure) on page 2132
- Configuring MAC Move Limiting (CLI Procedure)
- Configuring or Disabling Storm Control (CLI Procedure) on page 2023

Configuring or Disabling Storm Control (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Disabling or Enabling Storm Control (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.
On EX4300 switches, the factory default configuration enables storm control on all Layer 2 switch interfaces. The default storm control level is set to 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.

Storm control is not enabled by default on EX9200 switches.

You can customize the storm control level for a specific interface. You specify the storm control level as the traffic rate in kilobits per second (Kbps) of the combined traffic streams or as the percentage of available bandwidth used by the combined traffic streams.

You can selectively disable storm control for broadcast, multicast, or unknown unicast traffic on all interfaces or on a specified interface. You can additionally disable storm control on registered or unregistered multicast traffic.

This topic describes:

- Configuring Storm Control on page 2025
- Disabling Storm Control on Broadcast Traffic on page 2025
- Disabling Storm Control on All Multicast Traffic on page 2025
- Disabling Storm Control on Registered Multicast Traffic on page 2026
- Disabling Storm Control on Unregistered Multicast Traffic on page 2026
- Disabling Storm Control on Unknown Unicast Traffic on page 2026
- Disabling Storm Control on Multiple Types of Traffic on page 2026
Configuring Storm Control

You can configure storm control for a specific interface. The storm control level can be customized by explicitly configuring either the bandwidth level or the bandwidth percentage.

- **bandwidth-level**—Configures the storm control level as the bandwidth in kilobits per second of the combined traffic streams.
- **bandwidth-percentage**—Configures the storm control level as a percentage of the available bandwidth used by the combined traffic streams.

To configure storm control:

1. Create a storm control profile and set the storm control level as the traffic rate in kilobits per second of the combined traffic streams:

   ```
   [edit forwarding-options]
   user@switch# set storm-control-profiles profile-name all bandwidth-level kbps
   ```

2. Bind the storm control profile to a logical interface:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name
   ```

Disabling Storm Control on Broadcast Traffic

To disable storm control on broadcast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams and exclude broadcast traffic:

   ```
   [edit forwarding-options]
   user@switch# set storm-control-profiles profile-name all bandwidth-level kbps no-broadcast
   ```

2. Bind the storm control profile to a logical interface:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name
   ```

Disabling Storm Control on All Multicast Traffic

To disable storm control on all multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams but exclude multicast traffic:

   ```
   [edit forwarding-options]
   user@switch# set storm-control-profiles profile-name all bandwidth-level kbps no-multicast
   ```

2. Bind the storm control profile to a logical interface:

   ```
   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name
   ```
Disabling Storm Control on Registered Multicast Traffic

To disable storm control on only registered multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams but exclude registered multicast traffic:

   [edit forwarding-options]
   user@switch# set storm-control-profiles profile-name all bandwidth-level kbps no-registered-multicast

2. Bind the storm control profile to a logical interface:

   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name

Disabling Storm Control on Unregistered Multicast Traffic

To disable storm control on only unregistered multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams but exclude unregistered multicast traffic:

   [edit forwarding-options]
   user@switch# set storm-control-profiles profile-name all bandwidth-level kbps no-unregistered-multicast

2. Bind the storm control profile to a logical interface:

   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name

Disabling Storm Control on Unknown Unicast Traffic

To disable storm control on only unknown unicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams but exclude unregistered multicast traffic:

   [edit forwarding-options]
   user@switch# set storm-control-profiles profile-name all bandwidth-level kbps no-unknown-unicast

2. Bind the storm control profile to a logical interface:

   [edit]
   user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name

Disabling Storm Control on Multiple Types of Traffic

To disable storm control on broadcast and multicast traffic:

1. Create a storm control profile with the storm control level set as the traffic rate in kilobits per second of the combined traffic streams but exclude broadcast and multicast traffic:
[edit forwarding-options]
user@switch# set storm-control-profiles profile-name all bandwidth-level kbps no-broadcast no-multicast

2. Bind the storm control profile to a logical interface:

[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching storm-control profile-name

Related Documentation
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
- Understanding Storm Control on EX Series Switches on page 2015

Configuration Statements

- [edit switch-options] Configuration Statement Hierarchy on EX Series Switches on page 2027

[edit switch-options] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit switch-options] hierarchy level on EX Series switches.

- Supported statements are those that you can use to configure some aspect of a software feature on the switch.
- Unsupported statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit switch-options] Hierarchy Level on page 2027
- Unsupported Statements in the [edit switch-options] Hierarchy Level on page 2028

Supported Statements in the [edit switch-options] Hierarchy Level

The following hierarchy shows the [edit switch-options] configuration statements supported on EX Series switches:

switch-options {
  authentication-whitelist mac-address {
    interface interface-name;
    vlan-assignment (vlan-id | vlan-name);
  }
  interface interface-name {
    interface-mac-limit number {
      packet-action action;
    }
    no-mac-learning;
    persistent-learning
Unsupported Statements in the [edit switch-options] Hierarchy Level

All statements in the [edit switch-options] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 259: Unsupported [edit switch-options] Configuration Statements on EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-error-disable</td>
<td>[edit switch-options]</td>
</tr>
<tr>
<td>disable-timeout</td>
<td>[edit switch-options port-error-disable]</td>
</tr>
</tbody>
</table>

NOTE: Variables, such as filename, are not shown in the statements or hierarchies.
**action-shutdown**

**Syntax**

```
action-shutdown;
```

**Hierarchy Level**

- For platforms with ELS:
  ```
  [edit forwarding-options storm-control-profiles profile-name]
  ```
- For platforms without ELS:
  ```
  [edit ethernet-switching-options storm-control]
  ```

**Release Information**

Statement introduced in Junos OS Release 9.6 for EX Series switches.


(See “Getting Started with Enhanced Layer 2 Software” on page 3 for information about ELS.)

**Description**

Shut down or disable interfaces when the storm control level is exceeded, as follows:

- If you set both the action-shutdown and the port-error-disable statements, the interfaces are disabled temporarily and recover automatically when the disable timeout expires.

- If you set both the action-shutdown and the recovery-timeout statements, the interfaces are disabled temporarily and recover automatically when the recovery timeout expires.

- If you set the action-shutdown statement and do not specify the port-error-disable statement, the interfaces that are enabled for storm control are shut down when the storm control level is exceeded and they do not recover automatically from that port-error condition. You must issue the clear ethernet-switching port-error command to clear the port error and restore the interfaces to service.

- If you set the action-shutdown statement and do not specify the recovery-timeout statement, the interfaces that are enabled for storm control are shut down when the storm control level is exceeded and they do not recover automatically from that port-error condition. You must issue the clear ethernet-switching recovery-timeout command to clear the port error and restore the interfaces to service.

**Default**

The action-shutdown option is not enabled. When the storm control level is exceeded, the switch drops applicable types of traffic on the specified interfaces. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- port-error-disable
- disable-timeout
- recovery-timeout on page 2040
- clear ethernet-switching port-error
- clear ethernet-switching recovery-timeout on page 2045
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 2023
**bandwidth-level**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>bandwidth-level kbps;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit forwarding-options storm-control-profiles profile-name all]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Configure the storm control level as the bandwidth in kilobits per second of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams.</td>
</tr>
</tbody>
</table>

**NOTE:** When you configure storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control level of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.

**Default**

On EX4300 switches—If you do not specify the storm control level using either the bandwidth-level or the bandwidth-percentage statements, the storm control level defaults to 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.

On EX9200 switches—Storm control is not enabled by default.

**Options**

- **bandwidth-level kbps**—Traffic rate in kilobits per second of the combined broadcast, multicast, and unknown unicast traffic streams.
  - **Range:** 100 through 10,000,000
  - **Default:** None

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- bandwidth-percentage on page 2032
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
- Configuring or Disabling Storm Control (CLI Procedure) on page 2023
bandwidth-percentage

Syntax      bandwidth-percentage percentage;

Hierarchy Level [edit forwarding-options storm-control-profiles profile-name all]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Configure the storm control level as the percentage of available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams on an interface. The storm control level is configured as part of the storm control profile.

NOTE: When you configure storm control level on an aggregated Ethernet interface, the storm control level for each member of the aggregated Ethernet interface is set to that bandwidth. For example, if you configure a storm control level of 15,000 Kbps on ae1, and ae1 has two members, ge-0/0/0 and ge-0/0/1, each member has a storm control level of 15,000 Kbps. Thus, the storm control level on ae1 allows a traffic rate of up to 30,000 Kbps of combined broadcast, multicast, and unknown unicast traffic.

Default On EX4300 switches—The storm control level is 80 percent of the available bandwidth used by the combined broadcast, unknown unicast, and multicast traffic streams.

On EX9200 switches—Storm control is not enabled by default.

Required Privilege Level system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

• bandwidth-level on page 2031

• Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019

• Configuring or Disabling Storm Control (CLI Procedure) on page 2023
### interface (Unknown Unicast Forwarding)

**Syntax**

Syntax: `interface interface-name;`

**Hierarchy Level**

- For platforms with ELS:
  
  `[edit switch-options unknown-unicast-forwarding vlan vlan-name]`

- For platforms without ELS:

  `[edit ethernet-switching-options unknown-unicast-forwarding vlan vlan-name],`

**Release Information**

Statement introduced in Junos OS Release 9.3 for EX Series switches.


**Description**

Specify the interface to which unknown unicast packets will be forwarded.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- `show vlans`
- `show ethernet-switching table`
- `Configuring Unknown Unicast Forwarding (CLI Procedure)`
- `Understanding Unknown Unicast Forwarding on EX Series Switches on page 2017`
no-broadcast

**Syntax**

```yaml
no-broadcast;
```

**Hierarchy Level**

- For platforms with ELS:

  ```
  [edit forwarding-options storm-control-profiles profile-name all]
  ```

- For platforms without ELS:

  ```
  [edit ethernet-switching-options storm-control interface (all | interface-name)],
  ```

**Release Information**

Statement introduced in Junos OS Release 9.1 for EX Series switches.  
(See “Getting Started with Enhanced Layer 2 Software” on page 3 for information about ELS.)

**Description**

Disable storm control for broadcast traffic for the specified interface or for all interfaces.

**Default**

- On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control on broadcast, multicast, or unknown-unicast traffic.

- On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic.

- On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.

- On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually.

- On EX9200 switches—Storm control is not enabled by default.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches
- Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
- Disabling or Enabling Storm Control (CLI Procedure)
• Configuring or Disabling Storm Control (CLI Procedure) on page 2023
no-multicast

Syntax  no-multicast;

Hierarchy Level  • For platforms with ELS:
  [edit forwarding-options storm-control-profiles profile-name all]
  • For platforms without ELS:
  [edit ethernet-switching-options storm-control interface (all | interface-name)],

Release Information  Statement introduced in Junos OS Release 10.3 for EX Series switches.
  (See “Getting Started with Enhanced Layer 2 Software” on page 3 for information about ELS.)

Description  Disable storm control for all multicast traffic (both registered multicast and unregistered multicast) for the specified interface or for all interfaces.

Default  • On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams.

  • On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic.

  • On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.

  • On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually.

  • On EX9200 switches—Storm control is not enabled by default.

Required Privilege Level  system—To view this statement in the configuration.
  system-control—To add this statement to the configuration.

Related Documentation  • no-registered-multicast on page 2037
  • no-unregistered-multicast on page 2039
  • Disabling or Enabling Storm Control (CLI Procedure)
no-registered-multicast

Syntax
no-registered-multicast;

Hierarchy Level
- For platforms with ELS:
  [edit forwarding-options storm-control-profiles profile-name all]
- For platforms without ELS:
  [edit ethernet-switching-options storm-control interface (all | interface-name)],

Release Information

Description
(EX8200 switches only) Disable storm control for registered multicast traffic for the specified interface or for all interfaces.

(EX4300 and EX9200 switches only) Exclude storm control for registered multicast traffic from a storm control profile.

Default
EX4300 and EX8200 switches—Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic. The default storm control level is 80 percent of the available bandwidth used by the combined applicable traffic streams.

EX9200 switches—Storm control is not enabled by default.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- no-multicast on page 2036
- no-unregistered-multicast on page 2039
- Understanding Storm Control on EX Series Switches
- Understanding Storm Control on EX Series Switches on page 2015
no-unknown-unicast

Syntax  no-unknown-unicast;

Hierarchy Level  • For platforms with ELS:
  [edit forwarding-options storm-control-profiles profile-name all]
  • For platforms without ELS:
  [edit ethernet-switching-options storm-control interface (all | interface-name)],

Release Information Statement introduced in Junos OS Release 9.1 for EX Series switches.
(See “Getting Started with Enhanced Layer 2 Software” on page 3 for information about ELS.)

Description Disable storm control for unknown unicast traffic for the specified interface or for all interfaces.

Default  • On EX2200, EX3200, EX3300, and EX4200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control on broadcast, multicast, or unknown-unicast traffic.

  • On EX4300 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. You can selectively disable storm control on any type of traffic.

  • On EX4500 and EX8200 switches—The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined broadcast, multicast, and unknown unicast traffic streams. On EX8200 switches, you can selectively disable storm control on registered multicast traffic, on unregistered multicast traffic, or on both types of multicast traffic.

  • On EX6200 switches—Storm control does not apply to multicast traffic by default. The factory default configuration enables storm control on all interfaces at 80 percent of the available bandwidth used by the combined unknown unicast and broadcast traffic streams. You can selectively disable storm control for each type of traffic individually.

  • On EX9200 switches—Storm control is not enabled by default.

Required Privilege Level  system—To view this statement in the configuration.
  system-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
Disabling or Enabling Storm Control (CLI Procedure)

Configuring or Disabling Storm Control (CLI Procedure) on page 2023

no-unregistered-multicast

Syntax

```plaintext
no-unregistered-multicast;
```

Hierarchy Level

- For platforms with ELS:
  ```plaintext
  [edit forwarding-options storm-control-profiles profile-name all]
  ```
- For platforms without ELS:
  ```plaintext
  [edit ethernet-switching-options storm-control interface (all | interface-name)],
  ```

Release Information


Description

(EX8200 switches only) Disable storm control for unregistered multicast traffic for the specified interface or for all interfaces.

(EX4300 and EX9200 switches only) Exclude storm control for unregistered multicast traffic from a storm control profile.

Default

EX4300 and EX8200 switches—Storm control is enabled for unknown unicast traffic, multicast traffic, and broadcast traffic. The default storm control level is 80 percent of the available bandwidth used by the combined applicable traffic streams.

EX9200 switches—Storm control is not enabled by default.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- no-multicast on page 2036
- no-registered-multicast on page 2037
- Understanding Storm Control on EX Series Switches
- Understanding Storm Control on EX Series Switches on page 2015
**recovery-timeout**

**Syntax**
```
recovery-timeout seconds;
```

**Hierarchy Level**
```
[edit interfaces interface-name family ethernet-switching]
```

**Release Information**

**Description**
Disable rather than block an interface when enforcing MAC limiting, MAC move limiting, or rate-limiting configuration options for shutting down the interface, and allow the interface to recover automatically from the error condition after the specified period of time:

- If you have enabled MAC limiting with the `shutdown` option and you enable `recovery-timeout`, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.

- If you have enabled MAC move limiting (Not supported on EX9200) with the `shutdown` option and you enable `recovery-timeout`, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.

- If you have enabled storm control with the `action-shutdown` option and you enable `recovery-timeout` the switch disables (rather than shuts down) the interface when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.

**NOTE:** The recovery-timeout configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after recovery-timeout has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the operational mode command `clear ethernet-switching recovery-timeout`.

**Default**
Not enabled.

**Options**
- `seconds`— Number of seconds that the interface remains in a disabled state due to a port error prior to automatic recovery.

  **Range:** 10 through 3600

**Required Privilege Level**
system—To view this statement in the configuration.
system–control—To add this statement to the configuration.

**Related Documentation**
- action-shutdown on page 2029
- Configuring MAC Limiting (CLI Procedure) on page 2132
- Configuring MAC Move Limiting (CLI Procedure)
storm-control

Syntax
storm-control storm-control-profile;

Hierarchy Level
[edit interfaces interface-name unit number family ethernet-switching]

Release Information
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Bind a storm control profile to a logical interface.

Required Privilege
Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
• Understanding Storm Control on EX Series Switches on page 2015

storm-control-profiles

Syntax
storm-control-profiles profile-name {
    action-shutdown;
    all {
        bandwidth-level;
        bandwidth-percentage;
        no-broadcast;
        no-multicast;
        no-registered-multicast;
        no-unknown-unicast;
        no-unregistered-multicast;
    }
}

Hierarchy Level
[edit forwarding-options]

Release Information
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Configure a storm control profile on the switch.
The remaining statements are explained separately.

Required Privilege
Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Storm Control to Prevent Network Outages on EX Series Switches on page 2019
• Understanding Storm Control on EX Series Switches on page 2015
unknown-unicast-forwarding

Syntax

unknown-unicast-forwarding {
  vlan vlan-name {
    interface interface-name;
  }
}

Hierarchy Level

- For platforms with ELS:
  [edit switch-options on page 2027]
- For platforms without ELS:
  [edit ethernet-switching-options]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description

Configure the switch to forward all unknown unicast packets in a VLAN or on all VLANs to a particular interface.

NOTE: Before you can configure unknown unicast forwarding within a VLAN, you must first configure that VLAN.

The remaining statements are explained separately.

Default

Unknown unicast packets are flooded to all interfaces that belong to the same VLAN.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- show vlans
- show ethernet-switching table
- Configuring Unknown Unicast Forwarding (CLI Procedure)
- Configuring Unknown Unicast Forwarding (CLI Procedure) on page 2022
- Understanding Unknown Unicast Forwarding on EX Series Switches on page 2017
CHAPTER 37

Administration

- Routine Monitoring on page 2043
- Operational Commands on page 2044

Routine Monitoring

- Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface on page 2043

Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface

Purpose  Verify that a VLAN is forwarding all unknown unicast packets (those with unknown destination MAC addresses) to a single trunk interface instead of flooding unknown unicast packets across all interfaces that are members of the same VLAN.

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, See: Verifying That Unknown Unicast Packets Are Forwarded to a Trunk Interface. For ELS details see: "Getting Started with Enhanced Layer 2 Software" on page 3.
Action  Display the forwarding interface for unknown unicast packets for a VLAN (here, the VLAN name is v1):

```
user@switch> show configuration switch-options

unknown-unicast-forwarding {
  vlan v1 {
    interface ge-0/0/7.0;
  }
}
```

Display the Ethernet switching table:

```
user@switch> show ethernet-switching table vlan-name v1
Ethernet-switching table: 3 unicast entries
  VLAN  MAC address  Type     Age Interfaces
    v1     *          Flood    -   All-members
    v1  00:01:09:00:00:00 Learn    24   ge-0/0/7.0
    v1  00:11:09:00:01:00 Learn    37   ge-0/0/3.0
```

Meaning  The sample output from the `show configuration switch-options` command shows that the unknown unicast forwarding interface for VLAN v1 is interface ge-0/0/7. The `show ethernet-switching table` command shows that an unknown unicast packet is received on interface ge-0/0/3 with the destination MAC address (DMAC) 00:01:09:00:00:00 and the source MAC address (SMAC) of 00:11:09:00:01:00. This shows that the SMAC of the packet is learned in the normal way (through the interface ge-0/0/3.0), while the DMAC is learned on interface ge-0/0/7.

Related Documentation  • Configuring Unknown Unicast Forwarding (CLI Procedure) on page 2022

Operational Commands
clear ethernet-switching recovery-timeout

Syntax
clear ethernet-switching recovery-timeout

Release Information
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch, and restore the interfaces to service.

Options

none—Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch and restore these interfaces to service.

Required Privilege
Level
clear

Related Documentation
• Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 2023

Output Fields
This command produces no output.
CHAPTER 38

Overview

- Bridging and VLANs on page 2049
- Redundant Trunk Groups on page 2068
- Proxy ARP on page 2070

Bridging and VLANs

- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Understanding Integrated Routing and Bridging Interfaces and Routed VLAN Interfaces on EX Series Switches on page 2058
- Understanding Virtual Routing Instances on EX Series Switches on page 2062
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches on page 2063
- Understanding MAC Address Aging on page 2066

Understanding Bridging and VLANs on EX Series Switches

Network switches use Layer 2 bridging protocols to discover the topology of their LAN and to forward traffic toward destinations on the LAN. This topic explains the following concepts regarding bridging and VLANs on Juniper Networks EX Series Ethernet Switches:

- History of VLANs on page 2050
- How Bridging of VLAN Traffic Works on page 2050
- Packets Are Either Tagged or Untagged on page 2051
- Switch Interface Modes—Access, Trunk, or Tagged Access on page 2052
- Additional Advantages of Using VLANs on page 2054
- Maximum VLANs and VLAN Members Per Switch on page 2054
- A Default VLAN Is Configured on Most Switches on page 2055
- Assigning Traffic to VLANs on page 2055
- Forwarding VLAN Traffic on page 2056
- VLANs Communicate with Integrated Routing and Bridging Interfaces or Routed VLAN Interfaces on page 2056
History of VLANs

Ethernet LANs were originally designed for small, simple networks that primarily carried text. However, over time, the type of data carried by LANs grew to include voice, graphics, and video. This more complex data, when combined with the ever-increasing speed of transmission, eventually became too much of a load for the original Ethernet LAN design. Multiple packet collisions were significantly slowing down the larger LANs.

The IEEE 802.1D-2004 standard helped evolve Ethernet LANs to cope with the higher data and transmission requirements by defining the concept of transparent bridging (generally called simply bridging). Bridging divides a single physical LAN (now called a single broadcast domain) into two or more virtual LANs, or VLANs. Each VLAN is a collection of some of the LAN nodes grouped together to form individual broadcast domains.

When VLANs are grouped logically by function or organization, a significant percentage of data traffic stays within the VLAN. This relieves the load on the LAN because all traffic no longer has to be forwarded to all nodes on the LAN. A VLAN first transmits packets within the VLAN, thereby reducing the number of packets transmitted on the entire LAN. Because packets whose origin and destination are in the same VLAN are forwarded only within the local VLAN, packets that are not destined for the local VLAN are the only ones forwarded to other broadcast domains. This way, bridging and VLANs limit the amount of traffic flowing across the entire LAN by reducing the possible number of collisions and packet retransmissions within VLANs and on the LAN as a whole.

How Bridging of VLAN Traffic Works

Because the objective of the IEEE 802.1D-2004 standard was to reduce traffic and therefore reduce potential transmission collisions for Ethernet, a system was implemented to reuse information. Instead of having a switch go through a location process every time a frame is sent to a node, the transparent bridging protocol allows a switch to record the location of known nodes. Before sending a packet, a switch using bridging first consults the switching tables to see if that node has already been located. If the location of a node is known, the frame is sent directly to that node.

Transparent bridging uses five mechanisms to create and maintain Ethernet switching tables on the switch:

- Learning
- Forwarding
- Flooding
- Filtering
- Aging

The key bridging mechanism used by LANs and VLANs is learning. When a switch is first connected to an Ethernet LAN or VLAN, it has no information about other nodes on the network. As packets are sent, the switch learns the embedded MAC addresses of the
sending nodes and stores them in the Ethernet switching table, along with two other pieces of information—the interface (or port) on which the traffic was received on the destination node and the time the address was learned.

Learning allows switches to then do forwarding. By consulting the Ethernet switching table to see whether the table already contains the frame’s destination MAC address, switches save time and resources when forwarding packets to the known MAC addresses. If the Ethernet switching table does not contain an entry for an address, the switch uses flooding to learn that address.

Flooding finds a particular destination MAC address without using the Ethernet switching table. When traffic originates on the switch and the Ethernet switching table does not yet contain the destination MAC address, the switch first floods the traffic to all other interfaces within the VLAN. When the destination node receives the flooded traffic, it can send an acknowledgment packet back to the switch, allowing it to learn the MAC address of the node and add the address to its Ethernet switching table.

Filtering, the fourth bridging mechanism, is how broadcast traffic is limited to the local VLAN whenever possible. As the number of entries in the Ethernet switching table grows, the switch pieces together an increasingly complete picture of the VLAN and the larger LAN—it learns which nodes are in the local VLAN and which are on other network segments. The switch uses this information to filter traffic. Specifically, for traffic whose source and destination MAC addresses are in the local VLAN, filtering prevents the switch from forwarding this traffic to other network segments.

To keep entries in the Ethernet switching table current, the switch uses a fifth bridging mechanism, aging. Aging is the reason that the Ethernet switching table entries include timestamps. Each time the switch detects traffic from a MAC address, it updates the timestamp. A timer on the switch periodically checks the timestamp, and if it is older than a user-configured value, the switch removes the node’s MAC address from the Ethernet switching table. This aging process eventually flushes unavailable network nodes out of the Ethernet switching table.

Packets Are Either Tagged or Untagged

When an Ethernet LAN is divided into VLANs, each VLAN is identified by a unique 802.1Q ID. The VLAN IDs 1 through 4094 can be assigned to VLANs, while VLAN IDs 0 and 4095 are reserved by Junos OS and cannot be assigned.

Ethernet packets include a tag protocol identifier (TPID) EtherType field, which identifies the protocol being transported. When a device within a VLAN generates a packet, this field includes a value of 0x8100, which indicates that the packet is a VLAN-tagged packet. The packet also has a VLAN ID field that includes the unique 802.1Q ID, which identifies the VLAN to which the packet belongs.

In addition to the TPID EtherType value of 0x8100, EX Series switches that run Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style also support values of 0x88a8 (Provider Bridging and Shortest Path Bridging) and 0x9100 (Q-inQ).
For a simple network that has only a single VLAN, all packets include a default 802.1Q tag, which is the only VLAN membership that does not mark the packet as tagged. These packets are untagged packets.

**Switch Interface Modes—Access, Trunk, or Tagged Access**

Ports, or interfaces, on a switch operate in one of three modes:

- Access mode
- Trunk mode
- Tagged-access mode

**Access Mode**

An interface in access mode connects a switch to a single network device, such as a desktop computer, an IP telephone, a printer, a file server, or a security camera. Access interfaces accept only untagged packets.

By default, when you boot an EX Series switch that runs Junos OS that does not support ELS and use the factory default configuration, or when you boot such a switch and do not explicitly configure a port mode, all interfaces on the switch are in access mode and accept only untagged packets from the VLAN named `default`. You can optionally configure another VLAN and use that VLAN instead of `default`.

On an EX Series switch that runs Junos OS that supports ELS, the VLAN named `default` is not supported. Therefore, on such switches, you must explicitly configure at least one VLAN, even if your network is simple and you want only one broadcast domain to exist. After you assign an interface to a VLAN, the interface functions in access mode.

For EX Series switches that run either type of software, you can also configure a trunk port or interface to accept untagged packets from a user-configured VLAN. For details about this concept (native VLAN), see “Trunk Mode and Native VLAN” on page 2053.

**Trunk Mode**

Trunk mode interfaces are generally used to connect switches to one another. Traffic sent between switches can then consist of packets from multiple VLANs, with those packets multiplexed so that they can be sent over the same physical connection. Trunk interfaces usually accept only tagged packets and use the VLAN ID tag to determine both the packets’ VLAN origin and VLAN destination.

On an EX Series switch that runs software that does not support ELS, an untagged packet is not recognized on a trunk port unless you configure additional settings on that port.

On an EX Series switch that runs Junos OS that supports ELS, a trunk port recognizes untagged control packets for protocols such as the Link Aggregation Control Protocol (LACP) and the Link Layer Discovery Protocol (LLDP). However, the trunk port does not recognize untagged data packets unless you configure additional settings on that port.

In the rare case where you want untagged packets to be recognized by a trunk port on EX Series switches that run either type of software, you must configure the single VLAN
on a trunk port as a native VLAN. For more information about native VLANs, see "Trunk Mode and Native VLAN" on page 2053.

**Trunk Mode and Native VLAN**

On an EX Series switch that runs Junos OS that does not support ELS, a trunk port does not recognize packets that do not include VLAN tags, which are also known as untagged packets. On an EX Series switch that runs Junos OS that supports ELS, a trunk port recognizes untagged control packets, but it does not recognize untagged data packets. With native VLAN configured, untagged packets that a trunk port normally does not recognize are sent over the trunk interface. In a situation where packets pass from a device, such as an IP phone or printer, to a switch in access mode, and you want those packets sent from the switch over a trunk port, use native VLAN mode. Create a native VLAN by configuring a VLAN ID for it, and specify that the trunk port is a member of the native VLAN.

The switch’s trunk port will then treat those packets differently than the other tagged packets. For example, if a trunk port has three VLANs, 10, 20, and 30, assigned to it with VLAN 10 being the native VLAN, packets on VLAN 10 that leave the trunk port on the other end have no 802.1Q header (tag).

There is another native VLAN option for EX Series switches that do not support ELS. You can have the switch add and remove tags for untagged packets. To do this, you first configure the single VLAN as a native VLAN on a port attached to a device on the edge. Then, assign a VLAN ID tag to the single native VLAN on the port connected to a device. Last, add the VLAN ID to the trunk port. Now, when the switch receives the untagged packet, it adds the ID you specified and sends and receives the tagged packets on the trunk port configured to accept that VLAN.

**Tagged-Access Mode**

Only EX Series switches that run Junos OS that does not use the ELS configuration style support tagged-access mode. Tagged-access mode accommodates cloud computing, specifically scenarios including virtual machines or virtual computers. Because several virtual computers can be included on one physical server, the packets generated by one server can contain an aggregation of VLAN packets from different virtual machines on that server. To accommodate this situation, tagged-access mode reflects packets back to the physical server on the same downstream port when the destination address of the packet was learned on that downstream port. Packets are also reflected back to the physical server on the downstream port when the destination has not yet been learned. Therefore, the third interface mode, tagged access, has some characteristics of access mode and some characteristics of trunk mode:

- Like access mode, tagged-access mode connects the switch to an access layer device. Unlike access mode, tagged-access mode is capable of accepting VLAN tagged packets.

- Like trunk mode, tagged-access mode accepts VLAN tagged packets from multiple VLANs. Unlike trunk port interfaces, which are connected at the core/distribution layer, tagged-access port interfaces connect devices at the access layer.

Like trunk mode, tagged-access mode also supports native VLAN.
NOTE: Control packets are never reflected back on the downstream port.

**Additional Advantages of Using VLANs**

In addition to reducing traffic and thereby speeding up the network, VLANs have the following advantages:

- VLANs provide segmentation services traditionally provided by routers in LAN configurations, thereby reducing hardware equipment costs.

- Packets coupled to a VLAN can be reliably identified and sorted into different domains. You can contain broadcasts within parts of the network, thereby freeing up network resources. For example, when a DHCP server is plugged into a switch and starts broadcasting its presence, you can prevent some hosts from accessing it by using VLANs to split up the network.

- For security issues, VLANs provide granular control of the network because each VLAN is identified by a single IP subnetwork. All packets passing in and out of a VLAN are consistently tagged with the VLAN ID of that VLAN, thereby providing easy identification, because a VLAN ID on a packet cannot be altered. (For an EX Series switch that runs Junos OS that does not support ELS, we recommend that you avoid using 1 as a VLAN ID, because that ID is a default value.)

- VLANs react quickly to host relocation—this is also due to the persistent VLAN tag on packets.

- On an Ethernet LAN, all network nodes must be physically connected to the same network. In VLANs, the physical location of nodes is not important—you can group network devices in any way that makes sense for your organization, such as by department or business function, types of network nodes, or physical location.

**Maximum VLANs and VLAN Members Per Switch**

The number of VLANs supported per switch varies for each switch. Use the configuration-mode command `set vlans <vlan-name> vlan-id ?` to determine the maximum number of VLANs allowed on a switch. You cannot exceed this VLAN limit because you have to assign a specific ID number when you create a VLAN—you could overwrite one of the numbers, but you cannot exceed the limit.

You can, however, exceed the recommended VLAN member maximum for a switch.

On an EX Series switch that runs Junos OS that does not support the ELS configuration style, the maximum number of VLAN members allowed on the switch is eight times the maximum number of VLANs that the switch supports (vmember limit = vlan max * 8). If the configuration of the switch exceeds the recommended VLAN member maximum, a warning message appears when you commit the configuration. If you commit the configuration despite the warning, the commit succeeds, but there is a risk of the Ethernet switching process (eswd) failing as a result of memory allocation failure.
On an EX Series switch that runs Junos OS that supports ELS, the maximum number of VLAN members allowed on the switch is 24 times the maximum number of VLANs that the switch supports (vmember limit = vlan max * 24). If the configuration of the switch exceeds the recommended VLAN member maximum, a warning message appears in the system log (syslog).

**A Default VLAN Is Configured on Most Switches**

*NOTE:* EX Series switches that run Junos OS with the ELS configuration style do not support a default VLAN.

Some EX Series switches that run Junos OS that does not support the ELS configuration style are preconfigured with a VLAN named default that does not tag packets and operates only with untagged packets. On these switches, each interface already belongs to the VLAN named default and all traffic uses this VLAN until you configure more VLANs and assign traffic to those VLANs.

The following EX Series switches that run Junos OS that does not support the ELS are not preconfigured to belong to default or any other VLAN:

- Modular switches, such as the EX8200 switches and EX6200 switches
- Switches that are part of a Virtual Chassis

The reason that these switches are not preconfigured is that the physical configuration in both situations is flexible. There is no way of knowing which line cards have been inserted in either the EX8200 switch or EX6200 switch. There is also no way of knowing which switches are included in the Virtual Chassis. Switch interfaces in these two cases must first be defined as Ethernet switching interfaces. After an interface is defined as an Ethernet switching interface, the default VLAN appears in the output from the ? help and other commands.

*NOTE:* When a Juniper Networks EX4500 Ethernet Switch, EX4200 Ethernet Switch, or EX3300 Ethernet Switch is interconnected with other switches in a Virtual Chassis configuration, each individual switch that is included as a member of the configuration is identified with a member ID. The member ID functions as an FPC slot number. When you are configuring interfaces for a Virtual Chassis configuration, you specify the appropriate member ID (0 through 9) as the slot element of the interface name. The default factory settings for a Virtual Chassis configuration include FPC 0 as a member of the default VLAN because FPC 0 is configured as part of the ethernet-switching family. In order to include FPC 1 through FPC 9 in the default VLAN, add the ethernet-switching family to the configurations for those interfaces.

**Assigning Traffic to VLANs**

You can assign traffic on any switch to a particular VLAN by referencing either the interface port of the traffic or the MAC addresses of devices sending traffic.
Assign VLAN Traffic According to the Interface Port Source

This method is most commonly used to assign traffic to VLANs. In this case, you specify that all traffic received on a particular switch interface is assigned to a specific VLAN. You configure this VLAN assignment when you configure the switch, by using either the VLAN number (called a VLAN ID) or by using the VLAN name, which the switch then translates into a numeric VLAN ID. This method is referred to simply as creating a VLAN because it is the most commonly used method.

Assign VLAN Traffic According to the Source MAC Address

In this case, all traffic received from a specific MAC address is forwarded to a specific egress interface (next hop) on the switch. MAC-based VLANs are either static (named MAC addresses configured one at a time) or dynamic (configured using a RADIUS server).

To configure a static MAC-based VLAN on an EX Series switch that supports ELS, see Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure). To configure a static MAC-based VLAN on an EX Series switch that does not support ELS, see Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure).

For information about using 802.1X authentication to authenticate end devices and allow access to dynamic VLANs configured on a RADIUS server, see “Understanding Dynamic VLANs for 802.1X on EX Series Switches” on page 1670. You can optionally implement this feature to offload the manual assignment of VLAN traffic to automated RADIUS server databases.

Forwarding VLAN Traffic

To pass traffic within a VLAN, the switch uses Layer 2 forwarding protocols, including IEEE 802.1Q spanning-tree protocols and Multiple VLAN Registration Protocol (MVRP).

To pass traffic between two VLANs, the switch uses standard Layer 3 routing protocols, such as static routing, OSPF, and RIP. On EX Series switches, the same interfaces that support Layer 2 bridging protocols also support Layer 3 routing protocols, providing multilayer switching.

To pass traffic from a single device on an access port to a switch and then pass those packets on a trunk port, use the native mode configuration previously discussed under “Trunk Mode” on page 2052.

VLANs Communicate with Integrated Routing and Bridging Interfaces or Routed VLAN Interfaces

Traditionally, switches sent traffic to hosts that were part of the same broadcast domain (VLAN) but routers were needed to route traffic from one broadcast domain to another. Also, only routers performed other Layer 3 functions such as traffic engineering.

EX Series switches that run Junos OS that supports the ELS configuration style perform inter-VLAN routing functions using an integrated routing and bridging (IRB) interface named irb, while EX Series switches that run Junos OS that does not support ELS perform these functions using a routed VLAN interface (RVI) named vlan. These interfaces detect both MAC addresses and IP addresses and route data to Layer 3 interfaces, thereby frequently eliminating the need to have both a switch and a router.
Related Documentation

- Understanding Private VLANs on EX Series Switches
- Understanding Layer 2 Protocol Tunneling on EX Series Switches
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches on page 2063
- Understanding Integrated Routing and Bridging Interfaces and Routed VLAN Interfaces on EX Series Switches on page 2058
- Understanding Edge Virtual Bridging for Use with VEPA Technology
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073
- Example: Setting Up Bridging with Multiple VLANs for EX Series Switches
- Example: Connecting an Access Switch to a Distribution Switch
- Example: Connecting Access Switches to a Distribution Switch on page 2083
Understanding Integrated Routing and Bridging Interfaces and Routed VLAN Interfaces on EX Series Switches

Virtual LANs (VLANs), by definition, divide a LAN's broadcast environment into isolated virtual broadcast domains, thereby limiting the amount of traffic flowing across the entire LAN and reducing the possible number of collisions and packet retransmissions within the LAN. For example, you might want to create a VLAN that includes the employees in a department and the resources that they use often, such as printers, servers, and so on.

Of course, you also want to allow these employees to communicate with people and resources in other VLANs. To forward packets between VLANs, you traditionally needed a router that connected the VLANs. However, you can also accomplish this forwarding with a switch by configuring one of the following features:

- On Juniper Networks EX Series Ethernet Switches that run Juniper Networks Junos operating system (Junos OS) that supports the Enhanced Layer 2 Software (ELS) configuration style, configure an integrated routing and bridging (IRB) interface.
- On EX Series switches that run Junos OS that does not support ELS, configure a routed VLAN interface (RVI).

**NOTE:** IRB interfaces and RVIs provide the same functionality. Where the functionality for both features is the same, this topic uses the term these *interfaces* to refer collectively to both IRB interfaces and RVIs. Where differences exist between the two features, this topic calls out the IRB interfaces and RVIs separately.

Configuring a switch to route traffic between VLANs reduces complexity and eliminates the costs associated with purchasing, installing, managing, powering, and cooling a router.

These interfaces route only VLAN traffic and work by logically dividing a switch into multiple virtual routing instances, thereby isolating VLAN traffic traveling across the network into virtual segments. These interfaces allow switches to recognize which packets are being sent to another VLAN's MAC addresses—then, packets are bridged (switched) whenever the destination is within the same VLAN and are routed through these interfaces only when necessary. Whenever packets can be switched instead of routed, several layers of processing are eliminated. The switches rely on their Layer 3 capabilities to provide this basic routing between VLANs:

- Two VLANs on the same switch
- Two VLANs on different switches (routing is provided by an intermediary third switch.)
Figure 27 on page 2059 illustrates a switch routing VLAN traffic between two access layer switches using one of these interfaces.

Figure 27: An IRB Interface or RVI on a Switch Providing Routing Between Two Access Switches

This topic describes:

- When Should I Use an IRB Interface or RVI? on page 2059
- How Does an IRB Interface or RVI Work? on page 2059
- Creating an IRB Interface or RVI on page 2060
- Viewing IRB Interface and RVI Statistics on page 2061
- IRB Interfaces and RVI Functions and Other Technologies on page 2061

**When Should I Use an IRB Interface or RVI?**

Configure an IRB interface or an RVI for a VLAN if you need to:

- Allow traffic to be routed between VLANs.
- Provide Layer 3 IP connectivity to the switch.
- Monitor individual VLANs for billing purposes. Service providers often need to monitor traffic for this purpose, but this capability can be useful for enterprises where various groups share the cost of the network.

**How Does an IRB Interface or RVI Work?**

For an IRB interface, the switch provides the name irb, and for an RVI, the switch provides the name vlan. Like all Layer 3 interfaces, these interfaces require a logical unit number with an IP address assigned to it. In fact, to be useful, the implementation of these interfaces in an enterprise with multiple VLANs requires at least two logical units and two IP addresses—you must create units with addresses in each of the subnets associated with the VLANs between which you want traffic to be routed. That is, if you have two
VLANs (for example, VLAN red and VLAN blue) with corresponding subnets, your interfaces must have a logical unit with an address in the subnet for red and a logical unit with an address in the subnet for blue. The switch automatically creates direct routes to these subnets and uses these routes to forward traffic between VLANs.

The interface on the switch detects both MAC addresses and IP addresses, then routes data to other Layer 3 interfaces on routers or other switches. These interfaces detect both IPv4 and IPv6 unicast and multicast virtual routing and forwarding (VRF) traffic. Each logical interface can belong to only one routing instance and is further subdivided into logical interfaces, each with a logical interface number appended as a suffix to the names irb and vlan—for example, irb.10 and vlan.10.

Creating an IRB Interface or RVI

There are four basic steps in creating an IRB interface or RVI as shown in Figure 28 on page 2060.

Figure 28: Creating an IRB Interface or RVI

- Configure VLANs—Virtual LANs are groups of hosts that communicate as if they were attached to the same broadcast stream. VLANs are created with software and do not require a physical router to forward traffic. VLANs are Layer 2 constructs.

- Create IRB interfaces or RVIs for the VLANs—The switch’s IRB interfaces and RVIs use Layer 3 logical interfaces (unlike routers, which can use either physical or logical interfaces).
Assign an IP address to each VLAN—An IRB interface or RVI cannot be activated unless it is associated with a physical interface.

Bind the VLANs to the logical interfaces—There is a one-to-one mapping between a VLAN and an IRB interface or RVI, which means that only one of these interfaces can be mapped to a VLAN.

For specific instructions for creating an IRB interface, see “Configuring Integrated Routing and Bridging Interfaces (CLI Procedure)” on page 2122, and for an RVI, see Configuring Routed VLAN Interfaces (CLI Procedure).

Viewing IRB Interface and RVI Statistics

Some switches automatically track IRB interface and RVI traffic statistics. Other switches allow you to configure tracking. Table 260 on page 2061 illustrates the IRB interface– and RVI-tracking capability on various switches.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Input (ingress)</th>
<th>Output (Egress)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX4300</td>
<td>Automatic</td>
<td>Automatic</td>
</tr>
<tr>
<td>EX3200, EX4200</td>
<td>Automatic</td>
<td>–</td>
</tr>
<tr>
<td>EX8200</td>
<td>Configurable</td>
<td>Automatic</td>
</tr>
<tr>
<td>EX2200, EX3300, EX4500, EX6200</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

You can view input (ingress) and output (egress) totals with the following commands:

- For IRB interfaces, use the `show interfaces irb extensive` command. Look at the input and output values in the Transit Statistics field for IRB interface activity values.
- For RVI, use the `show interfaces vlan extensive` command. Look at the input and output values in the Logical Interface Transit Statistics field for RVI activity values.

IRB Interfaces and RVI Functions and Other Technologies

IRB interfaces and RVIs are similar to switch virtual interfaces (SVIs) and bridge-group virtual interfaces (BVIs), which are supported on other vendors’ devices. They can also be combined with other functions:

- VRF is often used in conjunction with Layer 3 subinterfaces, allowing traffic on a single physical interface to be differentiated and associated with multiple virtual routers. For more information about VRF, see “Understanding Virtual Routing Instances on EX Series Switches” on page 2062.
- For redundancy, you can combine an IRB interface or RVI with implementations of the Virtual Router Redundancy Protocol (VRRP) in both bridging and virtual private LAN service (VPLS) environments. For more information about VRRP, see “Understanding VRRP on EX Series Switches” on page 2220.
Understanding Virtual Routing Instances on EX Series Switches

Virtual routing instances allow administrators to divide a Juniper Networks EX Series Ethernet Switch into multiple independent virtual routers, each with its own routing table. Splitting a device into many virtual routing instances isolates traffic traveling across the network without requiring multiple devices to segment the network.

You can use virtual routing instances to isolate customer traffic on your network and to bind customer-specific instances to customer-owned interfaces.

Virtual routing and forwarding (VRF) is often used in conjunction with Layer 3 subinterfaces, allowing traffic on a single physical interface to be differentiated and associated with multiple virtual routers. Each logical Layer 3 subinterface can belong to only one routing instance.

EX Series switches support IPv4 and IPv6 unicast and multicast VRF traffic. Table 261 on page 2062 provides the number of IPv4 and IPv6 VRFs supported by each EX Series switch.

Table 261: Number of IPv4 and IPv6 VRFs Supported By EX Series Switches

<table>
<thead>
<tr>
<th>Juniper Networks Ethernet Switches</th>
<th>Number of Supported IPv4 VRFs</th>
<th>Number of Supported IPv6 VRFs</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3200 switches</td>
<td>254</td>
<td>252</td>
</tr>
<tr>
<td>EX4200 switches</td>
<td>254</td>
<td>252</td>
</tr>
<tr>
<td>EX4500 switches</td>
<td>254</td>
<td>35</td>
</tr>
<tr>
<td>EX4550 switches</td>
<td>254</td>
<td>35</td>
</tr>
<tr>
<td>EX6200 switches</td>
<td>254</td>
<td>35</td>
</tr>
<tr>
<td>EX8200 switches with non-extra-scale Ethernet line cards installed</td>
<td>254</td>
<td>252</td>
</tr>
<tr>
<td>EX8200 switches with extra-scale Ethernet line cards installed</td>
<td>1000</td>
<td>1000</td>
</tr>
</tbody>
</table>

Related Documentation

- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Understanding Virtual Routing Instances on EX Series Switches
- Example: Using Virtual Routing Instances to Route Among VLANs on EX Series Switches on page 2093
- Configuring Virtual Routing Instances (CLI Procedure) on page 2125
Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches

Multiple VLAN Registration Protocol (MVRP) is a Layer 2 messaging protocol that manages the addition, deletion, and renaming of active virtual LANs, thereby reducing network administrators’ time spent on these tasks. Use MVRP on Juniper Networks EX Series Ethernet Switches to dynamically register and unregister active VLANs on trunk interfaces. Using MVRP means that you do not have to manually register VLANs on all connections—that is, you do not need to explicitly bind a VLAN to each trunk interface. With MVRP, you configure a VLAN on one switch interface and the VLAN configuration is distributed through all active switches in the domain.

MVRP is an application protocol of the Multiple Registration Protocol (MRP) and is defined in the IEEE 802.1ak standard. MRP and MVRP replace Generic Attribute Registration Protocol (GARP) and GARP VLAN Registration Protocol (GVRP) and overcome GARP and GVRP limitations.

This topic describes:

- How MVRP Updates, Creates, and Deletes VLANs on the Switches on page 2063
- MVRP Is Disabled by Default on the Switches on page 2063
- MRP Timers Control MVRP Updates on page 2064
- MVRP Uses MRP Messages to Transmit Switch and VLAN States on page 2064
- Compatibility Issues with Junos OS Releases of MVRP on page 2065

How MVRP Updates, Creates, and Deletes VLANs on the Switches

When any MVRP-member VLAN is changed, that VLAN sends a protocol data unit (PDU) to all other MVRP-member active VLANs. The PDU informs the other VLANs which switches and interfaces currently belong to the sending VLAN. This way, all MVRP-member VLANs are always updated with the current VLAN state of all other MVRP-member VLANs. Timers dictate when PDUs can be sent and when switches receiving MVRP PDUs can update their MVRP VLAN information.

In addition to sending PDU updates, MVRP dynamically creates VLANs on member interfaces when a new VLAN is added to any one interface. This way, VLANs created on one member switch are propagated to other member switches as part of the MVRP message exchange process.

To keep VLAN membership information current, MVRP removes switches and interfaces when they become unavailable. Pruning VLAN information has these benefits:

- Limits the network VLAN configuration to active participants, thereby reducing network overhead.
- Limits broadcast, unknown unicast, and multicast (BUM) traffic to interested devices.

MVRP Is Disabled by Default on the Switches

MVRP is disabled by default on the switches and, when enabled, affects only trunk interfaces. Once you enable MVRP, all VLAN interfaces on the switch belong to MVRP.
(the default normal registration mode) and those interfaces accept PDU messages and send their own PDU messages. To prevent one or more interfaces from participating in MVRP, you can specifically configure an interface to forbidden registration mode instead of the default normal mode.

VLAN updating, dynamic VLAN configuration through MVRP, and VLAN pruning are all active on trunk interfaces when MVRP is enabled.

**MRP Timers Control MVRP Updates**

MVRP registration and updates are controlled by timers that are part of the MRP. The timers define when MVRP PDUs can be sent and when MVRP information can be updated on a switch.

The timers are set on a per-interface basis, and on EX Series switches that use Juniper Networks Junos operating system (Junos OS) with support for the Enhanced Layer 2 Software (ELS) configuration style, the timers are also set on a per-switch basis.

On an EX Series switch that uses Junos OS with support for ELS, if the timer value set on an interface level is different from the value set on a switch level, the value on the interface level takes precedence.

The following MRP timers are used to control the operation of MVRP:

- **Join timer**—Controls the interval for the next MVRP PDU transmit opportunity.
- **Leave timer**—Controls the period of time that an interface on the switch waits in the leave state before changing to the unregistered state.
- **LeaveAll timer**—Controls the frequency with which the interface generates LeaveAll messages.

---

**BEST PRACTICE:** Unless there is a compelling reason to change the timer settings, leave the default settings in place. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.

---

**MVRP Uses MRP Messages to Transmit Switch and VLAN States**

MVRP uses MRP messages to register and declare MVRP states for a switch or VLAN and to inform the switching network that a switch or VLAN is leaving MVRP. These messages are communicated as part of the PDU sent by any switch interface to the other switches in the network.

The following MRP messages are communicated for MVRP:

- **Empty**—MVRP information is not declared and no VLAN is registered.
- **In**—MVRP information is not declared but a VLAN is registered.
- **JoinEmpty**—MVRP information is declared but no VLAN is registered.
- **JoinIn**—MVRP information is declared and a VLAN is registered.
- Leave—MVRP information that was previously declared is withdrawn.
- LeaveAll—Unregister all VLANs on the switch. VLANs must re-register to participate in MVRP.
- New—The MVRP information is new and a VLAN might not be registered yet.

**Compatibility Issues with Junos OS Releases of MVRP**

Except in Junos OS Releases 11.2 and earlier, MVRP has conformed with IEEE standard 802.1ak and IEEE Draft 802.1Q regarding the inclusion of an extra byte in the protocol data units (PDUs) sent and received by MVRP. Table 262 on page 2065 outlines the MVRP versions and whether or not each version includes the extra byte in the PDU. Table 262 on page 2065 also labels each MVRP version with a scenario number, which is used throughout the remainder of this discussion for brevity.

**Table 262: Junos OS MVRP Versions and Inclusion of Extra Byte in PDU**

<table>
<thead>
<tr>
<th>Scenario 1</th>
<th>Scenario 2</th>
<th>Scenario 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVRP in Junos OS Releases 11.2 and Earlier For EX Series Switches That Do Not Support Enhanced Layer 2 Software (ELS) Configuration Style</td>
<td>MVRP in Junos OS Releases 11.3 and Later For EX Series Switches That Do Not Support ELS</td>
<td>MVRP in Junos OS Releases 13.2 and Later For EX Series Switches With Support For ELS</td>
</tr>
<tr>
<td>Includes extra byte in the PDU</td>
<td>By default, does not include extra byte in the PDU</td>
<td>By default, includes extra byte in the PDU</td>
</tr>
</tbody>
</table>

As a result of the non-conformance of Releases 11.2 and earlier and changes in the standards with regard to the extra byte, a compatibility issue exists between some of the Junos OS versions of MVRP. This issue can result in some versions of MVRP not recognizing PDUs without the extra byte.

To address this compatibility issue, the MVRP versions described in scenarios 2 and 3 include the ability to control whether or not the PDU includes the extra byte. Before using these controls, however, you must understand each scenario that applies to your environment and plan carefully so that you do not inadvertently create an additional compatibility issue between the MVRP versions in scenarios 2 and 3.

Table 263 on page 2065 provides a summary of environments that include the various MVRP scenarios and whether or not a particular environment requires you to take action.

**Table 263: MVRP Environments and Description of Required Actions**

<table>
<thead>
<tr>
<th>Environment</th>
<th>Action Required?</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes MVRP versions in scenario 1 only</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Includes MVRP versions in scenario 2 only</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Includes MVRP versions in scenario 3 only</td>
<td>No</td>
<td>—</td>
</tr>
</tbody>
</table>
### Table 263: MVRP Environments and Description of Required Actions (continued)

<table>
<thead>
<tr>
<th>Environment</th>
<th>Action Required?</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Includes MVRP versions in scenarios 1 and 2. MVRP version in scenario 2 is in its default state.</td>
<td>Yes</td>
<td>On switches running MVRP version in scenario 2, use the <code>add-attribute-length-in-pdu</code> statement. For more information, see Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure).</td>
</tr>
<tr>
<td>Includes MVRP versions in scenarios 1 and 3. MVRP version in scenario 3 is in its default state.</td>
<td>No</td>
<td>—</td>
</tr>
<tr>
<td>Includes MVRP versions in scenarios 2 and 3, and both versions are in their respective default states</td>
<td>Yes</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• On switches running MVRP version in scenario 2, use the <code>add-attribute-length-in-pdu</code> statement. For more information, see Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• On switches running MVRP version in scenario 3, use the <code>no-attribute-length-in-pdu</code> statement. For more information, see “Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)” on page 2126.</td>
</tr>
</tbody>
</table>

You can determine whether the switches in your network are running incompatible versions of MVRP by issuing the `show mvrp statistics` command. For more information on diagnosing and correcting this MVRP compatibility situation, see Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) or “Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)” on page 2126.

#### Related Documentation
- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096

### Understanding MAC Address Aging

Juniper Networks EX Series Ethernet Switches store MAC addresses in the Ethernet switching table, also called the MAC table. When the aging time for a MAC address in the table expires, the address is removed.

If your switch runs Juniper Networks Junos operating system (Junos OS) for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can configure the MAC table aging time on all VLANs on the switch. If your switch runs Junos OS that does not support ELS, you can configure the MAC table aging time on all VLANs on the switch or on specified VLANs, as well as configure aging time to be unlimited, either on all VLANs or on specified VLANs, so that MAC addresses never age out of the table.

To learn MAC addresses, the switch reads all packets that it detects on the LAN or on the local VLAN, looking for MAC addresses of sending nodes. It places these addresses
into its Ethernet switching table, along with two other pieces of information—the interface on which the traffic was received and the time when the address was learned.

When the switch receives traffic on an interface, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other interfaces associated with the VLAN. For example, if traffic is received on an interface that is associated with VLAN v-10 and there is no entry in the Ethernet switching table for VLAN v-10 (the Ethernet switching table is organized by VLAN), then the traffic is flooded to all access and trunk interfaces that are members of VLAN v-10.

Flooding allows the switch to learn about destinations that are not yet in its Ethernet switching table. If a particular destination MAC address is not in the Ethernet switching table, the switch floods the traffic to all interfaces except the interface on which it was received. When the destination node receives the flooded traffic, it sends an acknowledgment packet back to the switch, allowing the switch to learn the MAC address of the node and to add the address to its Ethernet switching table.

The switch uses a mechanism called aging to keep the Ethernet switching table current. For each MAC address in the Ethernet switching table, the switch records a timestamp of when the information about the network node was learned. Each time the switch detects traffic from a MAC address that is in its Ethernet switching table, it updates the timestamp of that MAC address. A timer on the switch periodically checks the timestamp, and if the MAC address of a node is older than the value set, the switch removes that MAC address from the Ethernet switching table. This aging process ensures that the switch tracks only active MAC addresses on the network and that it is able to flush out from the Ethernet switching table MAC addresses that are no longer available.

You configure how long MAC addresses remain in the Ethernet switching table by:

- (On switches that run Junos OS with support for the ELS configuration style) Using the `global-mac-table-aging-time` statement in the `[edit protocols l2-learning]` hierarchy.
- (On switches that run Junos OS that does not support ELS) Using the `mac-table-aging-time` statement in either the `[edit ethernet-switching-options]` or the `[edit vlans]` hierarchy, depending on whether you want to configure it for the entire switch or only for specific VLANs.

For example, in a topology with EX switches that run Junos OS that does not support ELS, if you have a printer VLAN, you might choose to configure the aging time for that VLAN to be considerably longer than for other VLANs so that MAC addresses of printers on this VLAN age out less frequently. Because the MAC addresses remain in the table, even if a printer has been idle for some time before traffic arrives for it, the switch still finds the MAC address and does not need to flood the traffic to all other interfaces.

Similarly, in a data center environment where the list of servers connected to the switch is fairly stable, you might choose to increase MAC address aging time, or even set it to unlimited, to increase the efficiency of the utilization of network bandwidth by reducing flooding.
Redundant Trunk Groups

Understanding Redundant Trunk Links on EX Series Switches

In a typical enterprise network composed of distribution and access layers, a redundant trunk link provides a simple solution for network recovery when a trunk port on a Juniper Networks EX Series Ethernet Switch goes down. In that case, traffic is routed to another trunk port, keeping network convergence time to a minimum.

To configure a redundant trunk link, create a redundant trunk group. The redundant trunk group is configured on the access switch and contains two links: a primary or active link, and a secondary link. If the active link fails, the secondary link automatically starts forwarding data traffic without waiting for normal spanning-tree protocol convergence.

NOTE: You can configure a maximum of 16 redundant trunk groups on most standalone switches or on Virtual Chassis. The EX8200 switch and EX8200 Virtual Chassis, however, support up to 254 redundant trunk groups.

Data traffic is forwarded only on the active link. Data traffic on the secondary link is dropped and shown as dropped packets when you issue the operational mode command `show interfaces interface-name extensive`.

While data traffic is blocked on the secondary link, Layer 2 control traffic is still permitted. For example, an LLDP session can be run between two switches on the secondary link.

Rapid Spanning Tree Protocol (RSTP) is enabled by default on EX Series switches to create a loop-free topology, but an interface is not allowed to be in both a redundant trunk group and in a spanning-tree protocol topology at the same time. You must disable RSTP on an interface if a redundant trunk group is configured on that interface. For example, in Figure 29 on page 2069, in addition to disabling RSTP on the Switch 3 interfaces, you must also disable RSTP on the Switch 1 and Switch 2 interfaces connected to Switch 3. Spanning-tree protocols can, however, continue operating on other interfaces on those switches—for example on the link between Switch 1 and Switch 2.

Figure 29 on page 2069 shows three switches in a basic topology for redundant trunk links. Switch 1 and Switch 2 make up the distribution layer, and Switch 3 makes up the access layer. Switch 3 is connected to the distribution layer through trunk ports ge-0/0/9.0 (Link 1) and ge-0/0/10.0 (Link 2). Link 1 and Link 2 are in a redundant trunk group called group1. Link 1 is designated as the primary link. Traffic flows between Switch 3 in the access layer and Switch 1 in the distribution layer through Link 1. While Link 1 is active, Link 2 blocks traffic.
Figure 29: Redundant Trunk Group, Link 1 Active

Figure 30 on page 2069 illustrates how the redundant trunk link topology works when the primary link goes down.

Figure 30: Redundant Trunk Group, Link 2 Active
When Link 1 between Switch 1 and Switch 3 goes down, Link 2 takes over as the active link. Traffic between the access layer and the distribution layer is then automatically switched to Link 2 between Switch 1 and Switch 2.

**Related Documentation**

- *Example: Configuring Redundant Trunk Links for Faster Recovery*
- *Example: Configuring Redundant Trunk Links for Faster Recovery on page 2108*

### Proxy ARP

**Understanding Proxy ARP on EX Series Switches**

You can configure proxy Address Resolution Protocol (ARP) on your Juniper Networks EX Series Ethernet Switch to enable the switch to respond to ARP queries for network addresses by offering its own Ethernet media access control (MAC) address. With proxy ARP enabled, the switch captures and routes traffic to the intended destination.

Proxy ARP is useful in situations where hosts are on different physical networks and you do not want to use subnet masking. Because ARP broadcasts are not propagated between hosts on different physical networks, hosts will not receive a response to their ARP request if the destination is on a different subnet. Enabling the switch to act as an ARP proxy allows the hosts to transparently communicate with each other through the switch. Proxy ARP can help hosts on a subnet reach remote subnets without your having to configure routing or a default gateway.

- *What Is ARP? on page 2070*
- *Proxy ARP Overview on page 2070*
- *Best Practices for Proxy ARP on EX Series Switches on page 2071*

#### What Is ARP?

Ethernet LANs use ARP to map Ethernet MAC addresses to IP addresses. Each device maintains a cache containing a mapping of MAC addresses to IP addresses. The switch maintains this mapping in a cache that it consults when forwarding packets to network devices. If the ARP cache does not contain an entry for the destination device, the host (the DHCP client) broadcasts an ARP request for that device's address and stores the response in the cache.

**Proxy ARP Overview**

When proxy ARP is enabled, if the switch receives an ARP request for which it has a route to the target (destination) IP address, the switch responds by sending a proxy ARP reply packet containing its own MAC address. The host that sent the ARP request then sends its packets to the switch, which forwards them to the intended host.

**NOTE:** For security reasons, the source address in an ARP request must be on the same subnet as the interface on which the ARP request is received.
You can configure proxy ARP for each interface. You can also configure proxy ARP for an integrated routing and bridging (IRB) interface named irb or a routed VLAN interface (RVI) named vlan. (On EX Series switches that use Juniper Networks Junos operating system (Junos OS) with support for the Enhanced Layer 2 Software (ELS) configuration style, the feature is known as an IRB interface. On EX Series switches that use Junos OS that does not support ELS, the feature is known as an RVI.)

EX Series switches support two modes of proxy ARP, restricted and unrestricted. Both modes require that the switch have an active route to the destination address of the ARP request.

- **Restricted**—The switch responds to ARP requests in which the physical networks of the source and target are different and does not respond if the source and target IP addresses are on the same subnet. In this mode, hosts on the same subnet communicate without proxy ARP. We recommend that you use this mode on the switch.

- **Unrestricted**—The switch responds to all ARP requests for which it has a route to the destination. This is the default mode (because it is the default mode in Juniper Networks Junos operating system (Junos OS) configurations other than those on the switch). We recommend using restricted mode on the switch.

### Best Practices for Proxy ARP on EX Series Switches

We recommend these best practices for configuring proxy ARP on the switches:

- Set proxy ARP on the interfaces that you want, including IRB interfaces or RVIs, to restricted mode.
- If you set proxy ARP to unrestricted, disable gratuitous ARP requests on each interface enabled for proxy ARP.

### Related Documentation

- Example: Configuring Proxy ARP on an EX Series Switch on page 2113
- Configuring Proxy ARP (CLI Procedure) on page 2130
EX Series switches use bridging and virtual LANs (VLANs) to connect network devices in a LAN—desktop computers or laptops, IP telephones, printers, file servers, wireless access points, and others—and to segment the LAN into smaller broadcast domains.

This example describes how to configure basic bridging and a VLAN on an EX Series switch:

- Requirements on page 2074
- Overview and Topology on page 2074

Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs Junos OS that does not support ELS, see Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.
Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you set up bridging and a VLAN, be sure you have:

- Installed your EX Series switch. See the installation instructions for your switch.
- Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure).

Overview and Topology

EX Series switches connect network devices in an office LAN or a data center LAN to provide sharing of common resources such as printers and file servers and to enable wireless devices to connect to the LAN through wireless access points. Without bridging and VLANs, all devices on the Ethernet LAN are in a single broadcast domain, and all the devices detect all the packets on the LAN. Bridging creates separate broadcast domains on the LAN, creating VLANs, which are independent logical networks that group together related devices into separate network segments. The grouping of devices on a VLAN is independent of where the devices are physically located in the LAN.

To use an EX Series switch to connect network devices on a LAN, you must, at a minimum, explicitly configure at least one VLAN, even if your network is simple and you want only one broadcast domain to exist, as is the case with this example. You must also assign all needed interfaces to the VLAN, after which the interfaces function in access mode. After the VLAN is configured, you can plug access devices—such as desktop or laptop computers, IP telephones, file servers, printers, and wireless access points—into the switch, and they are joined immediately into the VLAN, and the LAN is up and running.

The topology used in this example consists of one EX4300-24P switch, which has a total of 24 ports. All ports support Power over Ethernet (PoE), which means they provide both network connectivity and electric power for the device connecting to the port. To these ports, you can plug in devices requiring PoE, such as Avaya VoIP telephones, wireless access points, and some IP cameras. (Avaya phones have a built-in hub that allows you to connect a desktop PC to the phone, so the desktop and phone in a single office require only one port on the switch.) Table 264 on page 2075 details the topology used in this configuration example.
### Table 264: Components of the Basic Bridging Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX4300-24P switch, with 24 Gigabit Ethernet ports: in this example, 8 ports are used as PoE ports (ge-0/0/0 through ge-0/0/7) and 16 ports used as non-PoE ports (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>employee-vlan</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>10</td>
</tr>
<tr>
<td>Connection to wireless access point (requires PoE)</td>
<td>ge-0/0/0</td>
</tr>
<tr>
<td>Connections to Avaya IP telephone—with integrated hub, to connect phone and desktop PC to a single port (requires PoE)</td>
<td>ge-0/0/1 through ge-0/0/7</td>
</tr>
<tr>
<td>Direct connections to desktop PCs and laptops (no PoE required)</td>
<td>ge-0/0/8 through ge-0/0/12</td>
</tr>
<tr>
<td>Connections to file servers (no PoE required)</td>
<td>ge-0/0/17 and ge-0/0/18</td>
</tr>
<tr>
<td>Connections to integrated printer/fax/copier machines (no PoE required)</td>
<td>ge-0/0/19 through ge-0/0/20</td>
</tr>
<tr>
<td>Unused ports (for future expansion)</td>
<td>ge-0/0/13 through ge-0/0/16, and ge-0/0/21 through ge-0/0/23</td>
</tr>
</tbody>
</table>

### Configuration

**To set up basic bridging and a VLAN:**

**CLI Quick Configuration**

To quickly configure a VLAN, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set vlans employee-vlan vlan-id 10
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/4 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/5 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/6 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/7 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/8 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/12 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/15 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/16 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/17 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/18 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/19 unit 0 family ethernet-switching vlan members employee-vlan
set interfaces ge-0/0/20 unit 0 family ethernet-switching vlan members employee-vlan
```
You must then plug the wireless access point into PoE-enabled port `ge-0/0/0` and the Avaya IP phones into the PoE-enabled ports `ge-0/0/1` through `ge-0/0/7`. Also, plug the PCs, file servers, and printers into ports `ge-0/0/8` through `ge-0/0/12` and `ge-0/0/17` through `ge-0/0/20`.

### Step-by-Step Procedure

To set up basic bridging and a VLAN:

1. Create a VLAN named `employee-vlan` and specify the VLAN ID of 10 for it:
   ```
   [edit vlans]
   user@switch# set employee-vlan vlan-id 10
   ```

2. Assign interfaces `ge-0/0/0` through `ge-0/0/12`, and `ge-0/0/17` through `ge-0/0/20` to the `employee-vlan` VLAN:
   ```
   [edit interface]
   user@switch# set ge-0/0/0/0 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/1 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/2 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/3 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/4 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/5 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/6 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/7 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/8 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/9 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/10 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/11 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/12 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/17 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/18 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/19 unit 0 family ethernet-switching vlan members employee-vlan
   user@switch# set ge-0/0/0/20 unit 0 family ethernet-switching vlan members employee-vlan
   ```

3. Connect the wireless access point to switch port `ge-0/0/0`.

4. Connect the seven Avaya phones to switch ports `ge-0/0/1` through `ge-0/0/7`.

5. Connect the five PCs to ports `ge-0/0/8` through `ge-0/0/12`.

6. Connect the two file servers to ports `ge-0/0/17` and `ge-0/0/18`.

7. Connect the two printers to ports `ge-0/0/19` and `ge-0/0/20`. 
Results

Check the results of the configuration:

```plaintext
user@switch> show configuration
ge-0/0/0 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/3 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/4 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/5 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/6 {
    unit 0 {
        family ethernet-switching {
```
vlan {
    members employee-vlan;
}

ge-0/0/7 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/8 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/9 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/10 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/11 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
ge-0/0/12 {
    unit 0 {
        family ethernet-switching {
            vlan {
                members employee-vlan;
            }
        }
    }
}
Verification

To verify that switching is operational and that employee-vlan has been created, perform these tasks:

- Verifying That the VLAN Has Been Created on page 2079
- Verifying That Interfaces Are Associated with the Proper VLANs on page 2080

Verifying That the VLAN Has Been Created

Purpose

Verify that the VLAN named employee-vlan has been created on the switch.
**Action**  
List all VLANs configured on the switch:

<table>
<thead>
<tr>
<th>Routing instance</th>
<th>VLAN name</th>
<th>Tag</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-switch</td>
<td>employee-vlan</td>
<td>10</td>
<td>ge-0/0/0.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/3.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/4.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/5.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/6.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/7.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/8.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/9.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/10.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/11.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/12.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/17.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/18.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/19.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ge-0/0/20.0</td>
</tr>
</tbody>
</table>

...  

**Meaning**  
The `show vlans` command lists the VLANs configured on the switch. This output shows that the VLAN `employee-vlan` has been created.

**Verifying That Interfaces Are Associated with the Proper VLANs**

**Purpose**  
Verify that Ethernet switching is enabled on switch interfaces and that all interfaces are included in the VLAN.
Action

List all interfaces on which switching is enabled:

```
user@switch> show ethernet-switching interfaces
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                        LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/0.0                    65535                                 untagged  
        employee-vlan 10           65535          Discarding
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                        LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/1.0                    65535                                 untagged  
        employee-vlan 10           65535          Discarding
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                        LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/2.0                    65535                                 untagged  
        employee-vlan 10           65535          Discarding
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                        LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/3.0                    65535                                 untagged  
        employee-vlan 10           65535          Discarding
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                        LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/4.0                    65535                                 untagged  
        employee-vlan 10           65535          Discarding
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                        LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/5.0                    65535                                 untagged  
        employee-vlan 10           65535          Discarding
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                        LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/6.0                    65535                                 untagged  
        employee-vlan 10           65535          Discarding
Routing Instance Name : default-switch
```
<table>
<thead>
<tr>
<th>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/7.0</td>
</tr>
<tr>
<td>Routing Instance Name: default-switch</td>
</tr>
<tr>
<td>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</td>
</tr>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/8.0</td>
</tr>
<tr>
<td>Routing Instance Name: default-switch</td>
</tr>
<tr>
<td>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</td>
</tr>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/9.0</td>
</tr>
<tr>
<td>Routing Instance Name: default-switch</td>
</tr>
<tr>
<td>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</td>
</tr>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
</tr>
<tr>
<td>Routing Instance Name: default-switch</td>
</tr>
<tr>
<td>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</td>
</tr>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
</tr>
<tr>
<td>Routing Instance Name: default-switch</td>
</tr>
<tr>
<td>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</td>
</tr>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/12.0</td>
</tr>
<tr>
<td>Routing Instance Name: default-switch</td>
</tr>
<tr>
<td>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</td>
</tr>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/17.0</td>
</tr>
<tr>
<td>Routing Instance Name: default-switch</td>
</tr>
<tr>
<td>Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down)</td>
</tr>
<tr>
<td>Logical interface members</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
</tr>
</tbody>
</table>
Meaning

The `show ethernet-switching interfaces` command lists all interfaces on which switching is enabled (in the Logical interface column), along with the VLANs that are active on the interfaces (in the VLAN members column). The output in this example shows all the connected interfaces, ge-0/0/0 through ge-0/0/12 and ge-0/0/17 through ge-0/0/20 and that they are all part of VLAN `employee-vlan`. Notice that the interfaces listed are the logical interfaces, not the physical interfaces. For example, the output shows ge-0/0/0.0 instead of ge-0/0/0. This is because Junos OS creates VLANs on logical interfaces, not directly on physical interfaces.

Related Documentation

- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
- Example: Connecting Access Switches to a Distribution Switch on page 2083
- Understanding Bridging and VLANs on EX Series Switches on page 2049

Example: Connecting Access Switches to a Distribution Switch

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Connecting an Access Switch to a Distribution Switch. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

In large local area networks (LANs), you commonly need to aggregate traffic from a number of access switches into a distribution switch.

This example describes how to connect access switches to a distribution switch:

- Requirements on page 2084
- Overview and Topology on page 2084
- Configuring the Access Switch on page 2086
• Configuring the Distribution Switch on page 2090
• Verification on page 2092

Requirements

This example uses the following hardware and software components:

• Three EX Series access switches.
• One EX Series distribution switch.

NOTE: In an access switch-distribution switch topology, you can connect EX Series switches that run a version of Junos OS that supports ELS with EX Series switches that do not run a version of Junos OS that supports ELS. However, this example uses switches running ELS only to show how to configure this topology using the ELS CLI.

• Junos OS Release 12.3R2 or later that supports ELS for EX Series switches.

Before you connect an access switch to a distribution switch, be sure you have:

• Installed the switches. See the installation instructions for your switch.

• Performed the initial software configuration on both switches. For information about the initial software configuration for all EX Series switches except the EX9200 Series switches, see Connecting and Configuring an EX Series Switch (CLI Procedure). For information about the initial software configuration for the EX9200 Series switches, see Connecting and Configuring an EX9200 Switch (CLI Procedure).

Overview and Topology

In a large office that is spread across several floors or buildings, or in a data center, you commonly aggregate traffic from a number of access switches into a distribution switch. This configuration example shows a simple topology to illustrate how to connect three access switches to a distribution switch.

In the topology, the LAN is segmented into two VLANs, one for the sales department and the second for the support team. One 1-Gigabit Ethernet port on one of the access switch’s uplink modules connects to the distribution switch, to one 1-Gigabit Ethernet port on the distribution switch.

Figure 31 on page 2085 shows an EX9200 distribution switch that is connected to three EX4300 access switches.
Table 265 on page 2085 describes the components of the example topology. The example shows how to configure one of the three access switches. The other access switches could be configured in the same manner.

Table 265: Components of the Topology for Connecting an Access Switch to a Distribution Switch

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access switch hardware</td>
<td>Three EX4300 switches, each with an uplink module with 1-Gigabit Ethernet ports.</td>
</tr>
<tr>
<td>Distribution switch hardware</td>
<td>One EX9208 with up to three EX9200-40T line cards installed, which at full duplex, can provide up to 240 1-Gigabit ports.</td>
</tr>
<tr>
<td>VLAN names and tag IDs</td>
<td>sales, tag 100&lt;br&gt;support, tag 200</td>
</tr>
<tr>
<td>VLAN subnets</td>
<td>sales: 192.0.2.0/25 (addresses 192.0.2.1 through 192.0.2.126)&lt;br&gt;support: 192.0.2.128/25 (addresses 192.0.2.129 through 192.0.2.254)</td>
</tr>
<tr>
<td>Trunk port interfaces</td>
<td>On the access switch: ge-0/2/0&lt;br&gt;On the distribution switch: ge-0/0/0</td>
</tr>
<tr>
<td>Access port interfaces in VLAN sales (on access switch)</td>
<td>Avaya IP telephones: ge-0/0/3 through ge-0/0/19&lt;br&gt;Wireless access points: ge-0/0/0 and ge-0/0/1&lt;br&gt;Printers: ge-0/0/22 and ge-0/0/23&lt;br&gt;File servers: ge-0/0/20 and ge-0/0/21</td>
</tr>
</tbody>
</table>
Table 265: Components of the Topology for Connecting an Access Switch to a Distribution Switch (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
</table>
| Access port interfaces in VLAN support (on access switch) | Avaya IP telephones: ge-0/0/25 through ge-0/0/43  
Wireless access points: ge-0/0/24  
Printers: ge-0/0/44 and ge-0/0/45  
File servers: ge-0/0/46 and ge-0/0/47 |

**Configuring the Access Switch**

To configure the access switch:

**CLI Quick Configuration**

To quickly configure the access switch, copy the following commands and paste them into the switch terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 description "Sales wireless access point port"
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/0 unit 0 family network-switching vlan members sales
set interfaces ge-0/0/3 unit 0 description "Sales phone port"
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/22 unit 0 description "Sales printer port"
set interfaces ge-0/0/22 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/20 unit 0 description "Sales file server port"
set interfaces ge-0/0/20 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/26 unit 0 description "Support wireless access point port"
set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/24 unit 0 description "Support phone port"
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/26 unit 0 description "Support printer port"
set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/44 unit 0 description "Support file server port"
set interfaces ge-0/0/44 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/0/46 unit 0 description "Support file server port"
set interfaces ge-0/0/46 unit 0 family ethernet-switching vlan members sales
set interfaces ge-0/2/0 unit 0 description "Uplink module port connection to distribution switch"
set interfaces ge-0/2/0 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/2/0/0 native-vlan-id 1
set interfaces ge-0/2/0 unit 0 family ethernet-switching vlan members [sales support]
set interfaces ge-0/2/0 unit 0 family ethernet-switching vlan members sales
set interfaces irb unit 0 family inet address 192.0.2.1/25
set interfaces irb unit 1 family inet address 192.0.2.129/25
set vlans sales description "Sales VLAN"
set vlans sales i3-interface irb.0
set vlans sales vlan-id 100
set vlans support description "Support VLAN"
set vlans support vlan-id 200
set vlans support i3-interface irb.1
```

**Step-by-Step Procedure**

To configure the access switch:

1. Configure the 1-Gigabit Ethernet interface on the uplink module to be the trunk port that connects to the distribution switch:

   ```
   [edit interfaces]
   user@access-switch# set ge-0/2/0 unit 0 description "Uplink module port connection to distribution switch"
   user@access-switch# set ge-0/2/0 unit 0 family ethernet-switching interface-mode trunk
   ```

2. Specify the VLANs to be aggregated on the trunk port:
3. To handle untagged packets that are received on the trunk port, create a native VLAN by configuring a VLAN ID and specifying that the trunk port is a member of the native VLAN:

```
[edit interfaces]
user@access-switch# set ge-0/2/0 unit 0 family ethernet-switching vlan members
```

4. Configure the sales VLAN:

```
[edit vlans]
user@access-switch# set sales description "Sales VLAN"
user@access-switch# set sales vlan-id 100
user@access-switch# set sales l3-interface irb.0
```

5. Configure the support VLAN:

```
[edit vlans]
user@access-switch# set support description "Support VLAN"
user@access-switch# set support vlan-id 200
user@access-switch# set support l3-interface irb.1
```

6. Create the subnet for the sales VLAN:

```
[edit interfaces]
user@access-switch# set irb unit 0 family inet address 192.0.2.1/25
```

7. Create the subnet for the support VLAN:

```
[edit interfaces]
user@access-switch# set irb unit 1 family inet address 192.0.2.129/25
```

8. Configure the interfaces in the sales VLAN:

```
[edit interfaces]
user@access-switch# set ge-0/0/0 unit 0 description "Sales wireless access point port"
user@access-switch# set ge-0/0/0 unit 0 family ethernet-switching vlan members sales
user@access-switch# set ge-0/0/3 unit 0 description "Sales phone port"
user@access-switch# set ge-0/0/3 unit 0 family ethernet-switching vlan members sales
user@access-switch# set ge-0/0/20 unit 0 description "Sales file server port"
user@access-switch# set ge-0/0/20 unit 0 family ethernet-switching vlan members sales
user@access-switch# set ge-0/0/22 unit 0 description "Sales printer port"
user@access-switch# set ge-0/0/22 unit 0 family ethernet-switching vlan members sales
user@access-switch# set ge-0/0/24 unit 0 description "Support wireless access point port"
user@access-switch# set ge-0/0/24 unit 0 family ethernet-switching vlan members support
user@access-switch# set ge-0/0/26 unit 0 description "Support phone port"
user@access-switch# set ge-0/0/26 unit 0 family ethernet-switching vlan members support
user@access-switch# set ge-0/0/44 unit 0 description "Support printer port"
user@access-switch# set ge-0/0/44 unit 0 family ethernet-switching vlan members support
user@access-switch# set ge-0/0/46 unit 0 description "Support file server port"
user@access-switch# set ge-0/0/46 unit 0 family ethernet-switching vlan members support
```
Results  Display the results of the configuration:

    user@access-switch> show configuration
    interfaces {
      ge-0/0/0 {
        unit 0 {
          description "Sales wireless access point port";
          family ethernet-switching {
            vlan {
              members sales;
            }  
          }
        }
      }  
      ge-0/0/3 {
        unit 0 {
          description "Sales phone port";
          family ethernet-switching {
            vlan {
              members sales;
            }  
          }
        }
      }  
      ge-0/0/20 {
        unit 0 {
          description "Sales file server port";
          family ethernet-switching {
            vlan {
              members sales;
            }  
          }
        }
      }  
      ge-0/0/22 {
        unit 0 {
          description "Sales printer port";
          family ethernet-switching {
            vlan {
              members sales;
            }  
          }
        }
      }  
      ge-0/0/24 {
        unit 0 {
          description "Support wireless access point port";
          family ethernet-switching {
            vlan {
              members support;
            }  
          }
        }
      }  
      ge-0/0/26 {
        unit 0 {
          description "Support phone port";
          family ethernet-switching {
            vlan {
              members support;
            }  
          }
        }
      }
ge-0/0/44 { 
    unit 0 { 
        description "Support printer port";
        family ethernet-switching { 
            vlan { 
                members support;
            } 
        } 
    } 
} 

ge-0/0/46 { 
    unit 0 { 
        description "Support file server port";
        family ethernet-switching { 
            vlan { 
                members support;
            } 
        } 
    } 
} 

ge-0/2/0 { 
    native-vlan-id 1;
    unit 0 { 
        description "Uplinking module connection to distribution switch";
        family ethernet-switching { 
            interface-mode trunk;
            vlan { 
                members [ 1 sales support ];
            } 
        } 
    } 
    irb { 
        unit 0 { 
            family inet { 
                address 192.0.2.1/25;
            } 
        } 
        unit 1 { 
            family inet { 
                address 192.0.2.129/25;
            } 
        } 
    } 
} 

vlans { 
    sales { 
        description "Sales VLAN";
        vlan-id 100;
        l3-interface irb.0;
    } 
    support { 
        description "Support VLAN";
        vlan-id 200;
        l3-interface irb.1;
    } 
}
TIP: To quickly configure the access switch, issue the load merge terminal command, then copy the hierarchy and paste it into the switch terminal window.

Configuring the Distribution Switch

To configure the distribution switch:

**CLI Quick Configuration**

To quickly configure the distribution switch, copy the following commands and paste them into the switch terminal window:

- `set interfaces ge-0/0/0 unit 0 description "Connection to access switch"`
- `set interfaces ge-0/0/0 unit 0 family ethernet-switching interface-mode trunk`
- `set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members [sales support]`
- `set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members 1`
- `set interfaces irb unit 0 family inet address 192.0.2.2/25`
- `set interfaces irb unit 1 family inet address 192.0.2.130/25`
- `set vlans sales description "Sales VLAN"`
- `set vlans sales vlan-id 100`
- `set vlans sales l3-interface irb.0`
- `set vlans support description "Support VLAN"`
- `set vlans support vlan-id 200`
- `set vlans support l3-interface irb.1`

**Step-by-Step Procedure**

To configure the distribution switch:

1. Configure the interface on the switch to be the trunk port that connects to the access switch:

   ```
   [edit interfaces]
   user@distribution-switch# set ge-0/0/0 unit 0 description "Connection to access switch"
   user@distribution-switch# set ge-0/0/0 unit 0 family ethernet-switching interface-mode trunk
   ```

2. Specify the VLANs to be aggregated on the trunk port:

   ```
   [edit interfaces]
   user@distribution-switch# set ge-0/0/0 unit 0 family ethernet-switching vlan members [sales support]
   ```

3. To handle untagged packets that are received on the trunk port, create a native VLAN by configuring a VLAN ID and specifying that the trunk port is a member of the native VLAN:

   ```
   [edit interfaces]
   user@distribution-switch# set ge-0/0/0 native-vlan-id 1
   user@distribution-switch# set ge-0/0/0 unit 0 family ethernet-switching vlan members 1
   ```

4. Configure the sales VLAN:

   ```
   [edit vlans]
   user@distribution-switch# set sales description "Sales VLAN"
   user@distribution-switch# set sales vlan-id 100
   user@distribution-switch# set sales l3-interface irb.0
   ```
The VLAN configuration for the distribution switch includes the `set l3-interface irb.0` command to route traffic between the sales and support VLANs. The VLAN configuration for the access switch does not include this statement because the access switch is not monitoring IP addresses. Instead, the access switch is passing the IP addresses to the distribution switch for interpretation.

5. Configure the support VLAN:

```
[edit vlans]
user@distribution-switch# set support description "Support VLAN"
user@distribution-switch# set support vlan-id 200
user@distribution-switch# set support l3-interface irb.1
```

The VLAN configuration for the distribution switch includes the `set l3-interface irb.1` command to route traffic between the sales and support VLANs. The VLAN configuration for the access switch does not include this statement because the access switch is not monitoring IP addresses. Instead, the access switch is passing the IP addresses to the distribution switch for interpretation.

6. Create the subnet for the sales VLAN:

```
[edit interfaces]
user@distribution-switch# set irb unit 0 family inet address 192.0.2.2/25
```

7. Create the subnet for the support VLAN:

```
[edit interfaces]
user@distribution-switch# set irb unit 1 family inet address 192.0.2.130/25
```
Results Display the results of the configuration:

user@distribution-switch> show configuration
interfaces {
  ge-0/0/0 {
    native-vlan-id 1;
    unit 0 {
      description "Connection to access switch";
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members [ 1 sales support ];
        }
      }
    }
  }
  irb {
    unit 0 {
      family inet {
        address 192.0.2.2/25;
      }
    }
    unit 1 {
      family inet {
        address 192.0.2.130/25;
      }
    }
  }
}
vlans {
  sales {
    description "Sales VLAN";
    vlan-id 100;
    l3-interface irb.0;
  }
  support {
    description "Support VLAN";
    vlan-id 200;
    l3-interface irb.1;
  }
}

TIP: To quickly configure the distribution switch, issue the load merge terminal command, then copy the hierarchy and paste it into the switch terminal window.

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying the VLAN Members and Interfaces on the Access Switch on page 2093
- Verifying the VLAN Members and Interfaces on the Distribution Switch on page 2093
Verifying the VLAN Members and Interfaces on the Access Switch

**Purpose**
Verify that the sales and support VLANs have been created on the switch.

**Action**
List all VLANs configured on the switch:

```
user@access-switch> show vlans
Routing instance  VLAN name  Tag  Interfaces
default-switch  sales       100  ge-0/0/20.0
                ge-0/0/22.0
                ge-0/0/3.0*
                ge-0/0/0.0*
                ge-0/2/0.0*

default-switch  support     200  ge-0/0/24.0
                ge-0/0/26.0
                ge-0/0/44.0*
                ge-0/0/46.0*
                ge-0/2/0.0*
```

**Meaning**
The output shows the sales and support VLANs and the interfaces that are configured as members of the respective VLANs.

Verifying the VLAN Members and Interfaces on the Distribution Switch

**Purpose**
Verify that the sales and support VLANs have been created on the switch.

**Action**
List all VLANs configured on the switch:

```
user@distribution-switch> show vlans
Routing instance  VLAN name  Tag  Interfaces
default-switch  sales       100  ge-0/0/0.0*

default-switch  support     200  ge-0/0/0.0*
```

**Meaning**
The output shows the sales and support VLANs and the interface (ge-0/0/0.0) that is configured as a member of both VLANs. Interface ge-0/0/0.0 is also the trunk interface connected to the access switch.

**Related Documentation**
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Example: Using Virtual Routing Instances to Route Among VLANs on EX Series Switches

Virtual routing instances allow each EX Series switch to have multiple routing tables on a device. With virtual routing instances, you can segment your network to isolate traffic without setting up additional devices.
This example describes how to create virtual routing instances:

- Requirements on page 2094
- Overview and Topology on page 2094
- Configuration on page 2094
- Verification on page 2096

Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 9.2 or later for EX Series switches

Before you create the virtual routing instances, make sure you have:

- Configured the necessary VLANs. See Configuring VLANs for EX Series Switches (CLI Procedure), “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119, or “Configuring VLANs for EX Series Switches (J-Web Procedure)” on page 2117.

Overview and Topology

In a large office, you may need multiple VLANs to properly manage your traffic. This configuration example shows a simple topology to illustrate how to connect a single EX Series switch with a virtual routing instance for each of two VLANs, enabling traffic to pass between those VLANs.

In the example topology, the LAN is segmented into two VLANs, each associated with an interface and a routing instance on the EX Series switch.

Configuration

CLI Quick Configuration

To quickly create and configure virtual routing instances, copy the following commands and paste them into the switch terminal window:

```
[edit]
set interfaces ge-0/0/3 vlan-tagging
set interfaces ge-0/0/3 unit 0 vlan-id 1030 family inet address 103.1.1.1/24
set interfaces ge-0/0/3 unit 1 vlan-id 1031 family inet address 103.1.1.1/24
set routing-instances r1 instance-type virtual-router
set routing-instances r1 interface ge-0/0/1.0
set routing-instances r1 interface ge-0/0/3.0
set routing-instances r2 instance-type virtual-router
set routing-instances r2 interface ge-0/0/2.0
set routing-instances r2 interface ge-0/0/3.1
```

Step-by-Step Procedure

To configure virtual routing instances:

1. Create a VLAN-tagged interface:
   ```
   [edit]user@switch# set interfaces ge-0/0/3 vlan-tagging
   ```

2. Create two subinterfaces, on the interface, one for each routing instance:
   ```
   [edit]user@switch# set interfaces ge-0/0/3 unit 0 vlan-id 1030 family inet address 103.1.1.1/24
   ```
user@switch# set interfaces ge-0/0/3 unit 1 vlan-id 1031 family inet address 103.1.1.1/24

3. Create two virtual routers:
   [edit]user@switch# set routing-instances r1 instance-type virtual-router
   user@switch# set routing-instances r2 instance-type virtual-router

4. Set the interfaces for the virtual routers:
   [edit]user@switch# set routing-instances r1 interface ge-0/0/1.0
   user@switch# set routing-instances r1 interface ge-0/0/3.0
   user@switch# set routing-instances r2 interface ge-0/0/2.0
   user@switch# set routing-instances r2 interface ge-0/0/3.1

Results Check the results of the configuration:

user@switch> show configuration
interfaces {
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/2 {
        unit 0 {
            family ethernet-switching;
        }
    }
    ge-0/0/3 {
        vlan-tagging;
        unit 0 {
            vlan-id 1030;
            family inet {
                address 103.1.1.1/24;
            }
        }
        unit 1 {
            vlan-id 1031;
            family inet {
                address 103.1.1.1/24;
            }
        }
    }
}

routing-instances {
    r1 {
        instance-type virtual-router;
        interface ge-0/0/1.0;
        interface ge-0/0/3.0;
    }
    r2 {
        instance-type virtual-router;
        interface ge-0/0/2.0;
        interface ge-0/0/3.1;
    }
}
Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Routing Instances Were Created on page 2096

**Verifying That the Routing Instances Were Created**

**Purpose**  
Verify that the virtual routing instances were properly created on the switch.

**Action**  
Use the `show route instance` command:

```
user@switch> show route instance

Instance       Type
master         Primary RIB forwarding Active/holddown/hidden
               inet.0            3/0/0
r1             virtual-router
               r1.inet.0        1/0/0
r2             virtual-router
               r2.inet.0        1/0/0
```

**Meaning**  
Each routing instance created is displayed, along with its type, information about whether it is active or not, and its primary routing table.

**Related Documentation**  
- Configuring Virtual Routing Instances (CLI Procedure) on page 2125

---

**Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches**

**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

As a network expands and the number of clients and VLANs increases, VLAN administration becomes complex and the task of efficiently configuring VLANs on multiple EX Series switches becomes increasingly difficult. However, you can automate VLAN administration by enabling Multiple VLAN Registration Protocol (MVRP) on the network. MVRP also dynamically creates VLANs, further simplifying the network overhead required to statically configure VLANs.

**NOTE:** Only trunk interfaces can be enabled for MVRP.
This example describes how to use MVRP to automate administration of VLAN membership changes within your network and how to use MVRP to dynamically create VLANs:

- Requirements on page 2097
- Overview and Topology on page 2097
- Configuring VLANs and MVRP on Access Switch A on page 2099
- Configuring VLANs and MVRP on Access Switch B on page 2101
- Configuring VLANs and MVRP on Distribution Switch C on page 2103
- Verification on page 2104

Requirements

This example uses the following hardware and software components:

- Two EX Series access switches
- One EX Series distribution switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you configure MVRP on an interface, you must enable one of the following spanning tree protocols on that interface:

- Rapid Spanning-Tree Protocol (RSTP). For more information about RSTP, see “Understanding RSTP for EX Series Switches” on page 4300.
- Multiple Spanning-Tree Protocol (MSTP). For more information about MSTP, see “Understanding MSTP for EX Series Switches” on page 4298.

Overview and Topology

MVRP is used to manage dynamic VLAN registration in a LAN. It can also be used to dynamically create VLANs.

This example uses MVRP to dynamically create VLANs on the switching network. Alternatively, you can disable dynamic VLAN creation and create VLANs statically. Enabling MVRP on the trunk interface of each switch in your switching network ensures that the active VLAN information for the switches in the network is propagated to each switch through the trunk interfaces, assuming dynamic VLAN creation is enabled for MVRP.

MVRP ensures that the VLAN membership information on the trunk interface is updated as the switch’s access interfaces become active or inactive in the configured VLANs in a static or dynamic VLAN creation setup.

You do not need to explicitly bind a VLAN to the trunk interface. When MVRP is enabled, the trunk interface advertises all the VLANs that are active (bound to access interfaces) on that switch. An MVRP-enabled trunk interface does not advertise VLANs that are configured on the switch but are not currently bound to an access interface. Thus, MVRP provides the benefit of reducing network overhead—by limiting the scope of broadcast, unknown unicast, and multicast (BUM) traffic to interested devices only.
When VLAN access interfaces become active or inactive, MVRP ensures that the updated information is advertised on the trunk interface. Thus, in this example, distribution Switch C does not forward traffic to inactive VLANs.

**NOTE:** This example shows a network with three VLANs: finance, sales, and lab. All three VLANs are running the same version of Junos OS. If switches in this network were running a mix of Junos OS releases that included Release 11.3, additional configuration would be necessary—see Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) for details.

Figure 32 on page 2098 shows MVRP configured on two access switches and one distribution switch.

Figure 32: MVRP Configured on Two Access Switches and One Distribution Switch for Automatic VLAN Administration

Table 266 on page 2098 explains the components of the example topology.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>• Access Switch A</td>
</tr>
<tr>
<td></td>
<td>• Access Switch B</td>
</tr>
<tr>
<td></td>
<td>• Distribution Switch C</td>
</tr>
</tbody>
</table>
Table 266: Components of the Network Topology *(continued)*

<table>
<thead>
<tr>
<th>Settings</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN names and tag IDs</td>
<td>finance, tag 100</td>
</tr>
<tr>
<td></td>
<td>lab, tag 200</td>
</tr>
<tr>
<td></td>
<td>sales, tag 300</td>
</tr>
</tbody>
</table>

Interfaces

Access Switch A interfaces:

- **ge-0/0/1**—Connects PC1 to access Switch A.
- **ge-0/0/2**—Connects PC2 to access Switch A.
- **ge-0/0/3**—Connects PC3 to access Switch A.
- **xe-0/1/1**—Connects access Switch A to distribution Switch C (trunk).

Access Switch B interfaces:

- **ge-0/0/0**—Connects PC4 to access Switch B.
- **ge-0/0/1**—Connects PC5 to access Switch B.
- **ge-0/0/2**—Reserved for future use,
- **xe-0/1/0**—Connects access Switch B to distribution Switch C. (trunk)

Distribution Switch C interfaces:

- **xe-0/1/1**—Connects distribution Switch C to access Switch A. (trunk)
- **xe-0/1/0**—Connects distribution Switch C to access Switch B. (trunk)

**Configuring VLANs and MVRP on Access Switch A**

To configure VLANs on the switch, bind access interfaces to the VLANs, and enable MVRP on the trunk interface of access Switch A, perform these tasks:

**CLI Quick Configuration**

To quickly configure access Switch A for MVRP, copy the following commands and paste them into the switch terminal window of Switch A:

```
[edit]
sedit vlans finance vlan-id 100
set vlans lab vlan-id 200
set vlans sales vlan-id 300
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members finance
set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members lab
set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members sales
set interfaces xe-0/1/1 unit 0 family ethernet-switching interface-mode trunk
set protocols mvrp interface xe-0/1/1
```
NOTE: This example uses default MVRP timers. The default values associated with each MVRP timer are: 200 ms for the join timer, 1000 ms for the leave timer, and 10000 ms (10 seconds) for the leaveall timer. We recommend retaining the use of default timer values as modifying timers to inappropriate values might cause an imbalance in the operation of MVRP. However, if you choose to change the default settings, keep in mind that on an EX Series switch that uses Junos OS with support for ELS, if the timer value set on an interface level is different from the value set on a switch level, then the value on the interface level takes precedence.

Step-by-Step Procedure

To configure access Switch A for MVRP:

1. Configure the finance VLAN:
   ```
   [edit]
   user@Access-Switch-A# set vlans finance vlan-id 100
   ```

2. Configure the lab VLAN:
   ```
   [edit]
   user@Access-Switch-A# set vlans lab vlan-id 200
   ```

3. Configure the sales VLAN:
   ```
   [edit]
   user@Access-Switch-A# set vlans sales vlan-id 300
   ```

4. Configure an Ethernet interface as a member of the finance VLAN:
   ```
   [edit]
   user@Access-Switch-A# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members finance
   ```

5. Configure an Ethernet interface as a member of the lab VLAN:
   ```
   [edit]
   user@Access-Switch-A# set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members lab
   ```

6. Configure an Ethernet interface as a member of the sales VLAN:
   ```
   [edit]
   user@Access-Switch-A# set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members sales
   ```

7. Configure a trunk interface:
   ```
   [edit]
   user@Access-Switch-A# set interfaces xe-0/1/1 unit 0 family ethernet-switching interface-mode trunk
   ```

8. Enable MVRP on the trunk interface:
   ```
   [edit]
   user@Access-Switch-A# set protocols mvrp interface xe-0/1/1
   ```

Results

Check the results of the configuration on Switch A:

```
[edit]
user@Access-Switch-A# show interfaces {
  ge-0/0/1 {
```
unit 0 [
  family ethernet-switching [
    vlan [
      members finance;
    ]
  ]
]

ge-0/0/2 [
  unit 0 [
    family ethernet-switching [
      vlan [
        members lab;
      ]
    ]
  ]
]

ge-0/0/3 [
  unit 0 [
    family ethernet-switching [
      vlan [
        members sales;
      ]
    ]
  ]
]

xe-0/1/1 [
  unit 0 [
    family ethernet-switching [
      interface-mode trunk;
    ]
  ]
]

protocols [
  mvrp [
    interface xe-0/1/1;
  ]
]

vlans [
  finance [
    vlan-id 100;
  ]
  lab [
    vlan-id 200;
  ]
  sales [
    vlan-id 300;
  ]
]

Configuring VLANs and MVRP on Access Switch B

To configure three VLANs on the switch, bind access interfaces for PC4 and PC5 to the VLANs, and enable MVRP on the trunk interface of access Switch B, perform these tasks:
CLI Quick Configuration

To quickly configure Access Switch B for MVRP, copy the following commands and paste them into the switch terminal window of Switch B:

```
[edit]
set vlans finance vlan-id 100
set vlans lab vlan-id 200
set vlans sales vlan-id 300
set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members finance
set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members lab
set interfaces xe-0/1/0 unit 0 family ethernet-switching interface-mode trunk
set protocols mvrp interface xe-0/1/0
```

Step-by-Step Procedure

To configure Access Switch B for MVRP:

1. Configure the finance VLAN:
   
   ```
   [edit]
   user@Access-Switch-B# set vlans finance vlan-id 100
   ```

2. Configure the lab VLAN:
   
   ```
   [edit]
   user@Access-Switch-B# set vlans lab vlan-id 200
   ```

3. Configure the sales VLAN:
   
   ```
   [edit]
   user@Access-Switch-B# set vlans sales vlan-id 300
   ```

4. Configure an Ethernet interface as a member of the finance VLAN:
   
   ```
   [edit]
   user@Access-Switch-B# set interfaces ge-0/0/0 unit 0 family ethernet-switching vlan members finance
   ```

5. Configure an Ethernet interface as a member of the lab VLAN:
   
   ```
   [edit]
   user@Access-Switch-B# set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members lab
   ```

6. Configure a trunk interface:
   
   ```
   user@Access-Switch-B# set interfaces xe-0/1/0 unit 0 family ethernet-switching interface-mode trunk
   ```

7. Enable MVRP on the trunk interface:
   
   ```
   [edit]
   user@Access-Switch-B# set protocols mvrp xe-0/1/0
   ```

**NOTE:** This example uses default MVRP timers. The default values associated with each MVRP timer are: 200 ms for the join timer, 1000 ms for the leave timer, and 10000 ms (10 seconds) for the leaveall timer. We recommend retaining the use of default timer values as modifying timers to inappropriate values might cause an imbalance in the operation of MVRP. However, if you choose to change the default values, keep in mind that on an EX Series switch that uses Junos OS with support for ELS, if the timer value set on an interface level is different from the value set on a switch level, then the value on the interface level takes precedence.
Results  Check the results of the configuration for Switch B:

```
[edit]
user@Access-Switch-B# show
interfaces {
  ge-0/0/0 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members finance;
        }
      }
    }
  }
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        vlan {
          members lab;
        }
      }
    }
  }
  xe-0/1/0 {
    unit 0 {
      family ethernet-switching {
        interface-modetrunk;
      }
    }
  }
}
protocols {
  mvrp {
    interface xe-0/1/0;
  }
}
vlans {
  finance {
    vlan-id 100;
  }
  lab {
    vlan-id 200;
  }
  sales {
    vlan-id 300;
  }
}
```

Configuring VLANS and MVRP on Distribution Switch C

CLI Quick Configuration  To quickly configure distribution Switch C for MVRP, copy the following commands and paste them into the switch terminal window of distribution Switch C:

```
[edit]
set interfaces xe-0/1/1 unit 0 family ethernet-switching interface-mode trunk
```
To configure distribution Switch C for MVRP:

1. Configure the trunk interface to access Switch A:
   ```
   [edit]
   user@Distribution-Switch-C# set interfaces xe-0/1/1 unit 0 family ethernet-switching interface-mode trunk
   ```

2. Configure the trunk interface to access Switch B:
   ```
   [edit]
   user@Distribution-Switch-C# set interfaces xe-0/1/0 unit 0 family ethernet-switching interface-mode trunk
   ```

3. Enable MVRP on the trunk interface for xe-0/1/1:
   ```
   [edit]
   user@Distribution-Switch-C# set protocols mvrp interface xe-0/1/1
   ```

4. Enable MVRP on the trunk interface for xe-0/1/0:
   ```
   [edit]
   user@Distribution-Switch-C# set protocols mvrp interface xe-0/1/0
   ```

Check the results of the configuration for Switch C:

```
[edit]
user@Distribution Switch-C# show interfaces {
  xe-0/1/0 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
      }
    }
  }
  xe-0/1/1 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
      }
    }
  }
}
protocols {
  mvrp {
    interface xe-0/1/0;
    interface xe-0/1/1;
  }
}
```
Verifying That MVRP Is Enabled on Access Switch A

**Purpose**
Verify that MVRP is enabled on the switch.

**Action**
Show the MVRP configuration:

```
user@Access-Switch-A> show mvrp
MVRP configuration for routing instance 'default-switch'
MVRP dynamic VLAN creation : Enabled
MVRP BPDU MAC address      : Customer bridge group (01-80-C2-00-00-21)
MVRP timers (ms)
  Interface       Join   Leave  LeaveAll
  xe-0/1/1         200    1000     10000
```

**Meaning**
The results show that MVRP is enabled on the trunk interface of Switch A and that the default timers are used.

Verifying That MVRP Is Updating VLAN Membership on Access Switch A

**Purpose**
Verify that MVRP is updating VLAN membership by displaying the Ethernet switching interfaces and associated VLANs that are active on Switch A.

**Action**
List Ethernet switching interfaces on the switch:

```
user@Access-Switch-A> show ethernet-switching interface
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop,
                       LH - MAC limit hit, DN - interface down )
Logical Vlan members TAG   MAC      STP       Logical Tagging
interface    members      limit    state     interface flags
ge-0/0/1.0   finance     65535                  Forwarding  tagged
ge-0/0/2.0   lab          65535                  Forwarding  tagged
ge-0/0/3.0   sales        65535                  Forwarding  tagged
```

Copyright © 2013, Juniper Networks, Inc.
Meaning

MVRP has automatically added `finance` and `lab` as VLAN members on the trunk interface because they are being advertised by access Switch B.

Verifying That MVRP Is Enabled on Access Switch B

Purpose

Verify that MVRP is enabled on the switch.

Action

Show the MVRP configuration:

```
user@Access-Switch-B> show mvrp
MVRP configuration for routing instance 'default-switch'
MVRP dynamic VLAN creation : Enabled
MVRP BPDU MAC address      : Customer bridge group (01-80-C2-00-00-21)
MVRP timers (ms)            
                           Interface       Join   Leave  LeaveAll
                           xe-0/1/0         200    1000     10000

Meaning

The results show that MVRP is enabled on the trunk interface of Switch B and that the default timers are used.

Verifying That MVRP Is Updating VLAN Membership on Access Switch B

Purpose

Verify that MVRP is updating VLAN membership by displaying the Ethernet switching interfaces and associated VLANs that are active on Switch B.

Action

List Ethernet switching interfaces on the switch:

```
user@Access-Switch-B> show ethernet-switching interface
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                           LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/0.0                    65535                                 tagged
finance 100 65535    Forwarding
lab 200 65535    Forwarding
```

Meaning

The results show that MVRP is enabled on the trunk interface of Switch B and that the default timers are used.

```
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                           LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/0/0.0                    65535                                 tagged
```

Meaning

The results show that MVRP is enabled on the trunk interface of Switch B and that the default timers are used.

```
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                           LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/1/0.0                    65535                                   tagged
```

Meaning

The results show that MVRP is enabled on the trunk interface of Switch B and that the default timers are used.

```
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                           LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/1/0.0                    65535                                   tagged
```

Meaning

The results show that MVRP is enabled on the trunk interface of Switch B and that the default timers are used.

```
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, 
                           LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
ge-0/1/0.0                    65535                                   tagged
```

Meaning

The results show that MVRP is enabled on the trunk interface of Switch B and that the default timers are used.
### Meaning
MVRP has automatically added finance, lab, and sales as VLAN members on the trunk interface because they are being advertised by access Switch A.

### Verifying That MVRP Is Enabled on Distribution Switch C

#### Purpose
Verify that MVRP is enabled on the switch.

#### Action
Show the MVRP configuration:

```bash
user@Distribution-Switch-C> show mvrp
MVRP configuration for routing instance 'default-switch'
MVRP dynamic VLAN creation : Enabled
MVRP BPDU MAC address      : Customer bridge group (01-80-C2-00-00-21)
MVRP timers (ms)          
Interface       Join   Leave  LeaveAll
xe-0/1/1         200    1000     10000
xe-0/1/0         200    1000     10000
```

#### Meaning
The results show that MVRP is enabled on the trunk interfaces of Switch C and that the default timers are used.

### Verifying That MVRP Is Updating VLAN Membership on Distribution Switch C

#### Purpose
Verify that MVRP is updating VLAN membership on distribution Switch C by displaying the Ethernet switching interfaces and associated VLANs on distribution Switch C.

#### Action
List the Ethernet switching interfaces on the switch:

```bash
user@Distribution-Switch-C> show ethernet-switching interface
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
xe-0/1/1.0                    65535                                 tagged
       mvrp_100               65535 Forwarding
       mvrp_200               65535 Forwarding
       mvrp_300               65535 Forwarding
Routing Instance Name : default-switch
Logical Interface flags (DL - disable learning, AD - packet action drop, LH - MAC limit hit, DN - interface down )
Logical      Vlan       TAG   MAC      STP          Logical         Tagging
interface    members          limit    state        interface flags
xe-0/1/0.0                    65535                                   tagged
       mvrp_100               65535 Forwarding
```

### Meaning
The results show that MVRP is enabled on the trunk interfaces of Switch C and that the default timers are used.
List the VLANs that were created dynamically using MVRP on the switch:

```
user@Distribution-Switch-C> show mvrp dynamic-vlan-memberships
```

MVRP dynamic vlans for routing instance 'default-switch'
(s) static vlan, (f) fixed registration

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>xe-0/1/1.0</td>
</tr>
<tr>
<td></td>
<td>xe-0/1/0.0</td>
</tr>
<tr>
<td>200</td>
<td>xe-0/1/1.0</td>
</tr>
<tr>
<td></td>
<td>xe-0/1/0.0</td>
</tr>
<tr>
<td>300</td>
<td>xe-0/1/1.0</td>
</tr>
</tbody>
</table>

Note that this scenario does not have any fixed registration, which is typical when MVRP is enabled.

**Meaning**

Distribution Switch C has two trunk interfaces. Interface `xe-0/1/1.0` connects Distribution Switch C to Access Switch A and is, therefore, updated to show that it is a member of all the VLANs that are active on Switch A. Any traffic for those VLANs will be passed on from Switch C to Switch A, through interface `xe-0/1/1.0`. Interface `xe-0/1/0.0` connects Switch C to Switch B and is updated to show that it is a member of the two VLANs that are active on Switch B. Thus, Switch C sends traffic for `finance` and `lab` to both Switch A and Switch B. But Switch C sends traffic for `sales` only to Switch A.

Switch C also has three dynamic VLANs created using MVRP: `mvrp_100`, `mvrp_200`, and `mvrp_300`. The dynamically created VLANs `mvrp_100` and `mvrp_200` are active on interfaces `xe-0/1/1.0` and `xe-0/1/0.0`, and dynamically created VLAN `mvrp_300` is active on interface `xe-0/1/1.0`.

**Related Documentation**

- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) on page 2126
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches on page 2063

**Example: Configuring Redundant Trunk Links for Faster Recovery**

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Configuring Redundant Trunk Links for Faster Recovery. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

You can manage network convergence by configuring both a primary link and a secondary link on a switch; this is called a redundant trunk group (RTG). If the primary link in a redundant trunk group fails, it passes its known MAC address locations to the secondary link, which automatically takes over after one minute.
This example describes how to create a redundant trunk group with a primary and a secondary link:

- Requirements on page 2109
- Overview and Topology on page 2109
- Disabling RSTP on Switches 1 and 2 on page 2111
- Configuring Redundant Trunk Links on Switch 3 on page 2112
- Verification on page 2113

Requirements

This example uses the following hardware and software components:

- Two EX Series distribution switches
- One EX Series access switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you configure the redundant trunk links network on the access and distribution switches, be sure you have:

- Configured interfaces ge-0/0/9 and ge-0/0/10 on the access switch, Switch 3, as trunk interfaces. See “Configuring Gigabit Ethernet Interfaces (CLI Procedure)” on page 2286.
- Configured one trunk interface on each distribution switch, Switch 1 and Switch 2.
- Connected the three switches as shown in the topology for this example (see Figure 33 on page 2111).

Overview and Topology

In a typical enterprise network composed of distribution and access layers, a redundant trunk link provides a simple solution for trunk interface network recovery. When a trunk interface fails, data traffic is routed to another trunk interface after one minute, thereby keeping network convergence time to a minimum.

This example shows the configuration of a redundant trunk group that includes one primary link (and its interface) and one unspecified link (and its interface) that serves as the secondary link.

A second type of redundant trunk group, not illustrated in the example, consists of two unspecified links (and their interfaces); in this case, neither of the links is primary. The software selects an active link by comparing the port numbers of the two links and activating the link with the higher port number. For example, if the two link interfaces use interfaces ge-0/1/0 and ge-0/1/1, the software activates ge-0/1/1. (In the interface names, the final number is the port number.)

The two links in a redundant trunk group generally operate the same way, whether they are configured as primary/unspecified or unspecified/unspecified. Data traffic initially passes through the active link but is blocked on the inactive link. While data traffic is blocked on the secondary link, note that Layer 2 control traffic is still permitted if the link...
is active. For example, an LLDP session can be run between two switches on the secondary link. If the active link either goes down or is disabled administratively, it broadcasts a list of its known MAC addresses for data traffic; the other link immediately picks up and adds the MAC addresses to its address table, becomes active, and begins forwarding traffic.

The one difference in operation between the two types of redundant trunk groups occurs when a primary link is active, goes down, is replaced by the secondary link, and then reactivates. When a primary link is re-enabled like this while the secondary link is active, the primary link waits 2 minutes (you can change the time interval by using the preempt cutover timer to accommodate your network) and then takes over as the active link. In other words, the primary link has priority and is always activated if it is available. This differs from the behavior of two unspecified links, both of which act as equals. Because the unspecified links are equal, the active link remains active until it either goes down or is disabled administratively; this is the only time that the other unspecified link learns the MAC addresses and immediately becomes active.

The example given here illustrates a primary/unspecified configuration for a redundant trunk group because that configuration gives you more control and is more commonly used.

---

**NOTE:** Rapid Spanning Tree Protocol (RSTP) is enabled by default on EX Series switches to create a loop-free topology, but an interface is not allowed to be in both a redundant trunk group and in a spanning-tree protocol topology at the same time. You will need to disable RSTP on the two distribution switches in the example, Switch 1 and Switch 2. Spanning-tree protocols can, however, continue operating in other parts of the network—for example, between the distribution switches and also in links between distribution switches and the enterprise core.

Figure 33 on page 2111 displays an example topology containing three switches. Switch 1 and Switch 2 make up the distribution layer, and Switch 3 makes up the access layer. Switch 3 is connected to the distribution layer through trunk interfaces ge-0/0/9.0 (Link 1) and ge-0/0/10.0 (Link 2).

Table 267 on page 2111 lists the components used in this redundant trunk group.

Because RSTP and RTGs cannot operate simultaneously on a switch, you disable RSTP on Switch 1 and Switch 2 in the first configuration task, and you disable RSTP on Switch 3 in the second task.

The second configuration task creates a redundant trunk group called example 1 on Switch 3. The trunk interfaces ge-0/0/9.0 and ge-0/0/10.0 are the two links configured in the second configuration task. You configure the trunk interface ge-0/0/9.0 as the primary link. You configure the trunk interface ge-0/0/10.0 as an unspecified link, which becomes the secondary link by default.
Figure 33: Topology for Configuring the Redundant Trunk Links

Table 267: Components of the Redundant Trunk Link Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>• Switch 1–1 EX Series distribution switch</td>
</tr>
<tr>
<td></td>
<td>• Switch 2–1 EX Series distribution switch</td>
</tr>
<tr>
<td></td>
<td>• Switch 3–1 EX Series access switch</td>
</tr>
<tr>
<td>Trunk interfaces</td>
<td>On Switch 3 (access switch): ge-0/0/9.0 and ge-0/0/10.0</td>
</tr>
<tr>
<td>Redundant trunk group</td>
<td>example1</td>
</tr>
</tbody>
</table>

Disabling RSTP on Switches 1 and 2

To disable RSTP on Switch 1 and Switch 2, perform this task on each switch:

CLI Quick Configuration

To quickly disable RSTP on Switch 1 and Switch 2, copy the following command and paste it into each switch terminal window:

```
[edit]
set protocols rstp disable
```

Step-by-Step Procedure

To disable RSTP on Switch 1 and Switch 2:

1. Disable RSTP on Switch 1 and Switch 2:

```
[edit]
user@switch# set protocols rstp disable
```

Results

Check the results of the configuration:
Configuring Redundant Trunk Links on Switch 3

To configure redundant trunk links on Switch 3, perform this task:

**CLI Quick Configuration**

To quickly configure the redundant trunk group example1 on Switch 3, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set protocols rstp disable
set switch-options redundant-trunk-group group example1 interface ge-0/0/9.0 primary
set switch-options redundant-trunk-group group example1 interface ge-0/0/10.0
set redundant-trunk-group group example1 preempt-cutover-timer 60
```

**Step-by-Step Procedure**

Configure the redundant trunk group example1 on Switch 3.

1. Turn off RSTP:
   ```plaintext
   [edit]
   user@switch# set protocols rstp disable
   ```

2. Name the redundant trunk group example1 while configuring trunk interface ge-0/0/9.0 as the primary link and ge-0/0/10 as an unspecified link to serve as the secondary link:
   ```plaintext
   [edit switch-options]
   user@switch# set redundant-trunk-group group example1 interface ge-0/0/9.0 primary
   user@switch# set redundant-trunk-group group example1 interface ge-0/0/10.0
   ```

3. (Optional) Change the time interval (from the default 120 seconds) that a re-enabled primary link waits to take over for an active secondary link:
   ```plaintext
   [edit switch-options]
   user@switch# set redundant-trunk-group group example1 preempt-cutover-timer 60
   ```

**Results**

Check the results of the configuration:

```plaintext
[edit]
user@switch# show
switch-options
redundant-trunk-group {
    group example1 {
        preempt-cutover-timer 60;
        interface ge-0/0/9.0 {
            primary;
        }
        interface ge-0/0/10.0;
    }
}
protocols {
    rstp {
        disable;
    }
}
```
Verification

To confirm that the configuration is set up correctly, perform this task:

- Verifying That a Redundant Trunk Group Was Created on page 2113

**Verifying That a Redundant Trunk Group Was Created**

**Purpose**
Verify that the redundant trunk group example1 has been created on Switch 1 and that trunk interfaces are members of the redundant trunk group.

**Action**
List all redundant trunk groups configured on the switch:

```bash
user@switch> show redundant-trunk-group
```

<table>
<thead>
<tr>
<th>Group name</th>
<th>Interface</th>
<th>State</th>
<th>Time of last flap</th>
<th>Flap count</th>
</tr>
</thead>
<tbody>
<tr>
<td>example1</td>
<td>ge-0/0/9.0</td>
<td>Up/Pri</td>
<td>Never</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/10.0</td>
<td>Up</td>
<td>Never</td>
<td>0</td>
</tr>
</tbody>
</table>

**Meaning**
The `show redundant-trunk-group` command lists all redundant trunk groups configured on the switch as well as the interface names and their current states (up or down for an unspecified link, and up or down and primary for a primary link). For this configuration example, the output shows that the redundant trunk group example1 is configured on the switch. The Up beside the interfaces indicates that both link cables are physically connected. The Pri beside trunk interface ge-0/0/9.0 indicates that it is configured as the primary link.

**Related Documentation**
- Understanding Redundant Trunk Links on EX Series Switches on page 2068

**Example: Configuring Proxy ARP on an EX Series Switch**

You can configure proxy Address Resolution Protocol (ARP) on your EX Series switch to enable the switch to respond to ARP queries for network addresses by offering its own MAC address. With proxy ARP enabled, the switch captures and routes traffic to the intended destination.

This example shows how to configure proxy ARP on an access switch:

- Requirements on page 2114
- Overview and Topology on page 2114
- Configuration on page 2114
- Verification on page 2115
Requirements

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 10.0 or later for EX Series switches

Overview and Topology

This example shows the configuration of proxy ARP on an interface of an EX Series switch using restricted mode. In restricted mode, the switch does not act as a proxy for hosts on the same subnet.

The topology for this example consists of one EX Series switch. When a host wants to communicate with a host that is not already in its ARP table, it broadcasts an ARP request for the MAC address of the destination host:

- When proxy ARP is not enabled, a host that shares the same IP address replies directly to the ARP request, providing its MAC address, and future transmissions are sent directly to the destination host MAC address.
- When proxy ARP is enabled, the switch responds to ARP requests, providing the switch’s MAC address—even when the destination IP address is the same as the source IP address. Thus, communications must be sent through the switch and then routed through the switch to the appropriate destination.

Configuration

To configure proxy ARP, perform the following tasks:

**CLI Quick Configuration**

To quickly configure proxy ARP on an interface, copy the following command and paste it into the switch terminal window:

```
[edit]
set interfaces ge-0/0/3 unit 0 proxy-arp restricted
```
Step-by-Step Procedure

You configure proxy ARP on individual interfaces.

1. To configure proxy ARP on an interface:

   [edit interfaces]
   user@switch# set ge-0/0/3 unit 0 proxy-arp restricted

   **BEST PRACTICE:** We recommend that you configure proxy ARP in restricted mode. In restricted mode, the switch does not act as a proxy if the source and target IP addresses are on the same subnet. If you use unrestricted mode, disable gratuitous ARP requests on the interface to avoid a situation wherein the switch's response to a gratuitous ARP request appears to the host to be an indication of an IP conflict.

   [edit interfaces]
   user@switch# set ge-0/0/3 no-gratuitous-arp-request

Results

Display the results of the configuration:

   user@switch> show configuration
   interfaces {
      ge-0/0/3 {
         unit 0 {
            proxy-arp restricted;
            family ethernet-switching;
         }
      }
   }

Verification

To verify that the switch is sending proxy ARP messages, perform these tasks:

- Verifying That the Switch Is Sending Proxy ARP Messages on page 2115

Verifying That the Switch Is Sending Proxy ARP Messages

Purpose

Verify that the switch is sending proxy ARP messages.

Action

List the system statistics for ARP messages:

   user@switch> show system statistics arp
   arp:
      90060 datagrams received
      34 ARP requests received
      610 ARP replies received
      2 resolution request received
      0 unrestricted proxy requests
      0 restricted proxy requests
      0 received proxy requests
      0 unrestricted proxy requests not proxied
      0 restricted proxy requests not proxied
      0 datagrams with bogus interface
      0 datagrams with incorrect length
      0 datagrams for non-IP protocol
      0 datagrams with unsupported op code
Meaning

The statistics show that two proxy ARP requests were received. The *unrestricted proxy requests not proxied* and *restricted proxy requests not proxied* fields indicate that all the unproxied ARP requests received have been proxied by the switch.

Related Documentation

- Configuring Proxy ARP (CLI Procedure)
- Configuring Proxy ARP (CLI Procedure) on page 2130
- Understanding Proxy ARP on EX Series Switches on page 2070

Configuration Tasks

- Configuring VLANs for EX Series Switches (J-Web Procedure) on page 2117
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
- Configuring MAC Table Aging (CLI Procedure) on page 2123
- Configuring the Native VLAN Identifier (CLI Procedure) on page 2124
- Configuring Virtual Routing Instances (CLI Procedure) on page 2125
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) on page 2126
- Configuring Redundant Trunk Groups (J-Web Procedure) on page 2129
- Configuring Proxy ARP (CLI Procedure) on page 2130
- Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure) on page 2131
- Configuring MAC Limiting (CLI Procedure) on page 2132
Configuring VLANs for EX Series Switches (J-Web Procedure)

You can use the VLAN Configuration page to add a new VLAN or to edit or delete an existing VLAN on an EX Series switch.

To access the VLAN Configuration page:

1. Select Configure > Switching > VLAN.

   The VLAN Configuration page displays a list of existing VLANs. If you select a specific VLAN, the specific VLAN details are displayed in the Details section.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Creates a VLAN.
   - **Edit**—Edits an existing VLAN configuration.
   - **Delete**—Deletes an existing VLAN.

   **NOTE:** If you delete a VLAN, the VLAN configuration for all the associated interfaces is also deleted.

When you are adding or editing a VLAN, enter information as described in Table 268 on page 2117.

### Table 268: VLAN Configuration Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Specifies a unique name for the VLAN.</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>VLAN ID/Range/VLAN ID/List</td>
<td>Specifies the identifier or range for the VLAN.</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td><strong>NOTE:</strong> EX4300 switches support only VLAN ID/List and not VLAN Range.</td>
<td></td>
<td>• VLAN ID—Type a unique identification number from 1 through 4094. If no value is specified, the ID defaults to 0.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the VLAN.</td>
<td>Enter a brief description for the VLAN.</td>
</tr>
</tbody>
</table>
Table 268: VLAN Configuration Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC-Table-Aging-Time</td>
<td>Specifies the maximum time that an entry can remain in the forwarding table before it ages out.</td>
<td>Type the number of seconds from 60 through 1000000.</td>
</tr>
<tr>
<td>NOTE: This option is not supported on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Input filter | Specifies the VLAN firewall filter that is applied to incoming packets. | To apply an input firewall filter, select the firewall filter from the list. |
| Output filter | Specifies the VLAN firewall filter that is applied to outgoing packets. | To apply an output firewall filter, select the firewall filter from the list. |

Ports tab

<table>
<thead>
<tr>
<th>Ports</th>
<th>Specifies the ports (interfaces) to be associated with this VLAN for data traffic. You can also remove the port association.</th>
<th>Click one of the following options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE: This option is not supported on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IP address tab

<table>
<thead>
<tr>
<th>IPv4 address</th>
<th>Specifies IPv4 address options for the VLAN.</th>
<th>Select IPv4 address to enable the IPv4 address options.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>To configure IPv4:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Enter the IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the subnet mask—for example, 255.255.255.0. You can also specify the address prefix.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. To apply an input firewall filter to an interface, select the firewall filter from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. To apply an output firewall filter to an interface, select the firewall filter from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click the ARP/MAC Details button. Enter the static IP address and MAC address in the window that is displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: In EX4300 switches, you also need to select L2 Interface in the window that is displayed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv6 address</th>
<th>Specifies IPv6 address options for the VLAN.</th>
<th>Select IPv6 address to enable the IPv6 address options.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>To configure IPv6:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Enter the IP address—for example: 2001:ab8:85a3::8a2e:370:7334.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the subnet mask.</td>
</tr>
</tbody>
</table>

VoIP tab
<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Specifies the ports to be associated with this VLAN for voice traffic. You can also remove the port association.</td>
<td>Click one of the following options:</td>
</tr>
</tbody>
</table>

- **Add**—Select the ports from the list of available ports. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.
- **Remove**—Select the port that you do not want associated with the VLAN.

---

**Related Documentation**

- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
- Configuring VLANs for EX Series Switches (CLI Procedure)
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch
- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
- Configuring Routed VLAN Interfaces (CLI Procedure)

### Configuring VLANs for EX Series Switches (CLI Procedure)

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring VLANs for EX Series Switches (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

EX Series switches use VLANs to make logical groupings of network nodes with their own broadcast domains. VLANs limit the traffic flowing across the entire LAN and reduce collisions and packet retransmissions.

- Why Create a VLAN? on page 2119
- Creating a VLAN Using the Minimum Procedure on page 2120
- Creating a VLAN Using All of the Options on page 2120
- Configuration Guidelines for VLANs on page 2121

**Why Create a VLAN?**

For switching to begin, you must explicitly configure at least one VLAN, even if your network is simple and you want only one broadcast domain to exist.

Some reasons to create more than one VLAN are:
• A LAN has more than 200 devices.
• A LAN has a large amount of broadcast traffic.
• A group of clients requires that a higher-than-average level of security be applied to traffic entering or exiting the group's devices.
• A group of clients requires that the group's devices receive less broadcast traffic than they are currently receiving, so that data speed across the group is increased.

Creating a VLAN Using the Minimum Procedure

These steps are required to create a VLAN:

• Uniquely identify the VLAN. You do this by assigning a name and an ID to the VLAN.
• Assign at least one switch port interface to the VLAN for communication. After assigning one or more interfaces to the VLAN, the interfaces function in access mode. All interfaces in a single VLAN are in a single broadcast domain, even if the interfaces are on different switches. You can assign traffic on any switch to a particular VLAN by referencing either the interface sending traffic or the MAC addresses of devices sending traffic.

The following example creates a VLAN using only a few required steps. The VLAN is created with the name `employee-vlan` and the VLAN ID of `100`. Then, three interfaces are assigned to that VLAN, and these interfaces, which function in access mode, transmit traffic among themselves.

```
[edit] set vlans employee-vlan
edit] set vlans employee-vlan vlan-id 100
[edit] set interfaces ge-0/0/1 unit 0 family ethernet-switching vlan members employee-vlan
[edit] set interfaces ge-0/0/2 unit 0 family ethernet-switching vlan members employee-vlan
[edit] set interfaces ge-0/0/3 unit 0 family ethernet-switching vlan members employee-vlan
```

In the example, all users connected to the interfaces ge-0/0/1, ge-0/0/2, and ge-0/0/3 can communicate with each other, but not with users on other interfaces in this network. To configure communication between VLANs, you must configure an integrated routing and bridging (IRB) interface. See "Configuring Integrated Routing and Bridging Interfaces (CLI Procedure)" on page 2122.

Creating a VLAN Using All of the Options

To configure a VLAN, follow these steps:

1. Create the VLAN by setting the unique VLAN name:

   ```
   [edit vlans]
   user@switch# set vlan-name
   ```

2. Configure the VLAN ID or a VLAN ID list for the VLAN. Using the VLAN ID list option, you can optionally specify a range of VLAN IDs.

   ```
   [edit vlans]
   user@switch# set vlan-name vlan-id vlan-id-number
   ```
or

[edit vlans]
user@switch# set vlan-name vlan-id-list [vlan-ids | vlan-id--vlan-id-]

3. Assign at least one interface to the VLAN:

[edit interfaces]
user@switch# set interface-name unit logical-unit-number family ethernet-switching vlan members [all | vlan-names | vlan-ids]

NOTE: You can also specify that a trunk interface is a member of all VLANs that are configured on this switch. When a new VLAN is configured on the switch, this trunk interface automatically becomes a member of the VLAN.

4. (Optional) Create a subnet for the VLAN because all computers that belong to a subnet are addressed with a common, identical, most-significant-bit group in their IP address. This makes it easy to identify VLAN members by their IP addresses. To create the subnet for the VLAN:

[edit interfaces]
user@switch# set vlan unit logical-unit-number family inet address ip-address/destination-prefix

5. (Optional) Specify the description of the VLAN:

[edit vlans]
user@switch# set vlan-name description text-description

6. (Optional) For security purposes, specify a VLAN firewall filter to be applied to incoming or outgoing packets:

[edit vlans]
user@switch# set vlan-name filter (input | output) filter-name

Configuration Guidelines for VLANs

To create a VLAN, you must uniquely identify the VLAN and assign at least one switch port interface to the VLAN for communication. After you assign one or more interfaces to the VLAN, the interfaces function in access mode.

After creating a VLAN, all users connected to interfaces that are assigned to the VLAN can communicate with each other but not with users on other interfaces in the network. To configure communication between VLANs, you must configure an IRB interface. For information about creating an IRB interface, see “Configuring Integrated Routing and Bridging Interfaces (CLI Procedure)” on page 2122.

The number of VLANs supported per switch varies. Use the command set vlans vlan-name vlan-id ? to determine the maximum number of VLANs allowed on a switch. You cannot exceed this VLAN limit because each VLAN is assigned an ID number when it is created.
Configuring Integrated Routing and Bridging Interfaces (CLI Procedure)

Integrated routing and bridging (IRB) interfaces allow an EX Series switch to recognize packets that are being sent to local addresses so that they are bridged (switched) whenever possible and are routed only when necessary. Whenever packets can be switched instead of routed, several layers of processing are eliminated.

An interface named irb functions as a logical router on which you can configure a Layer 3 logical interface for each virtual LAN (VLAN). For redundancy, you can combine an IRB interface with implementations of the Virtual Router Redundancy Protocol (VRRP) in both bridging and virtual private LAN service (VPLS) environments.

Jumbo frames of up to 9216 bytes are supported on an IRB interface. To route jumbo data packets on the IRB interface, you must configure the jumbo MTU size on the member physical interfaces of the IRB interface and also on the IRB interface itself (the interface named irb). However, for jumbo control packets—for example, to ping the IRB interface with a packet size of 6000 bytes or more—you must explicitly configure the jumbo MTU size on the interface named irb (the IRB interface).

CAUTION: Setting or deleting the jumbo MTU size on the IRB interface (the interface named irb) while the switch is transmitting packets might result in dropped packets.

To configure the IRB interface:

1. Create a Layer 2 VLAN by assigning it a name and a VLAN ID:

   [edit]
   user@switch# set vlans vlan-name vlan-id

2. Assign an interface to the VLAN by naming the VLAN as a trunk member on the logical interface, thereby making the interface part of the VLAN’s broadcast domain:

   [edit]
   user@switch# set interfaces interface-name unit logical-unit-number family ethernet-switching vlan members vlan-name

3. Create a logical Layer 3 IRB interface (its name will be irb.logical-interface-number, where the value for logical-interface-number is the value you supplied for vlan-id in Step 1; in the following command, it is the logical-unit-number) on a subnet for the VLAN’s broadcast domain:

   [edit]
   user@switch# set interfaces vlan unit logical-unit-number family inet address inet-address

4. Link the Layer 2 VLAN to the logical Layer 3 IRB interface:

   [edit]
   user@switch# set vlans vlan-name l3-interface irb.logical-interface-number

NOTE: Layer 3 interfaces on trunk ports allow the interface to transfer traffic between multiple Layer 2 VLANs. Within a VLAN, traffic is switched, while across VLANs, traffic is routed.
Configuring MAC Table Aging (CLI Procedure)

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring MAC Table Aging (CLI Procedure).

The Ethernet switching table (or MAC table) aging process ensures that the EX Series switch tracks only active MAC addresses on the network and is able to flush out MAC addresses that are no longer used.

You can configure the MAC table aging time, the maximum time that an entry can remain in the Ethernet Switching table before it ages out, on all VLANs on the switch. This setting can influence efficiency of network resource use by affecting the amount of traffic that is flooded to all interfaces because when traffic is received for MAC addresses no longer in the Ethernet switching table, the switch floods the traffic to all interfaces.

To configure the MAC table aging time on all VLANs on the switch:

```
[edit]
user@switch# set protocols l2-learning global-mac-table-aging-time seconds
```

**Related Documentation**

- Verifying Integrated Routing and Bridging Interface Status and Statistics on page 2178
- Understanding Integrated Routing and Bridging Interfaces and Routed VLAN Interfaces on EX Series Switches on page 2058
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073
- Example: Connecting Access Switches to a Distribution Switch on page 2083
- Understanding Bridging and VLANs on EX Series Switches on page 2049

Copyright © 2013, Juniper Networks, Inc.
### Configuring the Native VLAN Identifier (CLI Procedure)

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring the Native VLAN Identifier (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

EX Series switches can receive and forward routed or bridged Ethernet frames with 802.1Q VLAN tags. Typically, trunk ports, which connect switches to each other, accept untagged control packets but do not accept untagged data packets. You can enable a trunk port to accept untagged data packets by configuring a native VLAN ID on the interface on which you want the untagged data packets to be received. The logical interface on which untagged packets are to be received must be configured with the same VLAN ID as the native VLAN ID configured on the physical interface.

To configure the native VLAN ID by using the command-line interface (CLI):

1. On the interface on which you want untagged data packets to be received, set the **interface mode** to **trunk**, which specifies that the interface is in multiple VLANs and can multiplex traffic between different VLANs:

   ```
   [edit interfaces]
   user@switch# set interface-name unit logical-unit-number family ethernet-switching interface-mode trunk
   ```

2. Configure the native VLAN ID:

   ```
   [edit interfaces]
   user@switch# set interface-name native-vlan-id vlan-id
   ```

3. Specify that the logical interface that will receive the untagged data packets is a member of the native VLAN:

   ```
   [edit interfaces]
   user@switch# set interface-name unit logical-unit-number family ethernet-switching vlan members vlan-id
   ```

**Related Documentation**

- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Example: Connecting Access Switches to a Distribution Switch on page 2083
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073
Configuring Virtual Routing Instances (CLI Procedure)

Use virtual routing and forwarding (VRF) to divide an EX Series switch into multiple virtual routing instances. VRF allows you to isolate traffic traversing the network without using multiple devices to segment your network. VRF is supported on all Layer 3 interfaces.

Before you begin, make sure to set up your VLANs. See Configuring VLANs for EX Series Switches (CLI Procedure), “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119, or “Configuring VLANs for EX Series Switches (J-Web Procedure)” on page 2117.

To configure virtual routing instances:

1. Create a routing instance:

   [edit routing-instances]user@switch# set routing-instance-name instance-type virtual-router

   **NOTE:** EX Series switches only support the virtual-router instance type.

2. Bind each routing instance to the corresponding physical interfaces:

   [edit routing-instances]user@switch# set routing-instance-name interface interface-name.logical-unit-number

3. Create the logical interfaces that are bound to the routing instance.

   • To create a logical interface with an IPv4 address:

     [edit interfaces]user@switch# set interface-name unit logical-unit-number family inet address ip-address

   • To create a logical interface with an IPv6 address:

     [edit interfaces]user@switch# set interface-name unit logical-unit-number family inet6 address ipv6-address

   **NOTE:** Do not create a logical interface using the family ethernet-switching option in this step. Binding an interface using the family ethernet-switching option to a routing instance can cause the interface to shutdown.

4. Enable VLAN tagging on each physical interface that was bound to the routing instance:

   [edit interfaces]user@switch# set interface-name vlan-tagging

**Related Documentation**

- Example: Using Virtual Routing Instances to Route Among VLANs on EX Series Switches on page 2093
- Verifying That Virtual Routing Instances Are Working on page 2177
- Understanding Virtual Routing Instances on EX Series Switches on page 2062
Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs Junos OS that does not support ELS, see Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Multiple VLAN Registration Protocol (MVRP) is used to manage dynamic VLAN registration in a LAN. You can use MVRP on EX Series switches.

MVRP is disabled by default on EX Series switches.

To enable MVRP or set MVRP options, follow these instructions:

- Enabling MVRP on page 2126
- Disabling MVRP on page 2126
- Disabling Dynamic VLANs on page 2126
- Configuring Timer Values on page 2127
- Configuring MVRP Registration Mode on page 2128
- Using MVRP in a Mixed-Release Network on page 2128

Enabling MVRP

MVRP can only be enabled on trunk interfaces.

To enable MVRP on a trunk interface:

````
[edit protocols mvrp]
user@switch# set interface interface-name
```

Disabling MVRP

MVRP is disabled by default. You only need to perform this procedure if you have previously enabled MVRP.

You can disable MVRP globally only. To disable MVRP on all trunk interfaces on a switch, use one of the following commands:

````
user@switch# deactivate protocols mvrp
user@switch# delete protocols mvrp
```

Disabling Dynamic VLANs

By default, dynamic VLANs can be created on interfaces participating in MVRP. Dynamic VLANs are VLANs created on one switch that are propagated to other switches dynamically; in this case, using MVRP.
Dynamic VLAN creation through MVRP cannot be disabled per switch interface. To disable dynamic VLAN creation for interfaces participating in MVRP, you must disable it for all interfaces on the switch.

To disable dynamic VLAN creation:

[edit protocols mvrp]
user@switch# set no-dynamic-vlan

Configuring Timer Values

The timers in MVRP define the amount of time all interfaces on a switch or a specific interface wait to join or leave MVRP, or to send or process the MVRP information for the switch after receiving an MVRP PDU. The join timer controls the amount of time the switch waits to accept a registration request, the leave timer controls the period of time that the switch waits in the Leave state before changing to the unregistered state, and the leaveall timer controls the frequency with which the LeaveAll messages are communicated.

The default MVRP timer values are 200 ms for the join timer, 1000 ms for the leave timer, and 10 seconds for the leaveall timer.

BEST PRACTICE: Maintain default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP.

On an EX Series switch that uses Junos OS with support for ELS, if the timer value set on an interface level is different from the value set on a switch level, then the value on the interface level takes precedence.

To set the join timer for all interfaces on the switch:

[edit protocols mvrp]
user@switch# set join-timer milliseconds

To set the join timer for a specific interface:

[edit protocols mvrp]
user@switch# set interface interface-name join-timer milliseconds

To set the leave timer for all interfaces on the switch:

[edit protocols mvrp]
user@switch# set leave-timer milliseconds

To set the leave timer for a specific interface:

[edit protocols mvrp]
user@switch# set interface interface-name leave-timer milliseconds

To set the leaveall timer for all interfaces on the switch:

[edit protocols mvrp]
user@switch# set leave-all-timer seconds
To set the leaveall timer for a specific interface:

```
[edit protocols mvrp]
user@switch# set interface interface-name leaveall-timer seconds
```

### Configuring MVRP Registration Mode

The default MVRP registration mode for any interface participating in MVRP is normal. An interface in normal registration mode participates in MVRP when MVRP is enabled on the switch.

You can change the registration mode of a specific interface to **forbidden**. An interface in forbidden registration mode does not participate in MVRP even if MVRP is enabled on the switch.

To set an interface to forbidden registration mode:

```
[edit protocols mvrp]
user@switch# set interface xe-0/0/1.0 registration forbidden
```

To set an interface to normal registration mode:

```
[edit protocols mvrp]
user@switch# set interface xe-0/0/1.0 registration normal
```

### Using MVRP in a Mixed-Release Network

Except in Junos OS Releases 11.2 and earlier, MVRP has conformed with IEEE standard 802.1ak and IEEE Draft 802.1Q regarding the inclusion of an extra byte in the protocol data units (PDUs) sent and received by MVRP. As a result of changes in the standards with regard to the extra byte, MVRP in Junos OS Releases 13.2 and later for EX Series switches with support for the Enhanced Layer 2 Software (ELS) includes the extra byte, while MVRP in Junos OS Releases 11.3 and later for EX Series switches that do not support ELS does not include the extra byte. A compatibility issue arises, wherein the ELS version of MVRP does not recognize PDUs without the extra byte sent by the non-ELS version of MVRP.

For more information about this issue, see “Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches” on page 2063.

You can recognize an MVRP version compatibility issue by observing the switch running the ELS version of MVRP. Because a switch running the ELS version of MVRP cannot interpret an unmodified PDU from a switch running the non-ELS version of MVRP, the switch will not add VLANs from the non-ELS version of MVRP. When you use the `show mvrp statistics` command in the ELS version of MVRP, the values for `Received Join Empty` and `Received Join In` will incorrectly display zero, even though the value for the `Received MVRP PDUs without error` has been increased. Another indication that MVRP is having a version compatibility issue is that unexpected VLAN activity, such as multiple VLAN creation, takes place on the switch running the ELS version of MVRP.

If your network includes a mix of EX Series switches running ELS and non-ELS versions of MVRP, you can eliminate the compatibility issue by entering the following command on the switches running the ELS version of MVRP:
The `no-attribute-length-in-pdu` statement prevents the ELS version of MVRP from sending PDUs with the extra byte, thereby eliminating the compatibility issue with the non-ELS version of MVRP.

**Related Documentation**
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096
- Verifying That MVRP Is Working Correctly on page 2180
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches on page 2063

**Configuring Redundant Trunk Groups (J-Web Procedure)**

A redundant trunk link provides a simple solution for network recovery when a trunk interface goes down. Traffic is routed to another trunk interface, keeping network convergence time to a minimum. You can configure redundant trunk groups (RTGs) with a primary link and a secondary link on trunk interfaces, or configure dynamic selection of the active interface. If the primary link fails, the secondary link automatically takes over without waiting for normal Spanning Tree Protocol (STP) convergence. An RTG can be created only if the following conditions are satisfied:

- A minimum of two trunk interfaces that are not part of any RTG are available.
- All the selected trunk interfaces to be added to the RTG have the same VLAN configuration.
- The selected trunk interfaces are not part of a spanning-tree configuration.

To configure an RTG by using the J-Web interface:

1. Select **Configure > Switching > RTG**.

   The RTG Configuration page displays a list of existing RTGs. If you select a specific RTG, the details of the selected RTG are displayed in the Details of group section.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Creates an RTG.
   - **Edit**—Modifies an RTG.
   - **Delete**—Deletes an RTG.
When you are adding or editing an RTG, enter information as described in Table 269 on page 2130.

3. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.

Table 269: RTG Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Specifies a unique name for the RTG.</td>
<td>Enter a name.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only on EX4300 switches, you can select the name from a list.</td>
<td></td>
</tr>
<tr>
<td>Member Interface 1</td>
<td>Specifies a logical interface containing multiple trunk interfaces.</td>
<td>Select a trunk interface from the list.</td>
</tr>
<tr>
<td>Member Interface 2</td>
<td>Specifies a trunk interface containing multiple VLANs.</td>
<td>Select a trunk interface from the list.</td>
</tr>
</tbody>
</table>
| Select Primary Interface | Enables you to specify one of the interfaces in the RTG as the primary link. The interface without this option is the secondary link in the RTG. | 1. Select the option button.  
2. Select the primary interface. |
| Dynamically select my active interface | Specifies that the system dynamically select the active interface. | Select the option button. |

**Related Documentation**
- Example: Configuring Redundant Trunk Links for Faster Recovery on page 2108
- Example: Configuring Redundant Trunk Links for Faster Recovery
- Understanding Redundant Trunk Links on EX Series Switches on page 2068

**Configuring Proxy ARP (CLI Procedure)**

**NOTE:** This task uses Junos OS for EX Series switches and QFX3500 and QFX3600 switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Proxy ARP (CLI Procedure) or Configuring Proxy ARP. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

You can configure proxy Address Resolution Protocol (ARP) on your switch to enable the switch to respond to ARP queries for network addresses by offering its own media access control (MAC) address. With proxy ARP enabled, the switch captures and routes traffic to the intended destination.

To configure proxy ARP on a single interface:
```
[edit interfaces]
```
user@switch# set interface-name unit logical-unit-number proxy-arp (restricted | unrestricted)

**BEST PRACTICE:** We recommend that you configure proxy ARP in restricted mode. In restricted mode, the switch does not act as a proxy if the source and target IP addresses are on the same subnet. If you decide to use unrestricted mode, disable gratuitous ARP requests on the interface to avoid a situation wherein the switch’s response to a gratuitous ARP request appears to the host to be an indication of an IP conflict.

To configure proxy ARP on an integrated routing and bridging (IRB) interface:

```
[edit interfaces]
user@switch# set irb.logical-unit-number proxy-arp restricted
```

**Related Documentation**
- Example: Configuring Proxy ARP on an EX Series Switch on page 2113
- Verifying That Proxy ARP Is Working Correctly on page 2181
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122

---

The Ethernet switching table, also known as the forwarding table, specifies the known locations of VLAN nodes and the addresses of devices within those nodes. There are two ways to populate the Ethernet switching table on a switch. The easiest method is to let the switch update the table with MAC addresses.

The second way to populate the Ethernet switching table is to manually insert addresses into the table. You can do this to reduce flooding and speed up the switch’s automatic learning process.

Before configuring a static MAC address, be sure that you have:

- Set up the VLAN. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.

To configure an interface to have a static MAC address:

```
[edit vlans vlan-name switch-options]
user@switch# set static-mac mac-address
```

**Related Documentation**
- Understanding Bridging and VLANs on EX Series Switches on page 2049
Configuring MAC Limiting (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring MAC Limiting (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

This topic describes various ways of configuring a limitation on MAC addresses in packets that are received and forwarded by the switch.

The different ways of setting a MAC limit are described in the following sections:

- Limiting the Number of MAC Addresses Learned by an Interface on page 2132
- Limiting the Number of MAC Addresses Learned by a VLAN on page 2132

Limiting the Number of MAC Addresses Learned by an Interface

To secure a port, you can set the maximum number of MAC addresses that can be learned by an interface:

- Set the MAC limit on an interface, and specify an action that the switch takes after the specified limit is exceeded:

  ```
  [edit switch-options]
  user@switch# set interface interface-name interface-mac-limit limit packet-action action
  
  After you set a new MAC limit for the interface, the system clears existing entries in the MAC address forwarding table associated with the interface.
  ```

Limiting the Number of MAC Addresses Learned by a VLAN

To limit the number of MAC addresses learned by a VLAN:

1. Set the maximum number of MAC addresses that can be learned by a VLAN, and specify an action that the switch takes after the specified limit is exceeded:

   ```
   [edit vlans]
   user@switch# set vlan-name switch-options mac-table-size limit packet-action action
   
   After you set a new VLAN MAC limit, the system clears existing entries in the VLAN MAC address forwarding table.
   ```

2. Set the maximum number of MAC addresses that can be learned by one or all interfaces in a VLAN, and specify an action that the switch takes after the specified limit is exceeded:

   ```
   [edit vlans]
   user@switch# set vlan-name switch-options interface interface-name interface-mac-limit limit packet-action action
   
   After you set a new VLAN interface MAC limit, the system clears existing entries in the VLAN interface MAC address forwarding table.
   ```
NOTE: If you specify a MAC limit and packet action for all interfaces in the VLAN and a specific interface in the VLAN, the MAC limit and packet action specified at the specific interface level takes precedence. Also, at the VLAN interface level, only the drop and drop-and-log options are supported.

After you set new MAC limits for a VLAN by using the `mac-table-size` statement or for interfaces associated with a VLAN by using the `interface-mac-limit` statement, the system clears the corresponding existing entries in the MAC address forwarding table.

Related Documentation

- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Configuring Persistent MAC Learning (CLI Procedure) on page 4032

Configuration Statements

- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2133
- [edit switch-options] Configuration Statement Hierarchy on EX Series Switches on page 2134
- [edit protocols] Configuration Statement Hierarchy on EX4300 Switches on page 2135
- [edit vlans] Configuration Statement Hierarchy on EX Series Switches on page 2136

[edit interfaces] Configuration Statement Hierarchy on EX Series Switches

Each of the following topics lists the statements at a subhierarchy of the `edit interfaces` hierarchy:

- [edit interfaces ae] Configuration Statement Hierarchy on EX Series Switches on page 2354
- [edit interfaces et] Configuration Statement Hierarchy on EX Series Switches on page 2360
- [edit interfaces ge] Configuration Statement Hierarchy on EX Series Switches on page 2365
- [edit interfaces interface-range] Configuration Statement Hierarchy on EX Series Switches on page 2371
- [edit interfaces irb] Configuration Statement Hierarchy on EX Series Switches on page 2379
- [edit interfaces lo] Configuration Statement Hierarchy on EX Series Switches on page 2383
- [edit interfaces me] Configuration Statement Hierarchy on EX Series Switches on page 2386
- [edit interfaces vme] Configuration Statement Hierarchy on EX Series Switches on page 2389
- [edit interfaces xe] Configuration Statement Hierarchy on EX Series Switches on page 2393
This topic lists supported and unsupported configuration statements in the [edit switch-options] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.

- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit switch-options] Hierarchy Level on page 2134
- Unsupported Statements in the [edit switch-options] Hierarchy Level on page 2135

### Supported Statements in the [edit switch-options] Hierarchy Level

The following hierarchy shows the [edit switch-options] configuration statements supported on EX Series switches:

```json
switch-options {
    authentication-whitelist mac-address {
        interface interface-name;
        vlan-assignment (vlan-id | vlan-name);
    }
    interface interface-name {
        interface-mac-limit number {
            packet-action action;
        }
        no-mac-learning;
        persistent-learning
    }
}
```
no-mac-learning;
redundant-trunk-group {
  group name {
    description text;
    interface interface-name {
      primary;
      }
    preempt-cutover-timer seconds
    }
  }
unknown-unicast-forwarding {
  vlan (all | vlan-name | vlan-tag) {
    interface interface-name;
  }
}
voip {
  interface (all | [interface-name | access-ports]) {
    forwarding-class (assured-forwarding | best-effort | expedited-forwarding | mcast-af | mcast-be | mcast-ef | mcast-nc | network-control);
    vlan vlan-name;
  }
}

Unsupported Statements in the [edit switch-options] Hierarchy Level

All statements in the [edit switch-options] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 270: Unsupported [edit switch-options] Configuration Statements on EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-error-disable</td>
<td>[edit switch-options]</td>
</tr>
<tr>
<td>disable-timeout</td>
<td>[edit switch-options port-error-disable]</td>
</tr>
</tbody>
</table>

NOTE: Variables, such as filename, are not shown in the statements or hierarchies.

[edit protocols] Configuration Statement Hierarchy on EX4300 Switches

Each of the following topics lists the statements at a subhierarchy of the [edit protocols] hierarchy:

- [edit protocols bfd] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols bgp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches on page 1769
- [edit protocols igmp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols igmp-snooping] Configuration Statement Hierarchy on page 3329
- [edit protocols isis] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols lACP] Configuration Statement Hierarchy on EX Series Switches on page 2398
- [edit protocols l2-learning] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols layer2-control] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols lldp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols lldp-med] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols msdp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols mstp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols mvrp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols neighbor-discovery] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols oam] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols ospf] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols ospf3] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols pim] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols rip] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols ripng] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols router-advertisement] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols router-discovery] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols rstp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols sflow] Configuration Statement Hierarchy on EX Series Switches on page 3708
- [edit protocols uplink-failure-detection] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols vrrp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols vstp] Configuration Statement Hierarchy on EX Series Switches

Related Documentation

- EX Series Switch Software Features Overview

[edit vlans] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit vlans] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
• **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

• Supported Statements in the [edit vlans] Hierarchy Level on page 2137
• Unsupported Statements in the [edit vlans] Hierarchy Level on page 2139

**Supported Statements in the [edit vlans] Hierarchy Level**

The following hierarchy shows the [edit vlans] configuration statements supported on one or more of the EX Series switches:

```
vlans {
  vlan-name {
    description text-description;
    domain-type bridge;
    forwarding-options {
      dhcp-security {
        arp-inspection;
        group group-name {
          interface interface-name {
            static-ip ip-address {
              mac mac-address;
            }
          }
          overrides {
            no-option82;
            trusted;
          }
        }
      }
      ip-source-guard;
      no-dhcp-snooping;
      option-82 {
        circuit-id {
          prefix {
            host-name;
            logical-system-name;
            routing-instance-name;
          }
          use-interface-description (device | logical);
          use-vlan-id;
        }
        remote-id {
          host-name;
          use-interface-description (device | logical);
          use-string string;
        }
        vendor-id {
          use-string string;
        }
      }
    }
  }
}
```
filter {
    input filter-name;
    output filter-name;
}

flood {
    input filter-name;
}

l3-interface irb.logical-unit-number;
multicast-snooping-options {
    flood-groups [group-names];
    forwarding-cache {
        threshold {
            reuse threshold;
            suppress threshold;
        }
    }
    graceful-restart {
        disable;
        restart-duration duration;
    }
    host-outbound-traffic {
        dot1p bits;
        forwarding-class forwarding-class;
    }
    multichassis-lag-replicate-state;
    nexthop-hold-time time;
    options {
        syslog {
            level level;
            mark interval;
            upto level;
        }
    }
    traceoptions {
        file filename {
            files number;
            no-world-readable;
            size file-size;
            world-readable;
        }
        flag flag {
            disable;
        }
    }
}
switch-options {
    interface interface-name {
        interface-mac-limit limit {
            packet-action action;
        }
        static-mac mac-address;
    }
    interface-mac-limit limit {
}
### Unsupported Statements in the [edit vlans] Hierarchy Level

All statements in the [edit vlans] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

**Table 271: Unsupported [edit vlans] Configuration Statements on EX Series Switches**

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcae-mac-synchronize</td>
<td>[edit vlans]</td>
</tr>
<tr>
<td>no-irb-layer-2-copy</td>
<td>[edit vlans]</td>
</tr>
</tbody>
</table>

**NOTE:** Variables, such as filename, are not shown in the statements or hierarchies.

- Example: Connecting Access Switches to a Distribution Switch on page 2083
address

Syntax

`address (ip-address | ipv6-address);`

Hierarchy Level

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number family family],
[edit dynamic-profiles profile-name interfaces demux0 unit logical-unit-number family family],
[edit dynamic-profiles profile-name interfaces pp0 unit "$junos-interface-unit" family family],
[edit interfaces interface-name unit logical-unit-number family family inet],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]
```

Release Information

Statement introduced in Junos OS Release 9.2.
Support at the `[edit dynamic-profiles profile-name interfaces pp0 unit “$junos-interface-unit” family family]` hierarchy level introduced in Junos OS Release 10.1.
Support at the `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy level introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Configure the interface address.

Options

`ip-address`—IPv4 address of the interface.

`ipv6-address`—IPv6 address of the interface. When configuring an IPv6 address on a dynamically created interface, use the `$junos-ipv6-address` dynamic variable.

Required Privilege

Level

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

Related Documentation

- “Configuring the Protocol Family,” in Junos OS Network Interfaces Library for Routing Devices.
- Junos OS Administration Library for Routing Devices
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
**description (Interfaces)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>description text;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit interfaces interface-name], [edit interfaces interface-name unit logical-unit-number], [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a textual description of the interface or the logical unit. Any descriptive text you include is displayed in the output of the show interfaces commands, and is also exposed in the ifAlias Management Information Base (MIB) object. It has no effect on the operation of the interface on the router or switch. The textual description can also be included in the extended DHCP relay option 82 Agent Circuit ID suboption.</td>
</tr>
<tr>
<td>Options</td>
<td>text—Text to describe the interface. If the text includes spaces, enclose the entire text in quotation marks.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>interface—To view this statement in the configuration, interface-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
| Related Documentation | • Configuring Interface Description  
• Adding a Logical Unit Description to the Configuration on page 2299  
• Configuring Gigabit Ethernet Interfaces (CLI Procedure)  
• Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286  
• Configuring Gigabit and 10-Gigabit Ethernet Interfaces  
• Enabling and Disabling Insertion of Option 82 Information on page 1303  
• Junos OS Network Interfaces Library for Routing Devices  
• Example: Connecting Access Switches to a Distribution Switch on page 2083 |
**description (VLANs)**

**Syntax**  
description text-description;

**Hierarchy Level**  
[edit vlans vlan-name]

**Release Information**  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Option text-description enhanced from supporting up to 128 characters to supporting up to 256 characters in Junos OS Release 10.2 for EX Series switches.

**Description**  
Provide a textual description of the VLAN. The text has no effect on the operation of the VLAN or switch.

**Options**  
text-description—Text to describe the interface. It can contain letters, numbers, and hyphens (-) and can contain 256 characters. If the text includes spaces, enclose the entire text in quotation marks.

**Required Privilege**  
* system—To view this statement in the configuration.  
* system-control—To add this statement to the configuration.

**Related Documentation**

- show vlans
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073
- Understanding Bridging and VLANs on EX Series Switches on page 2049
filter (VLANs)

Syntax  
filter (input | output) filter-name;

Hierarchy Level  
[edit vlans vlan-name]

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Apply a firewall filter to traffic coming into or exiting from the VLAN.

Default  
All incoming traffic is accepted unmodified to the VLAN, and all outgoing traffic is sent unmodified from the VLAN.

Options  
filter-name — Name of a firewall filter defined in a filter statement.

  • input — Apply a firewall filter to VLAN ingress traffic.
  • output — Apply a firewall filter to VLAN egress traffic.

Required Privilege Level  
system—To view this statement in the configuration.

  system-control—To add this statement to the configuration.

Related Documentation  
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Firewall Filters for EX Series Switches Overview on page 4088
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
global-mac-table-aging-time

**Syntax**

```
global-mac-table-aging-time seconds;
```

**Hierarchy Level**

```
[edit protocols l2-learning]
```

**Release Information**

Statement introduced in Junos OS Release 9.2.
Support for logical systems added in Junos OS Release 9.6.

**Description**

Configure the timeout interval for entries in the MAC table.

**Default**

300 seconds

**Options**

`seconds`—Time elapsed before MAC table entries are timed out and entries are deleted from the table.

**Range:** For MX Series routers: 10 through 1 million; for EX Series switches: 60 through 1 million

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring the MAC Table Timeout Interval
- Configuring MAC Table Aging (CLI Procedure) on page 2123

---

global-no-mac-learning

**Syntax**

```
global-no-mac-learning;
```

**Hierarchy Level**

```
[edit protocols l2-learning]
```

**Release Information**

Statement introduced in Junos OS Release 9.2.
Support for logical systems added in Junos OS Release 9.6.

**Description**

Disable MAC learning on the entire device.

**Default**

MAC learning is enabled.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Disabling Layer 2 Learning and Forwarding
## interface (MVRP)

| Syntax       | interface (all | interface-name) {  
|             | disable;      |
|             | join-timer milliseconds;  
|             | leave-timer milliseconds;  
|             | leaveall-timer (milliseconds | seconds);  
|             | registration (forbidden | normal);  
|             } |

| Hierarchy Level | [edit protocols mvrp] |
|                | [edit protocols mvrp] |

| Release Information | Statement introduced in Junos OS Release 10.0 for EX Series switches. |
| Description         | Specify interfaces on which to configure Multiple VLAN Registration Protocol (MVRP). |
| Default             | By default, MVRP is disabled. |
| Options             | all—All interfaces on the switch. |
|                     | interface-name—Names of interface to be configured for MVRP. |

The remaining statements are explained separately.

| Required Privilege Level | routing—To view this statement in the configuration.  
|                         | routing-control—To add this statement to the configuration. |

| Related Documentation   | Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches  
|                         | Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096  
|                         | Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)  
|                         | Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure ) on page 2126 |
interface-mac-limit

Syntax

interface-mac-limit limit {
  packet-action action;
}

Hierarchy Level

[edit bridge-domains bridge-domain-name bridge-options],
[edit bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name switch-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name switch-options interface interface-name],
[edit logical-systems logical-system-name switch-options interface interface-name],
[edit logical-systems logical-system-name switch-options],
[edit logical-systems logical-system-name switch-options interface interface-name],
[edit logical-systems logical-system-name switch-options interface interface-name interface interface-name],
[edit logical-systems logical-system-name switch-options],
[edit logical-systems logical-system-name switch-options interface interface-name],
[edit logical-systems logical-system-name switch-options interface interface-name]
[edit vlans vlan-name switch-options],
[edit vlans on page 2136 vlan-name switch-options],
[edit vlans on page 2136 vlan-name switch-options interface interface-name]

Release Information

Statement introduced in Junos OS Release 8.4.
Support for the switch-options statement added in Junos OS Release 9.2.
Support for top-level configuration for the virtual-switch type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.
Support for logical systems added in Junos OS Release 9.6.
Support at [edit switch-options], [edit switch-options interface interface-name], [edit vlans vlan-name switch-options], and [edit vlans vlan-name switch-options interface interface-name] hierarchy levels introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at hierarchy levels under [edit vlans vlan-name] introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Description: 
(MX Series routers and EX Series switches) Configure a limit to the number of MAC addresses that can be learned from a bridge domain or VLAN, virtual switch, or set of bridge domains or VLANs.

Default: 
All devices except the EX Series switches: 1024 MAC addresses for each logical interface; EX Series switches: 65,536 MAC addresses for each interface and VLAN.

Options: 
- limit—Maximum number of MAC addresses learned from an interface.
  - Range: 1 through 131,071 MAC addresses per interface, or 1 through 65,535 MAC addresses per interface

The remaining statement is explained separately.

Required Privilege: 
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation: 
- Layer 2 Learning and Forwarding for Bridge Domains Overview
- Layer 2 Learning and Forwarding for VLANs Overview
- Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports
- Configuring MAC Limiting (CLI Procedure) on page 2132
interface-mode

Syntax

interface-mode (access | trunk);

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family bridge],
[edit interfaces interface-name unit logical-unit-number family ethernet-switching],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family bridge]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description

(QFX Series 3500 and 3600 standalone switches)—Determine whether the logical interface accepts or discards packets based on VLAN tags. Specify the trunk option to accept packets with a VLAN ID that matches the list of VLAN IDs specified in the vlan-id or vlan-id-list statement, then forward the packet within the bridge domain or VLAN configured with the matching VLAN ID. Specify the access option to accept packets with no VLAN ID, then forward the packet within the bridge domain or VLAN configured with the VLAN ID that matches the VLAN ID specified in the vlan-id statement.

NOTE: On MX Series routers, if you want IGMP snooping to be functional for a bridge domain, then you should not configure interface-mode and irb for that bridge. Such a configuration commit succeeds, but IGMP snooping is not functional, and a message informing the same is displayed. For more information, see Configuring a Trunk Interface on a Bridge Network.

Options

access—Configure a logical interface to accept untagged packets. Specify the VLAN to which this interface belongs using the vlan-id statement.

trunk—Configure a single logical interface to accept packets tagged with any VLAN ID specified with the vlan-id or vlan-id-list statement.

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation

• Configuring a Logical Interface for Access Mode
• Configuring a Logical Interface for Trunk Mode
• Example: Connecting Access Switches to a Distribution Switch on page 2083
**join-timer (MVRP)**

**Syntax**
```
join-timer milliseconds;
```

**Hierarchy Level**
- For platforms with ELS:
  ```
  [edit protocols mvrp],
  [edit protocols mvrp interface interface-name]
  ```
- For platforms without ELS:
  ```
  [edit protocols mvrp interface (all interface-name)]
  ```

**Release Information**
Statement introduced in Junos OS Release 10.0 for EX Series switches.
Hierarchy level [edit protocols mvrp] introduced in Junos OS Release 13.2X50-D10 (ELS).
(See “Getting Started with Enhanced Layer 2 Software” on page 3 for information about ELS.)

**Description**
Configure the maximum number of milliseconds interfaces must wait before sending Multiple VLAN Registration Protocol (MVRP) protocol data units (PDUs).

Maintain default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP. However, if you choose to change the default values, keep in mind that on an EX Series switch that uses Junos OS with support for ELS, if the timer value set on an interface level is different from the value set on a switch level, then the value on the interface level takes precedence.

**Options**
- `milliseconds`—Number of milliseconds that an interface must wait before sending MVRP PDUs.
- **Default:** 200 milliseconds

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- leave-timer on page 2152
- leaveall-timer on page 2151
- *Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches*
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure ) on page 2126
I3-interface (VLANs)

Syntax  
```
I3-interface I3-interface-name.logical-interface-number {  
  I3-interface-ingress-counting;  
}
```

Hierarchy Level  
```
[edit vlans vlan-name]
```

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Associate a Layer 3 interface with the VLAN. Configure Layer 3 interfaces on trunk ports to allow the interface to transfer traffic between multiple VLANs. Within a VLAN, traffic is bridged, while across VLANs, traffic is routed.

Default  
No Layer 3 (routing) interface is associated with the VLAN.

Options  
```
I3-interface-name.logical-interface-number—For an integrated routing and bridging (IRB) interface, the Layer 3 interface name is irb; for a routed VLAN interface (RVI), the Layer 3 interface name is vlan. Number of the logical interface defined with a `set interfaces vlan unit` command. For the logical interface number, use the same number you configure in the `unit` statement.
```

The remaining statement is explained separately.

Required Privilege Level  
```
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.
```

Related Documentation  
```
• show ethernet-switching interfaces
• show ethernet-switching interface on page 2183
• show vlans
• show vlans on page 2206
• Configuring Routed VLAN Interfaces (CLI Procedure)
• Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
```
leaveall-timer (MVRP)

Syntax

```
leaveall-timer interval;
```

Hierarchy Level

- For platforms with ELS:
  
  ```
  [edit protocols mvrp],
  [edit protocols mvrp interface interface-name]
  ```

- For platforms without ELS:
  
  ```
  [edit protocols mvrp interface (all | interface-name)]
  ```

Release Information

Statement introduced in Junos OS Release 10.0 for EX Series switches.
Hierarchy level [edit protocols mvrp] introduced in Junos OS Release 13.2X50-D10 (ELS).
(See “Getting Started with Enhanced Layer 2 Software” on page 3 for information about ELS.)

Description

For Multiple VLAN Registration Protocol (MVRP), configure the interval at which the LeaveAll state operates on the interface.

Maintain default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP. However, if you choose to change the default values, keep in mind that on an EX Series switch that uses Junos OS with support for ELS, if the timer value set on an interface level is different from the value set on a switch level, then the value on the interface level takes precedence.

Options

- `interval`—Number of seconds or milliseconds between the sending of Leave All messages.
  
  Default: 10 seconds, or 10,000 milliseconds

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- join-timer on page 2149
- leave-timer on page 2152
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) on page 2126
leave-timer (MVRP)

Syntax
leave-timer milliseconds;

Hierarchy Level
- For platforms with ELS:
  [edit protocols mvrp],
  [edit protocols mvrp interface interface-name]
- For platforms without ELS:
  [edit protocols mvrp interface (all | interface-name)]

Release Information

Description
For Multiple VLAN Registration Protocol (MVRP), configure the number of milliseconds the switch retains a VLAN in the Leave state before the VLAN is unregistered. If the interface receives a join message before this timer expires, the VLAN remains registered.

Maintain default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values might cause an imbalance in the operation of MVRP. However, if you choose to change the default values, keep in mind that on an EX Series switch that uses Junos OS with support for ELS, if the timer value set on an interface level is different from the value set on a switch level, then the value on the interface level takes precedence.

Options
milliseconds—Number of milliseconds that the switch retains a VLAN in the Leave state before the VLAN is unregistered. At a minimum, set the leave-timer interval at twice the join-timer interval.

Default: 1000 milliseconds

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- join-timer on page 2149
- leaveall-timer on page 2151
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) on page 2126
mac (Static MAC-Based VLANs)

Syntax

```
mac mac-address {
    next-hop interface-name;
}
```

Hierarchy Level

[edit ethernet-switching-options static vlan vlan-name]

Description

Specify the MAC address to add to the Ethernet switching table.

The remaining statement is explained separately.

Options

- `mac-address`—MAC address

Required Privilege

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure)
**mac-table-size**

**Syntax**

```
mac-table-size limit {
    packet-action drop;
}
```

**Hierarchy Level**

- [edit bridge-domains bridge-domain-name bridge-options],
- [edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options],
- [edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options],
- [edit logical-systems logical-system-name routing-instances routing-instance-name switch-options],
- [edit logical-systems logical-system-name switch-options],
- [edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options],
- [edit routing-instances routing-instance-name switch-options],
- [edit switch-options]

**Release Information**

- Statement introduced in Junos OS Release 8.4.
- Support for the `switch-options` statement added in Junos OS Release 9.2.
- Support for top-level configuration for the `virtual-switch` type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.
- Support for logical systems added in Junos OS Release 9.6.
- Support at the `[edit vlans vlan-name switch-options]` hierarchy level introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Modify the size of the MAC address table for the bridge domain or VLAN, a set of bridge domains or VLANs associated with a trunk port, or a virtual switch.

**Options**

- `limit`—Specify the maximum number of addresses in the MAC address table.
  - **Range:** (EX Series switches only) 16 through 65,535 MAC addresses; (other devices) 16 through 1,048,575 MAC addresses
  - **Default:** (EX Series switches only) 65,536 MAC addresses; (other devices) 5120 MAC addresses

The remaining statement is explained separately.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- [Layer 2 Learning and Forwarding for Bridge Domains Overview](#)
- [Layer 2 Learning and Forwarding for VLANs Overview](#)
- [Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports](#)
- [Layer 2 Learning and Forwarding for VLANs Acting as a Switch for a Layer 2 Trunk Port](#)
- Configuring MAC Limiting (CLI Procedure) on page 2132
members

Syntax

```
members [(all | names | vlan-ids)];
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family ethernet-switching vlan (802.1Q Tagging)]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated with enhanced ? (CLI completion feature) functionality in Junos OS Release 9.5 for EX Series switches.

Description

For trunk interfaces, configure the VLANs that can carry traffic.

TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type ? after vlan or vlans in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

NOTE: The number of VLANs supported per switch varies for each model. Use the configuration-mode command set vlans id vlan-id ? to determine the maximum number of VLANs allowed on a switch. You cannot exceed this VLAN limit because each VLAN is assigned an ID number when it is created. You can, however, exceed the recommended VLAN member maximum.

On an EX Series switch that runs Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style, the maximum number of VLAN members allowed on the switch is 8 times the maximum number of VLANs the switch supports (vmember limit = vlan max * 8). If the switch configuration exceeds the recommended VLAN member maximum, you see a warning message when you commit the configuration. If you ignore the warning and commit such a configuration, the configuration succeeds but you run the risk of crashing the Ethernet switching process (eswd) due to memory allocation failure.

On an EX Series switch that runs Junos OS that supports ELS, the maximum number of VLAN members allowed on the switch is 24 times the maximum number of VLANs the switch supports (vmember limit = vlan max * 24). If the configuration of one of these switches exceeds the recommended VLAN member maximum, a warning message appears in the system log (syslog).

Options

all—Specifies that this trunk interface is a member of all the VLANs that are configured on this switch. When a new VLAN is configured on the switch, this trunk interface automatically becomes a member of the VLAN.
NOTE: Since VLAN members are limited, specifying all could cause the number of VLAN members to exceed the limit at some point.

*names*—Name of one or more VLANs. VLAN IDs are applied automatically in this case.

NOTE: all cannot be a VLAN name.

*vlan-ids*—Numeric identifier of one or more VLANs. For a series of tagged VLANs, specify a range; for example, 10–20 or 10–20 23–30.

NOTE: Each configured VLAN must have a specified VLAN ID to successfully commit the configuration; otherwise, the configuration commit fails.

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- *show ethernet-switching interfaces*
- *show ethernet-switching interface on page 2183*
- *show vlans*
- *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch*
- *Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073*
- *Example: Connecting an Access Switch to a Distribution Switch*
- *Example: Connecting Access Switches to a Distribution Switch on page 2083*
- *Configuring Gigabit Ethernet Interfaces (CLI Procedure)*
- *Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286*
- *Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289*
- *Configuring VLANs for EX Series Switches (CLI Procedure)*
- *Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119*
- *Creating a Series of Tagged VLANs (CLI Procedure)*
- *Understanding Bridging and VLANs on EX Series Switches on page 2049*
- *Junos OS Ethernet Interfaces Configuration Guide*
mvrp

Syntax

```
mvrp { interface interface-name { join-timer milliseconds; leave-timer milliseconds; leaveall-timer seconds; registration (forbidden | normal); } join-timer milliseconds; leave-timer milliseconds; leaveall-timer seconds; no-attribute-length-in-pdu no-dynamic-vlan; traceoptions (Spanning Trees) { file filename <files number > <size size > <world-readable | no-world-readable>; flag <flag > <disable >; } } }
```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

NOTE: If your switch command-line interface (CLI) displays different options for the mvrp statement from the options shown in this document, see mvrp.

Configure Multiple VLAN Registration Protocol (MVRP) on a trunk interface to ensure that the VLAN membership information on the trunk interface is updated as the switch’s access interfaces become active or inactive in the configured VLANs.

NOTE: In Junos OS Release 11.3, MVRP was updated to conform to the IEEE standard 802.1ak. This update might result in compatibility issues in mixed release networks. For details, see “Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)” on page 2126.

The remaining statements are explained separately.

Default MVRP is disabled by default.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096
native-vlan-id

Syntax  native-vlan-id number;

Hierarchy Level  [edit interfaces ge-fpc/pic/port],
[edit interfaces interface-name]

Release Information  Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description  For 1-, 4-, and 8-port Gigabit Ethernet IQ2 and IQ2-E PICs, for 1-port 10-Gigabit Ethernet
IQ2 and IQ2-E PICs configured for 802.1Q flexible VLAN tagging, for all Ethernet interfaces
on MX Series routers, and for aggregated Ethernet interfaces on IQ2 and IQ2-E PICs or
MX Series DPCs, and for 100-Gigabit Ethernet Type 5 PIC with CFP, configure mixed
tagging support for untagged packets on a port. When the native-vlan-id statement is
included with the flexible-vlan-tagging statement, untagged packets are accepted on
the same mixed VLAN-tagged port.

NOTE: Mixed VLAN tagging is not supported on EX Series switches.

The logical interface on which untagged packets are received must be configured with
the same VLAN ID as the native VLAN ID configured on the physical interface. To configure
the logical interface, include the vlan-id statement (matching the native-vlan-id statement
on the physical interface) at the [edit interfaces interface-name unit logical-unit-number]
hierarchy level.

When the native-vlan-id statement is included with the interface-mode statement,
untagged packets are accepted and forwarded within the bridge domain or VLAN that
is configured with the matching VLAN ID.

Options  number—VLAN ID number.
Range: (ACX Series routers and EX Series switches) 0 through 4094.

Required Privilege  interface—To view this statement in the configuration.
Level  interface-control—To add this statement to the configuration.

Related Documentation  • Configuring Mixed Tagging Support for Untagged Packets
• Configuring a Logical Interface for Access Mode
• Configuring the Native VLAN Identifier (CLI Procedure) on page 2124
• Understanding Bridging and VLANs on EX Series Switches on page 2049
• flexible-vlan-tagging
no-attribute-length-in-pdu

**Syntax**

no-attribute-length-in-pdu;

**Hierarchy Level**

[edit protocols mvrp]

**Release Information**

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Include an extra byte in protocol data units (PDUs) sent by the Multiple VLAN Registration Protocol (MVRP). You can disable the extra byte to address a compatibility issue between MVRP in Junos OS Releases 13.2 and later for EX Series switches with support for the Enhanced Layer 2 Software (ELS), which includes the extra byte, and MVRP in Junos OS Releases 11.3 and later for EX Series switches that do not support ELS, which does not include the extra byte. If this compatibility issue arises, the ELS version of MVRP does not recognize PDUs without the extra byte sent by the non-ELS version of MVRP.

You can recognize an MVRP version compatibility issue by observing the switch running the ELS version of MVRP. Because a switch running the ELS version of MVRP cannot interpret an unmodified PDU from a switch running the non-ELS version of MVRP, the switch will not add VLANs from the non-ELS version of MVRP. When you execute the command `show mvrp statistics` in the ELS version of MVRP, the values for `Received Join Empty` and `Received Join In` will incorrectly display zero, even though the value for the `Received MVRP PDUs without error` has been increased. Another indication that MVRP is having a version compatibility issue is that unexpected VLAN activity, such as multiple VLAN creation, takes place on the switch running the ELS version of MVRP.

**Required Privilege Level**

routing—To view this statement in the configuration.

routing control—To add this statement to the configuration.

**Related Documentation**

- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) on page 2126
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches on page 2063
no-dynamic-vlan

Syntax
no-dynamic-vlan;

Hierarchy Level
[edit protocols mvrp]
[edit protocols mvrp]

Release Information
Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description
Disable the dynamic creation of VLANs using Multiple VLAN Registration Protocol (MVRP) for interfaces participating in MVRP.

Dynamic VLAN configuration can be enabled on an interface independent of MVRP. The MVRP dynamic VLAN configuration setting does not override the interface configuration dynamic VLAN configuration setting. If dynamic VLAN creation is disabled on the interface in the interface configuration, no dynamic VLANs are created on the interface, including dynamic VLANs created using MVRP.

This option can be applied globally; it cannot be applied per interface.

Default
If MVRP is enabled, the dynamic creation of VLANs as a result of MVRP protocol exchange messages is enabled.

Required Privilege
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)
- Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) on page 2126
no-gratuitous-arp-request

**Syntax**

no-gratuitous-arp-request;

**Hierarchy Level**

[edit interfaces interface-name]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure the switch not to respond to gratuitous ARP requests. You can disable responses to gratuitous ARP requests on Layer 2 Ethernet switching interfaces, and integrated routing and bridging (IRB) interfaces or routed VLAN interfaces (RVIs). (On EX Series switches that use Junos OS with support for the Enhanced Layer 2 Software (ELS) configuration style, the feature is known as an IRB interface. On EX Series switches that use Junos OS that does not support ELS, the feature is known as an RVI.)

**Default**

Gratuitous ARP responses are enabled on all Ethernet switching interfaces, and IRB interfaces or RVIs.

**Required Privilege Level**

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Proxy ARP on an EX Series Switch on page 2113
- Configuring Proxy ARP (CLI Procedure)
- Configuring Proxy ARP (CLI Procedure) on page 2130
no-mac-learning

Syntax  no-mac-learning;

Hierarchy Level  [edit bridge-domains bridge-domain-name bridge-options],
[edit bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name switch-options],
[edit logical-systems logical-system-name switch-options],
[edit bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name],
[edit routing-instances routing-instance-name protocols evpn],
[edit routing-instances routing-instance-name protocols evpn interface interface-name],
[edit routing-instances routing-instance-name switch-options],
[edit switch-options],
[edit switch-options on page 2027],
[edit switch-options on page 2027 interface interface-name],
[set vlans vlan-name switch-options]

Release Information  Statement introduced in Junos OS Release 8.4.
Support for the switch-options statement added in Junos OS Release 9.2.
Support for top-level configuration for the virtual-switch type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or bridge domain configured within a virtual switch.
Support for logical systems added in Junos OS Release 9.6.
[edit switch-options], [edit switch-options interface interface-name], [edit vlans vlan-name switch-options], and [edit vlans vlan-name switch-options interface interface-name] hierarchy levels introduced in Junos OS Release 12.3 R2 for EX Series switches.
Support for EVPNPs added in Junos OS Release 13.2 for MX 3D Series routers.
Hierarchy levels [edit switch-options interface interface-name] and [edit vlans vlan-name switch-options] introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  For MX Series routers and EX Series switches, disable MAC learning for a virtual switch, for a bridge domain or VLAN, for a specific logical interface in a bridge domain or VLAN, or for a set of bridge domains or VLANs associated with a Layer 2 trunk port. On platforms that support EVPNPs, you can disable MAC learning on an EVPN.
NOTE: When MAC learning is disabled for a VPLS routing instance, traffic is not load balanced and only one of the equal-cost next hops is used.

<table>
<thead>
<tr>
<th>Default</th>
<th>MAC learning is enabled.</th>
</tr>
</thead>
</table>

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- Configuring EVPN Routing Instances
- Layer 2 Learning and Forwarding for Bridge Domains Overview
- Layer 2 Learning and Forwarding for VLANs Overview
- Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports
- Understanding Bridging and VLANs on EX Series Switches on page 2049
packet-action

Syntax  packet-action action;

Hierarchy Level  [edit bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit bridge-domains bridge-domain-name bridge-options interface-mac-limit limit],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit logical-systems logical-system-name routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit],
[edit logical-systems logical-system-name routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit],
[edit logical-systems logical-system-name switch-options interface-mac-limit limit],
[edit logical-systems logical-system-name switch-options interface-mac-limit limit],
[edit protocols l2-learning global-mac-limit limit],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name switch-options interface interface-name interface-mac-limit limit],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name switch-options interface interface-name interface-mac-limit limit],
[edit routing-instances routing-instance-name protocols evpn interface-mac-limit limit],
[edit routing-instances routing-instance-name protocols evpn interface interface-name interface-mac-limit limit],
[edit routing-instances routing-instance-name protocols evpn mac-table-size limit],
[edit routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit],
[edit routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit],
[edit switch-options interface interface-name interface-mac-limit limit],
[edit switch-options interface interface-name interface-mac-limit limit],
[edit switch-options interface interface-name interface-mac-limit limit],
[edit switch-options interface interface-name interface-mac-limit limit],
[edit switch-options interface interface-name interface-mac-limit limit],
[edit switch-options on page 2027 interface interface-name interface-mac-limit limit],
[edit vlans vlan-name switch-options interface interface-name interface-mac-limit limit],
[edit vlans vlan-name switch-options interface-mac-limit limit],
[edit vlans vlan-name switch-options mac-table-size limit]
[edit vlans on page 2136 vlan-name switch-options interface-mac-limit limit],
[edit vlans on page 2136 vlan-name switch-options interface-mac-limit limit],
[edit vlans on page 2136 vlan-name switch-options mac-table-size limit]
[edit vlans on page 2136 vlan-name switch-options mac-table-size limit]

Release Information  Statement introduced in Junos OS Release 8.4.
Support for the switch-options statement added in Junos OS Release 9.2.
Support for top-level configuration for the virtual-switch type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy

Description Specify the action taken when packets with new source MAC addresses are received after the MAC address limit is reached. If this statement is not configured, packets with new source MAC addresses are forwarded by default.

Default Disabled. The default is for packets for new source MAC addresses to be forwarded after the MAC address limit is reached.

Options drop—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses.

drop-and-log—(EX Series switches only) Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

log—(EX Series switches only) Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

none—(EX Series switches only) Forward packets with new source MAC addresses, and learn the new source MAC address.

shutdown—(EX Series switches only) Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.

Required Privilege Level routing—to view this statement in the configuration.

routing-control—to add this statement to the configuration.
Related Documentation

- Configuring EVPN Routing Instances
- Configuring MAC Limiting (CLI Procedure) on page 2132
- Configuring Persistent MAC Learning (CLI Procedure) on page 4032
- Layer 2 Learning and Forwarding for Bridge Domains Overview
- Layer 2 Learning and Forwarding for VLANs Overview
- Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports
- Layer 2 Learning and Forwarding for VLANs Overview
- Layer 2 Learning and Forwarding for VLANs Acting as a Switch for a Layer 2 Trunk Port
**proxy-arp**

**Syntax**
```
proxy-arp (restricted | unrestricted);
```

**Hierarchy Level**
```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.6 for EX Series switches.
**restricted** added in Junos OS Release 10.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

**Description**
For Ethernet interfaces only, configure the router or switch to respond to any ARP request, as long as the router or switch has an active route to the ARP request’s target address.

**NOTE:** You must configure the IP address and the inet family for the interface when you enable proxy ARP.

**Default**
Proxy ARP is not enabled. The router or switch responds to an ARP request only if the destination IP address is its own.

**Options**
- **none**—The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address.
- **restricted**—(Optional) The router or switch responds to ARP requests in which the physical networks of the source and target are different and does not respond if the source and target IP addresses are in the same subnet. The router or switch must also have a route to the target IP address.
- **unrestricted**—(Optional) The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address.

**Default:** unrestricted

**Required Privilege Level**
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**
- Configuring Restricted and Unrestricted Proxy ARP on page 2333
- Configuring Proxy ARP (CLI Procedure)
- Configuring Proxy ARP (CLI Procedure) on page 2130
- Example: Configuring Proxy ARP on an EX Series Switch on page 2113
- Configuring Gratuitous ARP on page 2331
**redundant-trunk-group**

**Syntax**
```
redundant-trunk-group {
  group name {
    interface interface-name <primary>;
    interface interface-name;
    preempt-cutover-timer seconds;
  }
}
```

**Hierarchy Level**
- For platforms with ELS:
  [edit switch-options]
- For platforms without ELS:
  [edit ethernet-switching-options]

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.
(See “Getting Started with Enhanced Layer 2 Software” on page 3 for information about ELS.)

**Description**
Configure a primary link and secondary link on trunk ports. If the primary link fails, the secondary link automatically takes over without waiting for normal spanning-tree protocol convergence. You can configure a maximum of 16 redundant trunk groups on most standalone switches or on Virtual Chassis. The EX8200 switch and EX8200 Virtual Chassis, however, support up to 254 redundant trunk groups.

The remaining statements are explained separately.

**Required Privilege Level**
- **system**—To view this statement in the configuration.
- **system–control**—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring Redundant Trunk Links for Faster Recovery*
- *Example: Configuring Redundant Trunk Links for Faster Recovery on page 2108*
registration

Syntax registration (forbidden | normal);

Hierarchy Level [edit protocols mvrp interface (all | interface-name)],
[edit protocols mvrp interface interface-name]

Release Information Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description Specifies the Multiple VLAN Registration Protocol (MVRP) registration mode for the interface if MVRP is enabled.

Default normal

Options forbidden—The interface or interfaces do not register and do not participate in MVRP.

normal—The interface or interfaces accept MVRP messages and participate in MVRP.

Required Privilege Level routing—To view this statement in the configuration.

route-control—To add this statement to the configuration.

Related Documentation • Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)

• Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure) on page 2126
**vlan (802.1Q Tagging)**

**Syntax**

```
vlan {
    members [(all | names | vlan-ids)];
}
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family ethernet-switching]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Bind an 802.1Q VLAN tag ID to a logical interface.

The remaining statement is explained separately.

**Required Privilege Level**

- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**Related Documentation**

- `show ethernet-switching interfaces`
- `show ethernet-switching interface on page 2183`
- *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
- *Configuring Routed VLAN Interfaces (CLI Procedure)*
- *Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122*
- *Understanding Bridging and VLANs on EX Series Switches on page 2049*
- *Junos OS Ethernet Interfaces Configuration Guide*
**vlan-id (802.1Q Tagging)**

**Syntax**  
`vlan-id number;`

**Hierarchy Level**  
`[edit vlans vlan-name]`

**Release Information**  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Configure an 802.1Q tag to apply to all traffic that originates on the VLAN.

The number zero is reserved for priority tagging and the number 4095 is also reserved.

**Default**  
If you use the default factory configuration, all traffic originating on the VLAN is untagged and has a VLAN identifier of 1.

**Options**  
`number` — VLAN tag identifier

**Range:**

- 1 through 4094 (all switches except EX8200 Virtual Chassis)
- 1 through 4092 (EX8200 Virtual Chassis only)

**Default:** 1

**Required Privilege Level**  
`system`—To view this statement in the configuration.

`system-control`—To add this statement to the configuration.

**Related Documentation**

- Example: Setting Up Bridging with Multiple VLANs for EX Series Switches
- Example: Connecting Access Switches to a Distribution Switch on page 2083
- Example: Configuring a Private VLAN on a Single EX Series Switch
- Example: Configuring a Private VLAN Spanning Multiple EX Series Switches
- Creating a Private VLAN on a Single EX Series Switch (CLI Procedure)
- Creating a Private VLAN Spanning Multiple EX Series Switches (CLI Procedure)
vlan-id-list

**Syntax**

```bash
vlan-id-list [vlan-id-numbers ];
```

**Hierarchy Level**

- `edit bridge-domains bridge-domain-name`
- `edit logical-systems logical-system-name bridge-domains bridge-domain-name`
- `edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name`
- `edit routing-instances routing-instance-name bridge-domains bridge-domain-name`
- `edit interfaces interface-name unit 0`
- `edit vlans vlan-name`

**Release Information**

Statement introduced in Junos OS Release 9.4.
Support for logical systems added in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

Specify a VLAN identifier list to use for a bridge domain or VLAN in trunk mode.

Specify the `trunk` option in the `interface-mode` statement to accept packets with a VLAN ID that matches the list of VLAN IDs specified in the `vlan-id-list` statement to forward the packet within the bridge domain or VLAN configured with the matching VLAN ID. Specify the `access` option to accept packets with no VLAN ID to forward the packet within the bridge domain or VLAN configured with the VLAN ID that matches the VLAN ID specified in the `vlan-id` statement.

**Options**

- `vlan-id-numbers`—Valid VLAN identifiers. You can combine individual numbers with range lists including a hyphen.
  
  **Range:** 0 through 4095

  **NOTE:** On EX Series switches, the range is 0 through 4094.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring a Bridge Domain
- Configuring a VLAN
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
- Configuring VLAN Identifiers for Bridge Domains and VPLS Routing Instances
- Configuring VLAN Identifiers for VLANs and VPLS Routing Instances
vlans

Syntax

vlans {
  vlan-name {
    description text-description;
    dot1q-tunneling {
      customer-vlans (id | range)
      layer2-protocol-tunneling all | protocol-name {
        drop-threshold number;
        shutdown-threshold number;
      }
    }
    filter input filter-name;
    filter output filter-name;
    interface interface-name [
      egress;
      ingress;
      mapping (native (push | swap) | policy | tag (push | swap));
      pvlan-trunk;
    ]
    isolation-id id-number;
    l3-interface l3-interface-name.logical-interface-number;
    l3-interface-ingress-counting layer-3-interface-name;
    mac-limit limit action action;
    mac-table-aging-time seconds;
    no-local-switching;
    no-mac-learning;
    primary-vlan vlan-name;
    vlan-id number;
    vlan-prune;
    vlan-range vlan-id-low~vlan-id-high;
  }
}

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure VLAN properties on EX Series switches. The following configuration guidelines apply:

- Only private VLAN (PVLAN) firewall filters can be used when the VLAN is enabled for Q-in-Q tunneling.
- An S-VLAN tag is added to the packet if the VLAN is Q-in-Q-tunneled and the packet is arriving from an access interface.
- You cannot use a firewall filter to assign an integrated routing and bridging (IRB) interface or a routed VLAN interface (RVI) to a VLAN.
- VLAN assignments performed using a firewall filter override all other VLAN assignments.

Options vlan-name—Name of the VLAN. The name can include letters, numbers, hyphens (-), and periods (.) and can contain up to 255 characters long.
The remaining statements are explained separately.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- *Configuring VLANs for EX Series Switches (CLI Procedure)*
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
- *Configuring Q-in-Q Tunneling (CLI Procedure)*
- Creating a Series of Tagged VLANs (CLI Procedure)
- *Configuring Routed VLAN Interfaces (CLI Procedure)*
- Configuring Routed VLAN Interfaces (CLI Procedure) on page 2122
- *Understanding Bridging and VLANs on EX Series Switches on page 2049*
CHAPTER 40

Administration

- Routine Monitoring on page 2177
- Operational Commands on page 2182

Routine Monitoring

- Verifying That Virtual Routing Instances Are Working on page 2177
- Verifying Integrated Routing and Bridging Interface Status and Statistics on page 2178
- Verifying That MVRP Is Working Correctly on page 2180
- Verifying That Proxy ARP Is Working Correctly on page 2181

Verifying That Virtual Routing Instances Are Working

**Purpose**
After creating a virtual routing instance, make sure it is set up properly.

**Action**

1. Use the `show route instance` command to list all of the routing instances and their properties:

   ```
   user@switch> show route instance
   Instance          Type                  Primary RIB             Active/holddown/hidden
   master            forwarding           inet.0                  3/0/0
   __juniper_private1__ forwarding
   __juniper_private1__.inet.0                  1/0/3
   __juniper_private2__ forwarding
   instance1         forwarding
   r1                virtual-router       r1.inet.0               1/0/0
   r2                virtual-router       r2.inet.0               1/0/0
   ```

2. Use the `show route forwarding-table` command to view the forwarding table information for each routing instance:

   ```
   user@switch> show route forwarding-table
   Routing table: r1.inet
   Internet:
   ```
<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>539</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>perm</td>
<td>0</td>
<td>dscd</td>
<td>537</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.1.1.0/24</td>
<td>ifdn</td>
<td>0</td>
<td>rslv</td>
<td>579</td>
<td>ge-0/0/3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.1.1.0/32</td>
<td>iddn</td>
<td>0</td>
<td>recv</td>
<td>577</td>
<td>ge-0/0/3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.1.1.1/32</td>
<td>user</td>
<td>0</td>
<td>rjct</td>
<td>539</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.1.1.1/32</td>
<td>intf</td>
<td>0</td>
<td>locl</td>
<td>578</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.1.1.1/32</td>
<td>iddn</td>
<td>0</td>
<td>locl</td>
<td>578</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>103.1.1.255/32</td>
<td>iddn</td>
<td>0</td>
<td>bcst</td>
<td>576</td>
<td>ge-0/0/3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>perm</td>
<td>0</td>
<td>mdsc</td>
<td>538</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>224.0.0.1/32</td>
<td>perm</td>
<td>0</td>
<td>mcst</td>
<td>534</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>255.255.255.255/32</td>
<td>perm</td>
<td>0</td>
<td>bcst</td>
<td>535</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Meaning**
The output confirms that the virtual routing instances are created and the links are up and displays the routing table information.

**Related Documentation**
- Configuring Virtual Routing Instances (CLI Procedure) on page 2125
- Example: Using Virtual Routing Instances to Route Among VLANs on EX Series Switches on page 2093

### Verifying Integrated Routing and Bridging Interface Status and Statistics

**Purpose**
Determine status information and traffic statistics for integrated routing and bridging (IRB) interfaces.

**Action**
Display IRB interfaces and their current states:
```bash
user@switch> show interfaces irb terse
Interface  Admin  Link  Proto    Local                 Remote
irb        up    up      inet     111.111.111.1/24
irb.111    up    up      inet     111.111.111.1/24
...
```

Display Layer 2 VLANs, including any tags assigned to the VLANs and the interfaces associated with the VLANs:
```bash
user@switch> show vlans
Routing instance  VLAN name  Tag  Interfaces
default-switch    irb        101  ge-0/0/18.0
default-switch    support    111  ge-0/0/18.0
...
```

Display Ethernet switching table entries for the VLAN that is attached to the IRB interface:
```bash
user@switch> show ethernet-switching table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)
Routing instance : default-switch
Vlan Name          MAC address          MAC flags          Age Logical interface
```
Display the ingress-counting statistics of an IRB interface with either the `show interfaces irb detail` command or the `show interfaces irb extensive` command. Ingress counting is displayed as **Input bytes** and **Input packets** and egress counting is displayed as **Output bytes** and **Output packets** under **Transit Statistics**.

```
user@switch> show interfaces irb.111 detail
```

Logical interface irb.111 (Index 65) (SNMP ifIndex 503) (HW Token 100) (Generation 131)
Flags: SNMP-Traps 0x4000  Encapsulation: ENET2
Bandwidth: 1000mbps
Routing Instance: default-switch Bridging Domain: irb+111
Traffic statistics:
  Input bytes: 17516756
  Output bytes: 411764
  Input packets: 271745
  Output packets: 8256
Local statistics:
  Input bytes: 3240
  Output bytes: 411764
  Input packets: 54
  Output packets: 8256
Transit statistics:
  Input bytes: 17513516 0 bps
  Output bytes: 0 0 bps
  Input packets: 271745 0 pps
  Output packets: 0 0 pps
Protocol inet, MTU: 1514, Generation: 148, Route table: 0
Flags: None
Addresses, Flags: iS-Preferred  Is-Primary
  Destination: 50.1.1/24, Local: 50.1.1.1, Broadcast: 50.1.1.255, Generation: 136

**Meaning**
- `show interfaces irb terse` displays a list of interfaces, including IRB interfaces, and their current states (up, down).
- `show vlans` displays a list of VLANs, including any tags assigned to the VLANs and the interfaces associated with the VLANs.
- `show ethernet-switching table` displays the Ethernet switching table entries, including VLANs attached to the IRB interface.
- `show interfaces irb detail` displays IRB interface ingress counting as **Input Bytes** and **Input Packets** under **Transit Statistics**.

**Related Documentation**
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
Verifying That MVRP Is Working Correctly

### Purpose

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see *Verifying That MVRP Is Working Correctly*. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

After configuring your EX Series switch to participate in MVRP, verify that the configuration is properly set and that MVRP messages are being sent and received on your switch.

### Action

1. Confirm that MVRP is enabled on your switch.

    ```
    user@switch> show mvrp
    MVRP configuration for routing instance 'default-switch'
    MVRP dynamic VLAN creation : Enabled
    MVRP BPDU MAC address      : Customer bridge group (01-80-C2-00-00-21)
    MVRP timers (ms)
        Interface       Join   Leave  LeaveAll
        xe-0/1/1         200    1000     10000
    ```

2. Confirm that MVRP messages are being sent and received on your switch.

    ```
    user@switch> show mvrp statistics
    MVRP statistics for routing instance 'default-switch'

    Interface name                  : xe-0/1/1
    VLAN IDs registered             : 117
    Sent MVRP PDUs                  : 118824
    Received MVRP PDUs without error: 118848
    Received MVRP PDUs with error   : 0
    Transmitted Join Empty          : 5229
    Transmitted Leave All           : 2
    Received Join In                : 11884924
    Transmitted Leave               : 888
    Transmitted Join In             : 1835
    Transmitted Empty               : 93606408
    Transmitted Leave In            : 13780024
    Transmitted New                 : 2692
    Received Leave All              : 118761
    Received Leave                  : 97
    Received In                     : 3869
    Received Empty                  : 828
    Received Join Empty             : 2020152
    Received New                    : 224
    ...                             
    ```

### Meaning

The output of `show mvrp` shows that interface xe-0/1/1 is enabled for MVRP participation.

The output for `show mvrp statistics` confirms that MVRP messages are being transmitted and received on interface xe-0/1/1.
NOTE: You can identify an MVRP compatibility issue by observing the output from this command. If Received Join Empty and Received Join In incorrectly display zero, even though the value for Received MVRP PDUs without error has been increased, you are probably running different versions of Junos OS on the switches in this network. Another indication that MVRP is having a version problem is that unexpected VLAN activity, such as multiple VLAN creation, takes place on the switch running the earlier release version. To remedy these problems, see “Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)” on page 2126.

Related Documentation
- Example: Configuring Automatic VLAN Administration Using MVRP on EX Series Switches on page 2096
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches on page 2063

Verifying That Proxy ARP Is Working Correctly

Purpose Verify that the switch is sending proxy ARP messages.

Action List the system statistics for ARP:

```
user@switch> show system statistics arp
arp:
90060 datagrams received
34 ARP requests received
610 ARP replies received
2 resolution request received
0 unrestricted proxy requests
0 restricted proxy requests
0 received proxy requests
0 unrestricted proxy requests not proxied
0 restricted proxy requests not proxied
0 datagrams with bogus interface
0 datagrams with incorrect length
0 datagrams for non-IP protocol
0 datagrams with unsupported op code
0 datagrams with bad protocol address length
0 datagrams with bad hardware address length
0 datagrams with multicast source address
0 datagrams with multicast target address
0 datagrams with my own hardware address
0 datagrams for an address not on the interface
0 datagrams with a broadcast source address
294 datagrams with source address duplicate to mine
89113 datagrams which were not for me
0 packets discarded waiting for resolution
0 packets sent after waiting for resolution
309 ARP requests sent
35 ARP replies sent
0 requests for memory denied
0 requests dropped on entry
0 requests dropped during retry
```
Meaning

The statistics show that two proxy ARP requests were received. The unrestricted proxy requests not proxied and restricted proxy requests not proxied fields indicate that all the unproxied ARP requests received have been proxied by the switch.

Related Documentation

- Configuring Proxy ARP
- Configuring Proxy ARP (CLI Procedure) on page 2130
**show ethernet-switching interface**

**Syntax**
```
show ethernet-switching interface
<brief | detail | extensive>
<intface-name>
```

**Release Information**
Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**
(MX Series routers and EX Series switches only) Display Layer 2 learning information for all the interfaces.

**Options**
- **none**—Display Ethernet-switching information for all interfaces.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **interface-name**—(Optional) Display Ethernet-switching information for the specified interface.

**Required Privilege Level**
view

**List of Sample Output**
show ethernet-switching interface ae10.0 on page 2184

**Output Fields**
Table 272 on page 2183 describes the output fields for the `show ethernet-switching interface` command. Output fields are listed in the approximate order in which they appear.

**Table 272: show ethernet-switching interface Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
</tr>
<tr>
<td>VLAN members</td>
<td>VLANs associated with this interface.</td>
</tr>
<tr>
<td>Tag</td>
<td>VLAN ID.</td>
</tr>
<tr>
<td>MAC limit</td>
<td>Number of MAC addresses that can be associated with the interface.</td>
</tr>
<tr>
<td>STP state</td>
<td>Spanning tree protocol (STP) state.</td>
</tr>
<tr>
<td>Logical interface flags</td>
<td>Status of Layer 2 learning properties for each interface:</td>
</tr>
<tr>
<td></td>
<td>• DL—MAC learning is disabled.</td>
</tr>
<tr>
<td></td>
<td>• LH—MAC interface limit has been reached.</td>
</tr>
<tr>
<td></td>
<td>• AD—Packets are dropped after the MAC interface limit is reached.</td>
</tr>
<tr>
<td></td>
<td>• DN—The MAC interface is down.</td>
</tr>
<tr>
<td>Tagging</td>
<td>Tagging state of the VLAN.</td>
</tr>
</tbody>
</table>
**Sample Output**

```bash
show ethernet-switching interface ae10.0
```

Logical Interface Flags  (DL - disable learning, AD - packet action drop,  
LH - MAC limit hit, DN - interface down)

<table>
<thead>
<tr>
<th>Logical interface</th>
<th>Vlan members</th>
<th>TAG</th>
<th>MAC limit</th>
<th>STP</th>
<th>Logical interface flags</th>
<th>Tagging</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae10.0</td>
<td></td>
<td>8192</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>701</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>702</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>703</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>704</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>705</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>706</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>707</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>708</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN70..</td>
<td>709</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN71..</td>
<td>710</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN71..</td>
<td>711</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN71..</td>
<td>712</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN71..</td>
<td>713</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN71..</td>
<td>714</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN71..</td>
<td>715</td>
<td>1024</td>
<td>Forwarding</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

[...output truncated...]

*Copyright © 2013, Juniper Networks, Inc.*
### show ethernet-switching table

**Syntax**

```plaintext
show ethernet-switching table
  <brief | count | detail | extensive | summary>
  <address>
  <instance instance-name>
  <interface interface-name>
  isid isid
  <logical-system logical-system-name>
  <persistent-learning (interface interface-name | mac mac-address)>
  <address>
  <vlan-id (all-vlan | vlan-id)>
  <vlan-name (all | vlan-name)>
```

**Release Information**

Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Options *logical-system*, *persistent-learning*, and *summary* introduced in Junos OS Release 13.2X50-D10 (ELS).

**Description**

NOTE: If your EX Series switch CLI displays different options for the `show ethernet-switching table` command from the options shown in this document, then see `show ethernet-switching table`.

(MX Series routers and EX Series switches only) Display Layer 2 MAC address information.

**Options**

- **none**—Display all learned Layer 2 MAC address information.
- **brief | count | detail | extensive | summary**—(Optional) Display the specified level of output.
- **address**—(Optional) Display the specified learned Layer 2 MAC address information.
- **instance instance-name**—(Optional) Display learned Layer 2 MAC addresses for the specified routing instance.
- **interface interface-name**—(Optional) Display learned Layer 2 MAC addresses for the specified interface.
- **isid isid**—(Optional) Display learned Layer 2 MAC addresses for the specified ISID.
- **logical-system logical-system-name**—(Optional) Display Ethernet-switching statistics information for the specified logical system.
- **persistent-learning (interface interface-name | mac mac-address)**—(Optional) Display dynamically learned MAC addresses that are retained despite device restarts and interface failures for a specified interface, or information about a specified MAC address.
- **vlan-id (all-vlan | vlan-id)**—(Optional) Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.
**vlan-name** *(all | vlan-name)*—*(Optional)* Display learned Layer 2 MAC addresses for all VLANs or for the specified VLAN.

**Additional Information**
When Layer 2 protocol tunneling is enabled, the tunneling MAC address 01:00:0c:cd:cd:d0 is installed in the MAC table. When the Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunk Protocol (VTP) is configured for Layer 2 protocol tunneling on an interface, the corresponding protocol MAC address is installed in the MAC table.

**Required Privilege Level**
view

**List of Sample Output**
show ethernet-switching table on page 2187
show ethernet-switching table brief on page 2188
show ethernet-switching table count on page 2189
show ethernet-switching table extensive on page 2190

**Output Fields**
Table 273 on page 2186 describes the output fields for the **show ethernet-switching table** command. Output fields are listed in the approximate order in which they appear.

Table 273: show ethernet-switching table Output fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>VLAN name</td>
<td>Name of the VLAN.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address or addresses learned on a logical interface.</td>
</tr>
<tr>
<td>MAC flags</td>
<td>Status of MAC address learning properties for each interface:</td>
</tr>
<tr>
<td></td>
<td>• S—Static MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• D—Dynamic MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• L—Locally learned MAC address is configured.</td>
</tr>
<tr>
<td></td>
<td>• SE—MAC accounting is enabled.</td>
</tr>
<tr>
<td></td>
<td>• NM—Non-configured MAC.</td>
</tr>
<tr>
<td></td>
<td>• R—Locally learned MAC address is configured.</td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
</tr>
<tr>
<td>MAC count</td>
<td>Number of MAC addresses learned on the specific routing instance or interface.</td>
</tr>
<tr>
<td>Learning interface</td>
<td>Name of the logical interface on which the MAC address was learned.</td>
</tr>
<tr>
<td>Learning VLAN</td>
<td>VLAN ID of the routing instance or VLAN in which the MAC address was learned.</td>
</tr>
<tr>
<td>Layer 2 flags</td>
<td>Debugging flags signifying that the MAC address is present in various lists.</td>
</tr>
<tr>
<td>Epoch</td>
<td>Spanning-tree-protocolepoch number identifying when the MAC address was learned. Used for debugging.</td>
</tr>
</tbody>
</table>
### Table 273: show ethernet-switching table Output fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td>Sequence number assigned to this MAC address. Used for debugging.</td>
</tr>
<tr>
<td>Learning mask</td>
<td>Mask of the Packet Forwarding Engines where this MAC address was learned. Used for debugging.</td>
</tr>
<tr>
<td>IPC generation</td>
<td>Creation time of the logical interface when this MAC address was learned. Used for debugging.</td>
</tr>
</tbody>
</table>

### Sample Output

**show ethernet-switching table**

```
user@host> show ethernet-switching table
MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
Routing instance : default-switch
Vlan   MAC         MAC     Age     Logical
  name  address     flags   interface
VLAN101 88:e0:f3:bb:07:f0 D        -   ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
Routing instance : default-switch
Vlan   MAC         MAC     Age     Logical
  name  address     flags   interface
VLAN102 88:e0:f3:bb:07:f0 D        -   ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
Routing instance : default-switch
Vlan   MAC         MAC     Age     Logical
  name  address     flags   interface
VLAN103 88:e0:f3:bb:07:f0 D        -   ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)
Routing instance : default-switch
Vlan   MAC         MAC     Age     Logical
  name  address     flags   interface
VLAN104 88:e0:f3:bb:07:f0 D        -   ae20.0
```
VLAN1101       00:1f:12:32:f5:c1   D             -   ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan                MAC                 MAC         Age    Logical
name                address             flags              interface

VLAN1102            00:1f:12:32:f5:c1   D             -   ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan                MAC                 MAC         Age    Logical
name                address             flags              interface

VLAN1103            00:1f:12:32:f5:c1   D             -   ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan                MAC                 MAC         Age    Logical
name                address             flags              interface

VLAN1104            00:1f:12:32:f5:c1   D             -   ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan                MAC                 MAC         Age    Logical
name                address             flags              interface

VLAN1105            00:1f:12:32:f5:c1   D             -   ae0.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan                MAC                 MAC         Age    Logical
name                address             flags              interface

VLAN1106            00:1f:12:32:f5:c1   D             -   ae0.0

[...output truncated...]

show ethernet-switching table brief

user@host>  show ethernet-switching table brief

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
          SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan                MAC                 MAC         Age    Logical
name                address             flags              interface

VLAN1101            88:e0:f3:bb:07:f0   D             -   ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan name    MAC address        MAC flags         Age    Logical interface
VLAN102     88:e0:f3:bb:07:f0   D             -   ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan name    MAC address        MAC flags         Age    Logical interface
VLAN103     88:e0:f3:bb:07:f0   D             -   ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan name    MAC address        MAC flags         Age    Logical interface
VLAN104     88:e0:f3:bb:07:f0   D             -   ae20.0

MAC flags (S - static MAC, D - dynamic MAC, L - locally learned
SE - statistics enabled, NM - non configured MAC, R - remote PE MAC)

Routing instance : default-switch
Vlan name    MAC address        MAC flags         Age    Logical interface
VLAN1101    00:1f:12:32:f5:c1   D             -   ae0.0

[...output truncated...]

show ethernet-switching table count

test@host> show ethernet-switching table count
0 MAC address learned in routing instance default-switch VLAN VLAN1000 ae26.0:1000

1 MAC address learned in routing instance default-switch VLAN VLAN101 ae20.0:101

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID  MAC count  Static MAC count
  101            1          0

1 MAC address learned in routing instance default-switch VLAN VLAN102 ae20.0:102

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID  MAC count  Static MAC count
  102            1          0

1 MAC address learned in routing instance default-switch VLAN VLAN103 ae20.0:103

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID  MAC count  Static MAC count
  103            1          0
MAC address learned in routing instance default-switch VLAN VLAN104
  ae20.0:104

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID  MAC count  Static MAC count
  104              1                 0

MAC address learned in routing instance default-switch VLAN VLAN105
  ae20.0:105

MAC address learned in routing instance default-switch VLAN VLAN106
  ae20.0:106

MAC address learned in routing instance default-switch VLAN VLAN107
  ae20.0:107

MAC address learned in routing instance default-switch VLAN VLAN108
  ae20.0:108

MAC address learned in routing instance default-switch VLAN VLAN109
  ae20.0:109

MAC address learned in routing instance default-switch VLAN VLAN110
  ae20.0:110

MAC address learned in routing instance default-switch VLAN VLAN1101
  ae0.0:1101

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID  MAC count  Static MAC count
  1101              1                 0

MAC address learned in routing instance default-switch VLAN VLAN1102
  ae0.0:1102

MAC address count per learn VLAN within routing instance:
  Learn VLAN ID  MAC count  Static MAC count
  1102              1                 0

[...output truncated...]

show ethernet-switching table extensive

user@host> show ethernet-switching table extensive

MAC address: 88:e0:f3:bb:07:f0
  Routing instance: default-switch
  VLAN ID: 101
    Learning interface: ae20.0
    Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
    Epoch: 0  Sequence number: 2
    Learning mask: 0x00000008

MAC address: 88:e0:f3:bb:07:f0
  Routing instance: default-switch
  VLAN ID: 102
    Learning interface: ae20.0
    Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
    Epoch: 0  Sequence number: 2
    Learning mask: 0x00000008
MAC address: 88:e0:f3:bb:07:f0  
Routing instance: default-switch  
VLAN ID: 103  
Learning interface: ae20.0  
Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd  
Epoch: 0  
Sequence number: 2  
Learning mask: 0x00000008  

MAC address: 88:e0:f3:bb:07:f0  
Routing instance: default-switch  
VLAN ID: 104  
Learning interface: ae20.0  
Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd  
Epoch: 0  
Sequence number: 2  
Learning mask: 0x00000008  

MAC address: 00:1f:12:32:f5:c1  
Routing instance: default-switch  
VLAN ID: 1101  
Learning interface: ae0.0  
Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd  
Epoch: 0  
Sequence number: 2  
Learning mask: 0x00000008  

MAC address: 00:1f:12:32:f5:c1  
Routing instance: default-switch  
VLAN ID: 1102  
Learning interface: ae0.0  
Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd  
Epoch: 0  
Sequence number: 2  
Learning mask: 0x00000008  

MAC address: 00:1f:12:32:f5:c1  
Routing instance: default-switch  
VLAN ID: 1103  
Learning interface: ae0.0  
Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd  
Epoch: 0  
Sequence number: 2  
Learning mask: 0x00000008  

MAC address: 00:1f:12:32:f5:c1  
Routing instance: default-switch  
VLAN ID: 1104  
Learning interface: ae0.0  
Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd  
Epoch: 0  
Sequence number: 2  
Learning mask: 0x00000008
show interfaces irb

Syntax

```
show interfaces irb
<brief | detail | extensive | terse>
<descriptions>
<media>
<routing-instance instance-name>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Command introduced in Junos OS Release 13.2 for the QFX Series

Description

Display integrated routing and bridging interfaces information.

Options

- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about network interfaces.
- `routing-instance instance-name`—(Optional) Display information for the interface with the specified SNMP index.
- `snmp-index snmp-index`—(Optional) Display information for the interface with the specified SNMP index.

Additional Information

Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another VLAN that has a Layer 3 protocol configured.

Required Privilege

Level

`view`

List of Sample Output

- `show interfaces irb extensive on page 2196`
- `show interfaces irb snmp-index on page 2197`

Output Fields

Table 274 on page 2192 lists the output fields for the `show interfaces irb` command. Output fields are listed in the approximate order in which they appear.

Table 274: show interfaces irb Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Possible values are described in the “Enabled Field” section under Common Output Fields Description.</td>
<td></td>
</tr>
</tbody>
</table>
Table 274: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proto</td>
<td>Protocol configured on the interface.</td>
<td>terse</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Type</td>
<td>Physical interface type.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source: Internal or External. Always unspecified on IRB interfaces.</td>
<td>detail extensive brief</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running. Always unspecified on IRB interfaces.</td>
<td>detail extensive brief</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under Common Output Fields Description.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under Common Output Fields Description.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>Link type</td>
<td>Physical interface link type: full duplex or half duplex.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Links Flags” section under Common Output Fields Description.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Physical Info</td>
<td>Physical interface information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Hardware address</td>
<td>MAC address of the hardware.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Alternate link address</td>
<td>Backup address of the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hours:minutes:seconds timezone (hours:minutes:seconds ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>


Table 274: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets</strong>—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>physical interface if IPv6 statistics tracking is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets</strong>—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>whose meaning might not be obvious:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC. If the interface is saturated, this number increments once for every</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Framing errors</strong>—Number of packets received with an invalid frame checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Giants</strong>—Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Policed discards</strong>—Number of frames that the incoming packet match code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>discarded because they were not recognized or not of interest. Usually, this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>whose meaning might not be obvious:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>up</strong>. This number does not normally increment quickly, increasing only when</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the cable is unplugged, the far-end system is powered down and up, or another</td>
<td></td>
</tr>
<tr>
<td></td>
<td>problem occurs. If the number of carrier transitions increments quickly (perhaps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>once every 10 seconds), the cable, the far-end system, or the DPC is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASIC. If the interface is saturated, this number increments once for every</td>
<td></td>
</tr>
<tr>
<td></td>
<td>packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

Logical Interface
### Table 274: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface (which reflects its initialization sequence).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number of the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under Common Output Fields Description.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Speed at which the interface is running.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Routing instance IRB is configured under.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Bridging Domain</td>
<td>Bridging domain IRB is participating in.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Statistics for traffic received from and transmitted to the Routing Engine.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Statistics for traffic transiting the router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the local interface. Possible values are described in the “Protocol Field” section under Common Output Fields Description.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Maximum labels</td>
<td>Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 274: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about address flags. Possible values are described in the &quot;Addresses Flags&quot; section under Common Output Fields Description.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Policer</td>
<td>The policer that is to be evaluated when packets are received or transmitted on the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the &quot;Logical Interface Flags&quot; section under Common Output Fields Description.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

#### Sample Output

**show interfaces irb extensive**

```
user@host> show interfaces irb extensive
  Physical interface: irb, Enabled, Physical link is Up
    Interface index: 129, SNMP ifIndex: 23, Generation: 130
    Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified, Speed: Unspecified
    Device flags : Present Running
    Interface flags: SNMP-Traps
    Link type : Full-Duplex
    Link flags : None
    Physical info : Unspecified
    Hold-times : Up 0 ms, Down 0 ms
    Current address: 02:00:00:00:00:30, Hardware address: 02:00:00:00:00:30
    Alternate link address: Unspecified
    Last flapped : Never
    Statistics last cleared: Never
    Traffic statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
    IPv6 transit statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
    Input errors:
      Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0, Resource errors: 0
    Output errors:
      Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0

  Logical interface irb.0 (Index 68) (SNMP ifIndex 70) (Generation 143)
    Flags: Hardware-Down SNMP-Traps 0x4000 Encapsulation: ENET2
    Bandwidth: 1000mbps
    Routing Instance: customer_0 Bridging Domain: bd0
```
Traffic statistics:
  Input  bytes :                    0
  Output bytes :                    0
  Input  packets:                    0
  Output packets:                    0
IPv6 transit statistics:
  Input  bytes :                   0
  Output bytes  :                   0
  Input  packets:                   0
  Output packets:                   0
Local statistics:
  Input  bytes :                    0
  Output bytes :                    0
  Input  packets:                    0
  Output packets:                    0
Transit statistics:
  Input  bytes :                    0  0 bps
  Output bytes :                    0  0 bps
  Input  packets:                    0  0 pps
  Output packets:                    0  0 pps
IPv6 transit statistics:
  Input  bytes :                   0
  Output bytes :                   0
  Input  packets:                   0
  Output packets:                   0
Protocol inet, MTU: 1500, Generation: 154, Route table: 0
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 10.51.1/24, Local: 10.51.1.2, Broadcast: 10.51.1.255,
    Generation: 155
Protocol multiservice, MTU: 1500, Generation: 155, Route table: 0
  Flags: Is-Primary
  Policer: Input: __default_arp_policer

show interfaces irb snmp-index

user@host> show interfaces irb snmp-index 25
Physical interface: irb, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 25
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514
  Device flags : Present Running
  Interface flags: SNMP-Traps
  Link type : Full-Duplex
  Link flags : None
  Current address: 02:00:00:00:00:30, Hardware address: 02:00:00:00:00:30
  Last flapped : Never
  Input packets : 0
  Output packets: 0

Logical interface irb.0 (Index 68) (SNMP ifIndex 70)
  Flags: Hardware-Down SNMP-Traps 0x4000 Encapsulation: ENET2
  Bandwidth: 1000mbps
  Routing Instance: customer_0 Bridging Domain: bd0
  Input packets : 0
  Output packets: 0
Protocol inet, MTU: 1500
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 10.51.1/24, Local: 10.51.1.2, Broadcast: 10.51.1.255
Protocol multiservice, MTU: 1500
  Flags: Is-Primary
### show mvrp

**Syntax**

```
show mvrp
```

**Release Information**

Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Display Multiple VLAN Registration Protocol (MVRP) configuration information.

**Required Privilege**

`view`

**Related Documentation**

- `show mvrp applicant-state`
- `show mvrp dynamic-vlan-memberships on page 2200`
- `show mvrp interface`
- `show mvrp registration-state`
- `show mvrp statistics`

**List of Sample Output**

`show mvrp on page 2198`

**Output Fields**

Table 275 on page 2198 lists the output fields for the `show mvrp` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVRPdynamic VLAN creation</td>
<td>Displays whether global MVRP dynamic Virtual LAN (VLAN) creation is <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>MVRP BPDU MAC address</td>
<td>Displays the multicast media access control (MAC) address for MVRP. If configured, the provider MVRP multicast MAC address is used; otherwise, the customer MVRP multicast MAC address is used.</td>
</tr>
<tr>
<td>MVRP timers (ms)</td>
<td>Displays MVRP timer information:</td>
</tr>
<tr>
<td></td>
<td>- <strong>interface</strong>—The interface on which MVRP is configured.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Join</strong>—The maximum number of milliseconds the interfaces must wait before sending VLAN advertisements.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Leave</strong>—The number of milliseconds an interface must wait after receiving a Leave message to remove the interface from the VLAN specified in the message.</td>
</tr>
<tr>
<td></td>
<td>- <strong>LeaveAll</strong>—The interval at which LeaveAll messages are sent on interfaces. LeaveAll messages maintain current MVRP VLAN membership information in the network.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show mvrp
```

```
user@host> show mvrp
```
MVRP configuration for routing instance 'default-switch'

MVRP dynamic VLAN creation : Enabled
MVRP BPDU MAC address      : Customer bridge group (01-80-C2-00-00-21)

MVRP timers (ms)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Join</th>
<th>Leave</th>
<th>LeaveAll</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/2/8</td>
<td>200</td>
<td>800</td>
<td>10000</td>
</tr>
<tr>
<td>ge-11/0/9</td>
<td>200</td>
<td>800</td>
<td>10000</td>
</tr>
<tr>
<td>ge-11/3/0</td>
<td>200</td>
<td>800</td>
<td>10000</td>
</tr>
</tbody>
</table>
**show mvrp dynamic-vlan-memberships**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>show mvrp dynamic-vlan-memberships</th>
</tr>
</thead>
</table>

**Release Information**
Command introduced in Junos OS Release 10.1.
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**
Display all Virtual LANs (VLANs) that have been created dynamically using Multiple VLAN Registration Protocol (MVRP) on the router or switch.

**Required Privilege Level**
clear

**Related Documentation**
- show mvrp on page 2198
- show mvrp applicant-state
- show mvrp interface
- show mvrp registration-state
- show mvrp statistics

**List of Sample Output**
show mvrp dynamic-vlan-memberships on page 2200

**Output Fields**
Table 276 on page 2200 lists the output fields for the show mvrp dynamic-vlan-memberships command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Id</td>
<td>The VLAN ID of the dynamically created VLAN.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The interface or interfaces that are bound to the dynamically created VLAN.</td>
</tr>
</tbody>
</table>

**Sample Output**
show mvrp dynamic-vlan-memberships

```
user@host> show mvrp dynamic-vlan-memberships
MVRP dynamic vlans for routing instance 'default-switch'
(s) static vlan, (f) fixed registration

<table>
<thead>
<tr>
<th>VLAN Id</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 (s)</td>
<td>ge-11/3/0</td>
</tr>
<tr>
<td>200 (s)</td>
<td>ge-11/3/0</td>
</tr>
<tr>
<td>300 (s)</td>
<td></td>
</tr>
</tbody>
</table>
```
show mvrp statistics

Syntax

show mvrp statistics
<interface interface-name>
<routing-instance routing-instance-name>

Release Information

Command introduced in Junos OS Release 13.2X50-D10 (ELS).

Description

Display Multiple VLAN Registration Protocol (MVRP) statistics in the form of Multiple Registration Protocol data unit (MRPDU) messages.

Required Privilege Level

view

Related Documentation

• show mvrp on page 2198
• Verifying That MVRP Is Working Correctly on page 2180

List of Sample Output

show mvrp statistics on page 2202

Output Fields

Table 277 on page 2201 lists the output fields for the show mvrp statistics command. Output fields are listed in the approximate order in which they appear.

Table 277: show mvrp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Interface for which MVRP statistics are displayed.</td>
</tr>
<tr>
<td>VLAN IDs registered</td>
<td>Number of Virtual LAN (VLAN) IDs registered.</td>
</tr>
<tr>
<td>Sent MRP PDUs</td>
<td>Number of MRPDU messages transmitted from the switch.</td>
</tr>
<tr>
<td>Received MRP PDUs without error</td>
<td>Number of MRPDU messages received on the switch.</td>
</tr>
<tr>
<td>Received MRP PDUs with error</td>
<td>Number of invalid MRPDU messages received on the switch.</td>
</tr>
<tr>
<td>Transmitted Join Empty</td>
<td>Number of JoinEmpty messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted Leave All</td>
<td>Number of MRP LeaveAll messages sent from the switch.</td>
</tr>
<tr>
<td>Received Join In</td>
<td>Number of MRP JoinIn messages received on the switch. Either this value or the value for Received Join Empty should increase when the value for Received MRP PDUs without error increases. If this value is not incrementing when it should, you might have a Junos OS release compatibility issue. To resolve the issue, see “Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)” on page 2126.</td>
</tr>
<tr>
<td>Transmitted Join In</td>
<td>Number of MRP JoinIn messages sent from the switch.</td>
</tr>
</tbody>
</table>
Table 277: show mvrp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmitted Empty</td>
<td>Number of MRP Empty messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted Leave</td>
<td>Number of MRP LeaveEmpty messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted In</td>
<td>Number of MRP In messages sent from the switch.</td>
</tr>
<tr>
<td>Transmitted New</td>
<td>Number of New messages transmitted from the switch.</td>
</tr>
<tr>
<td>Received Leave All</td>
<td>Number of LeaveAll messages received on the switch.</td>
</tr>
<tr>
<td>Received Leave</td>
<td>Number of MRP Leave messages received on the switch.</td>
</tr>
<tr>
<td>Received In</td>
<td>Number of MRP In messages received on the switch.</td>
</tr>
<tr>
<td>Received Empty</td>
<td>Number of MRP Empty messages received on the switch.</td>
</tr>
<tr>
<td>Received Join Empty</td>
<td>Number of MRP JoinEmpty messages received on the switch. Either this value or the value for Received Join In should increase when the value for Received MVRP PDUs without error increases. If this value is not incrementing when it should, you might have a Junos OS release compatibility issue. To resolve the issue, see “Configuring Multiple VLAN Registration Protocol (MVRP) (CLI Procedure)” on page 2126.</td>
</tr>
<tr>
<td>Received New</td>
<td>Number of New messages received on the switch.</td>
</tr>
</tbody>
</table>

Sample Output

```
show mvrp statistics

user@host> show mvrp statistics
MVPR statistics for routing instance 'default-switch'

  Interface name : xe-0/1/1
  VLAN IDs registered : 117
  Sent MVRP PDUs : 118824
  Received MVRP PDUs without error : 118848
  Received MVRP PDUs with error : 0
  Transmitted Join Empty : 5229
  Transmitted Leave All : 2
  Received Join In : 11884924
  Transmitted Join In : 1835
  Transmitted Empty : 93606408
  Transmitted Leave : 888
  Transmitted In : 13780024
  Transmitted New : 2692
  Received Leave All : 118761
  Received Leave : 97
  Received In : 3869
  Received Empty : 828
  Received Join Empty : 2020152
  Received New : 224
...
```
show redundant-trunk-group

**Syntax**

```
show redundant-trunk-group <group-name group-name>
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display information about redundant trunk groups.

**Options**

`group-name group-name`—Display information about the specified redundant trunk group.

**Required Privilege**

`view`

**Related Documentation**

- Example: Configuring Redundant Trunk Links for Faster Recovery
- Understanding Redundant Trunk Links on EX Series Switches on page 2068

**List of Sample Output**

`show redundant-trunk-group group-name Group1` on page 2203

**Output Fields**

Table 278 on page 2203 lists the output fields for the `show redundant-trunk-group` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Name of the redundant trunk port group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of an interface belonging to the trunk port group.</td>
</tr>
<tr>
<td>State</td>
<td>Operating state of the interface.</td>
</tr>
<tr>
<td></td>
<td>• Up denotes the interface is up.</td>
</tr>
<tr>
<td></td>
<td>• Down denotes the interface is down.</td>
</tr>
<tr>
<td></td>
<td>• Pri denotes a primary interface.</td>
</tr>
<tr>
<td></td>
<td>• Act denotes an active interface.</td>
</tr>
<tr>
<td>Time of last flap</td>
<td>Date and time at which the advertised link became unavailable, and then, available again.</td>
</tr>
<tr>
<td>Flap count</td>
<td>Total number of flaps since the last switch reboot.</td>
</tr>
</tbody>
</table>

**Sample Output**

`show redundant-trunk-group group-name Group1`

```
user@switch> show redundant-trunk-group group-name Group1
```

<table>
<thead>
<tr>
<th>Group name</th>
<th>Interface</th>
<th>State</th>
<th>Time of last flap</th>
<th>Flap Count</th>
</tr>
</thead>
</table>

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>Group</th>
<th>Interface</th>
<th>State</th>
<th>Description</th>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1</td>
<td>ge-0/0/45.0</td>
<td>UP/Pri/Act</td>
<td>Never</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Group1</td>
<td>ge-0/0/47.0</td>
<td>UP</td>
<td>Never</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
show system statistics arp

Syntax

show system statistics arp

Release Information

Command introduced in Junos OS Release 9.6 for EX Series switches.

Description

Display system-wide Address Resolution Protocol (ARP) statistics.

Required Privilege

view

Level

Related Documentation

• Example: Configuring Proxy ARP on an EX Series Switch on page 2113
• Verifying That Proxy ARP Is Working Correctly on page 2181

show system statistics arp

user@switch> show system statistics arp
arp:
  90060 datagrams received
  34 ARP requests received
  610 ARP replies received
  0 resolution request received
  0 unrestricted proxy requests
  0 restricted proxy requests
  0 received proxy requests
  0 unrestricted proxy requests not proxied
  0 restricted proxy requests not proxied
  0 datagrams with bogus interface
  0 datagrams with incorrect length
  0 datagrams for non-IP protocol
  0 datagrams with unsupported op code
  0 datagrams with bad protocol address length
  0 datagrams with bad hardware address length
  0 datagrams with multicast source address
  0 datagrams with multicast target address
  0 datagrams with my own hardware address
  0 datagrams for an address not on the interface
  0 datagrams with a broadcast source address
  294 datagrams with source address duplicate to mine
  89113 datagrams which were not for me
  0 packets discarded waiting for resolution
  0 packets sent after waiting for resolution
  309 ARP requests sent
  35 ARP replies sent
  0 requests for memory denied
  0 requests dropped on entry
  0 requests dropped during retry
  0 requests dropped due to interface deletion
  0 requests on unnumbered interfaces
  0 new requests on unnumbered interfaces
  0 replies for from unnumbered interfaces
  0 requests on unnumbered interface with non-subnetted donor
  0 replies from unnumbered interface with non-subnetted donor
show vlans

Syntax
show vlans
<brief | detail | extensive>
<instance instance-name>
<logical-system logical-system-name>
<operational>
<vlan-name>
<interface interface-name>

Release Information
Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Option interface introduced in Junos OS Release 13.2X50-D10 (ELS).

Description
NOTE: If your EX Series switch CLI displays different options for the show vlans command from the options shown in this document, see show vlans.

(MX Series routers and EX Series switches only) Display VLAN information.

Options
none—Display information for all VLANs.

brief | detail | extensive—(Optional) Display the specified level of output.

instance instance-name—(Optional) Display information for the specified routing instance.

logical-system logical-system-name—(Optional) Display Ethernet-switching statistics information for the specified logical system.

operational—(Optional) Display information for the operational routing instances.

vlan-name—(Optional) Display information about the specified VLAN.

interface interface-name—(Optional) Display information about the specified interface.

Required Privilege
view

List of Sample Output
show vlans brief on page 2206
show vlans detail on page 2207

Sample Output
show vlans brief

user@host> show vlans brief
Routing instance     VLAN name     Tag     Interfaces
VPLS-1               __VPLS-1__    all     ae1.0
VPLS-2               __VPLS-2__    all     ae3.0
gE-3/1/2.0
vt-3/3/10.1048576
<table>
<thead>
<tr>
<th>Default Switch</th>
<th>VLAN Name</th>
<th>State</th>
<th>Tag</th>
<th>Internal Index</th>
<th>Generation Index</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-switch</td>
<td>VLAN1000</td>
<td></td>
<td>1000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN101</td>
<td></td>
<td>101</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN102</td>
<td></td>
<td>102</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN103</td>
<td></td>
<td>103</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN104</td>
<td></td>
<td>104</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN105</td>
<td></td>
<td>105</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN106</td>
<td></td>
<td>106</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN107</td>
<td></td>
<td>107</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default-switch</td>
<td>VLAN108</td>
<td></td>
<td>108</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[...output truncated...]

```
user@host> show vlans detail
Routing instance: VPLS-1
  VLAN Name: __VPLS-1__                       State: Active
  Tag: all
  Internal index: 2, Generation Index: , Origin: Dynamic
  Interfaces:
    ae1.0,tagged
  Number of interfaces: Tagged 1    , Untagged 0
  Total MAC count: 0

Routing instance: VPLS-2
  VLAN Name: __VPLS-2__                       State: Active
  Tag: all
  Internal index: 3, Generation Index: , Origin: Dynamic
  Interfaces:
    ae3.0,tagged
    ge-3/1/2.0,tagged
    vt-3/3/10.1048576,tagged
  Number of interfaces: Tagged 3    , Untagged 0
  Total MAC count: 4

Routing instance: default-switch
  VLAN Name: VLAN1000                       State: Active
  Tag: 1000
  Internal index: 4, Generation Index: 1, Origin: Static
  Layer 3 interface: irb.1000
  Interfaces:
    ae26.0,tagged,trunk
  Number of interfaces: Tagged 1    , Untagged 0
  Total MAC count: 0

Routing instance: default-switch
  VLAN Name: VLAN101                        State: Active
  Tag: 101
  Internal index: 5, Generation Index: 2, Origin: Static
  Layer 3 interface: irb.101
  Interfaces:
    ae20.0,tagged,trunk
  Number of interfaces: Tagged 1    , Untagged 0
```
Total MAC count: 1

Routing instance: default-switch
   VLAN Name: VLAN102                        State: Active
   Tag: 102
   Internal index: 6, Generation Index: 3, Origin: Static
   Layer 3 interface: irb.102
   Interfaces:
      ae20.0,tagged,trunk
   Number of interfaces: Tagged 1 , Untagged 0
Total MAC count: 1
[...output truncated...]
Part 14

High Availability

- Overview on page 2211
- Configuration on page 2223
- Administration on page 2247
Overview

- High Availability Features Overview on page 2211
- Power Management Overview on page 2213
- VRRP Overview on page 2219

High Availability Features Overview

- High Availability Features for EX4300 Switches Overview on page 2211

High Availability Features for EX4300 Switches Overview

*High availability refers to the hardware and software components that provide redundancy and reliability for network communications. This topic covers the following high availability features of Juniper Networks EX4300 Ethernet Switches:*

- Redundant Routing Engines on page 2211
- Virtual Chassis on page 2212
- VRRP on page 2212
- Graceful Routing Engine Switchover on page 2212
- Link Aggregation on page 2213

Redundant Routing Engines

Redundant Routing Engines are two Routing Engines that are installed in a switch or a Virtual Chassis. When a switch has two Routing Engines, one functions as the master, while the other stands by as a backup in case the master Routing Engine fails. When a Virtual Chassis has two Routing Engines, the switch in the master role functions as the master Routing Engine and the switch in the backup role functions as the backup Routing Engine. Redundant Routing Engines are supported on Juniper Networks EX4300 Ethernet Switches configuring into a Virtual Chassis.

The master Routing Engine receives and transmits routing information, builds and maintains routing tables, communicates with interfaces and Packet Forwarding Engine components of the switch, and has full control over the control plane of the switch.

The backup Routing Engine stays in sync with the master Routing Engine in terms of protocol states, forwarding tables, and so forth. If the master becomes unavailable, the backup Routing Engine takes over the functions that the master Routing Engine performs.
Network reconvergence takes place more quickly on switches and on Virtual Chassis with redundant Routing Engines than on switches and on Virtual Chassis with a single Routing Engine.

Virtual Chassis

A Virtual Chassis is multiple switches connected together that operate as a single network entity. The advantages of connecting multiple switches into a Virtual Chassis include better-managed bandwidth at a network layer, simplified configuration and maintenance because multiple devices can be managed as a single device, a simplified Layer 2 network topology that minimizes or eliminates the need for loop prevention protocols such as Spanning Tree Protocol (STP), and improved fault tolerance and high availability. A Virtual Chassis improves high availability for the following reasons:

- Dual Routing Engine support. A Virtual Chassis automatically has two Routing Engines—the switches in the master and backup routing-engine roles—and, therefore, provides more high availability options than standalone switches. Many high availability features are available for an EX Series Virtual Chassis that are not available on standalone EX Series switches.

- Increased fault tolerance. You increase your fault tolerance options when you configure your EX Series switches into a Virtual Chassis. You can, for instance, configure interfaces into a link aggregation group (LAG) with member interfaces on different member switches in the same Virtual Chassis to ensure network traffic is received by a Virtual Chassis even when a switch or physical interface in the Virtual Chassis fails.

You can configure up to ten EX4300 switches into an EX4300 Virtual Chassis. See “Understanding EX4300 Virtual Chassis” on page 4459.

VRRP

You can configure Virtual Router Redundancy Protocol (VRRP) for IP and IPv6 on most switch interfaces, including Gigabit Ethernet interfaces, high-speed uplink interfaces, and logical interfaces. When VRRP is configured, the switches act as virtual routing platforms. VRRP enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routing platforms share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routing platforms is the master (active) and the others are backups. If the master routing platform fails, one of the backup routing platforms becomes the new master, providing a virtual default routing platform and enabling traffic on the LAN to be routed without relying on a single routing platform. Using VRRP, a backup switch can take over a failed default switch within a few seconds. This is done with minimum loss of VRRP traffic and without any interaction with the hosts.

Graceful Routing Engine Switchover

You can configure graceful Routing Engine switchover (GRES) on a switch with redundant Routing Engines or on a Virtual Chassis, allowing control to switch from the master Routing Engine to the backup Routing Engine with minimal interruption to network communications. When you configure GRES, the backup Routing Engine automatically synchronizes with the master Routing Engine to preserve kernel state information and
forwarding state. Any updates to the master Routing Engine are replicated to the backup Routing Engine as soon as they occur. If the kernel on the master Routing Engine stops operating, the master Routing Engine experiences a hardware failure, or the administrator initiates a manual switchover, mastership switches to the backup Routing Engine.

When the backup Routing Engine assumes mastership in a redundant failover configuration (that is, when GRES is not enabled), the Packet Forwarding Engines initialize their state to the boot state before they connect to the new master Routing Engine. In contrast, in a GRES configuration, the Packet Forwarding Engines do not reinitialize their state, but resynchronize their state to that of the new master Routing Engine. The interruption to traffic is minimal.

**Link Aggregation**

You can combine multiple physical Ethernet ports to form a logical point-to-point link, known as a link aggregation group (LAG) or bundle. A LAG provides more bandwidth than a single Ethernet link can provide. Additionally, link aggregation provides network redundancy by load-balancing traffic across all available links. If one of the links should fail, the system automatically load-balances traffic across all remaining links. In a Virtual Chassis, LAGs can be used to load-balance network traffic between member switches, which increases high availability by ensuring that network traffic is received by the Virtual Chassis even if a single interface fails for any reason.

The number of Ethernet interfaces you can include in a LAG and the number of LAGs you can configure on a switch depend on the switch model. For information about LAGs, see “Understanding Aggregated Ethernet Interfaces and LACP” on page 2272.

**Related Documentation**

- For more information about high availability features, see the *Junos OS High Availability Configuration Guide*.
- *EX Series Virtual Chassis Overview*
- Understanding EX4300 Virtual Chassis on page 4459
- Understanding VRRP on EX Series Switches on page 2220
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272

**Power Management Overview**

* Understanding Power Management on EX Series Switches on page 2213

**Understanding Power Management on EX Series Switches**

The power management feature for Juniper Networks Ethernet Switches helps ensure that normal operation of the system is not disrupted because of insufficient power to the switch. For example:

- Power management ensures that operating line cards continue to receive power if a user installs a new line card in an operating switch when power is insufficient for both the new and existing line cards.
• Power management reserves a certain amount of power to power supply redundancy, so that if a power supply fails, the switch can continue to operate normally. If power management must use some of this reserved power to provide power to switch components, it raises an alarm to indicate that power supply redundancy no longer exists and that normal operations might be disrupted if a power supply fails.

• If power supply failure requires power management to power down some components, it does so gracefully by powering down line cards and PoE ports in the order specified by the user.

Power management manages power to switch components by employing a power budget policy. In its power budget policy, power management:

• Budgets power for each installed switch component that requires power. With the exception of PoE power for line cards that support PoE, the amount that power management budgets for each component is the maximum power that component might consume under worst case operating conditions. For example, for the fan tray, power management budgets the amount of power required to run the fans at their maximum speed setting, even if the current fan speed is much lower.

• Reserves a set amount of power for power supply redundancy. In its default configuration, power management manages the switch for \( N+1 \) power redundancy, which ensures uninterrupted system operation if one power supply fails. For example, if a switch has four online 3000 W power supplies, power management reserves 3000 W in its power budget policy for redundancy. It allocates the remaining 9000 W to normal operating power.

• Specifies the rules under which components receive power. These rules are designed to ensure the least disruption to switch operation under conditions of insufficient power. For example, power management provides power to core system components, such as the Routing Engines, before it provides power to line cards.

You can configure certain aspects of power management’s budget policy, specifically:

• The power priority of individual line cards. By assigning different power priorities to the line cards, you can determine which line cards are more likely to receive power in the event of insufficient power.

• The power redundancy configuration. The default power redundancy configuration is \( N+1 \); you can optionally configure \( N+N \). For example, if you have deployed two independent AC power feeds to the switch, configure \( N+N \) redundancy. When you configure power management for \( N+N \) redundancy, it reserves the appropriate amount of power in its power budget and reports insufficient power conditions accordingly.

These configurable items are discussed further in:

• Power Priority of Line Cards on page 2215
• Power Supply Redundancy on page 2218
Power Priority of Line Cards

The power priority of line cards determines:

• The order in which line cards are allocated power
• The order in which line cards that support PoE are allocated power for PoE
• How power is reallocated in cases of changes in power availability or demand in an operating switch

NOTE: On EX6200 switches, the four 10-Gigabit Ethernet SFP+ uplink ports on a Switch Fabric and Routing Engine (SRE) module are treated like a line card in the power budget.

This section covers:

• How a Line Card’s Power Priority Is Determined on page 2215
• Line Card Priority and Line Card Power on page 2215
• Line Card Priority and PoE Power on page 2216
• Line Card Priority and Changes in the Power Budget on page 2216

How a Line Card’s Power Priority Is Determined

Using the CLI, you can assign a explicit power priority to a line-card slot. If more than one slot has the same assigned priority, the power priority is determined by slot number, with the lowest-numbered slots receiving power first.

By default, all slots in an EX8200 switch are assigned the lowest priority. Thus if you do not explicitly assign priorities to slots, power priority is determined by slot number, with slot 0 having the highest priority.

In an EX6200 switch, all slots are assigned the lowest priority, except for the slots containing an SRE module. Slots containing an SRE module are automatically assigned the highest priority. This means that the line cards that represent the 10-Gigabit Ethernet SFP+ ports on SRE modules have the highest priority among the line cards.

Line Card Priority and Line Card Power

When an EX6200 or EX8200 switch is powered on, power management allocates power to components according to its power budget policy. After power management has allocated power to the base chassis components, it allocates the remaining available power to the line cards. It powers on the line cards in priority order until all line cards are powered on or the available power (including reserved power, if necessary) is exhausted. Thus if available power is exhausted before all line cards receive power, higher-priority cards are powered on while lower-priority cards remain powered off.

A lower-priority card might receive power while a higher-priority card does not if the remaining available power is sufficient to power on the lower-priority card but not the higher-priority card. For example, if a line card requiring 450 W is in a higher-priority slot
than line card requiring 330 W, the line card requiring 330 W receives the power if there is less than 450 W but more than 330 W remaining in the power budget.

Line cards that have been administratively taken offline are not allocated power.

**NOTE:** Because power management does not allocate power to a line card that has been administratively taken offline, a line card that has been taken offline in an EX6200 or EX8200 switch is not automatically brought online when you commit a configuration. You must explicitly use the `request chassis fpc slot slot-number online` command to bring a line card online that was taken offline previously. This behavior differs from other platforms running Juniper Networks Junos operating system (Junos OS), which automatically bring an offline FPC online when you commit a configuration.

If power management cannot power on a line card because of insufficient power, it raises a major (red) alarm.

**Line Card Priority and PoE Power**

After all line cards have been powered on, power management allocates any remaining available power, including reserved power, to the PoE power budgets of line cards that have PoE ports. Power management allocates PoE power to line cards in the order of power priority. If enough power is available, a line card receives its full PoE power budget before power management allocates PoE power to the next highest-priority line card. If not enough power is available, a line card receives partial PoE power and lower-priority line cards receive no PoE power.

If power management is unable to allocate enough power to meet the PoE power budget for a line card, it logs a message to the system log.

The default PoE power budget for a line card is the amount of power needed to supply the maximum supported power to all PoE ports. In cases where powered devices do not require the maximum power or in which some PoE ports are not used for powered devices, you can configure a smaller PoE power budget for a line card. By configuring a smaller PoE power budget, you make more power available for the PoE power budgets of lower-priority line cards.

You can also configure the power priority of the PoE ports on a line card. If power management is unable to allocate enough power to a line card to meet its PoE power budget, the line card PoE controller will turn off power to PoE ports in reverse priority order as required to meet the reduced power allocation.

See “Configuring PoE (CLI Procedure)” on page 3942 for more information on how to configure the PoE power budget for a line card and how to configure PoE port priorities.

**Line Card Priority and Changes in the Power Budget**

In an operating switch, power management dynamically reallocates power in response to changes in power availability or demand or changes in line card priority. Power management uses line card priority to determine how to reallocate power in response to the following events:
• A power supply fails, is removed, or is taken offline:
  • If power is insufficient to meet the PoE power allocations of all PoE line cards, power
    management deallocates PoE power from the line cards in reverse priority order
    until power is sufficient to meet the remaining PoE power allocations.
  • If power is insufficient to meet the base (non-PoE) power requirements of all the
    line cards, all PoE power is deallocated. If, after the deallocation of PoE power, power
    is still not sufficient, power management turns off line cards in reverse priority order
    until power is sufficient for the remaining line cards.

• A new line card is inserted or a line card is brought online:
  • If the line card supports PoE and there is insufficient power to meet its PoE power
    budget, PoE power is reallocated from lower-priority line cards. If not enough PoE
    power can be reallocated from lower-priority line cards, the new line card receives
    a partial PoE power allocation.
  • If there is insufficient power to power on the new line card, PoE power is removed
    from PoE line cards in reverse priority order until the new line card can be powered
    on.
  • If the removal of all PoE power is insufficient to free up enough power to power on
    the line card, the line card remains powered off and the PoE line cards continue to
    receive their PoE power allocations. To minimize disruption on an operating switch,
    lower-priority line cards are not turned off to provide power to the new line card.
    However, if you restart the switch, power management reruns the current power
    budget policy and powers line cards on or off based on their priority. As a result, line
    cards receive power strictly by priority order and previously operating line cards might
    no longer receive power.

• A new power supply is brought online:
  • Any line cards that were powered off because of insufficient power are powered on
    in priority order.
  • After all line cards are powered on, remaining power is allocated to the PoE power
    budgets of line cards in priority order.

• A line card is removed or taken offline, freeing up power:
  • Any line cards that were powered down because of insufficient power are powered
    on in priority order.
  • After all line cards are powered on, any remaining power is allocated to the PoE
    power budgets of line cards in priority order.

• A user changes the assigned power priority of one or more line cards when power is
  insufficient to meet the power budget:
  • PoE power to the line cards is reallocated based on the new power priorities.
  • Base power allocation to the line cards is not changed—in other words, power
    management does not power down line cards that had been receiving power because
    they are now a lower priority. However, if you restart the switch, power management
    reruns the current power budget policy and powers line cards on or off based on their
priority. As a result, line cards receive power strictly by priority order and previously operating line cards might no longer receive power.

If, because of insufficient power, power management reduces or eliminates the PoE power budget for a line card, it logs a message to the system log. If power management must power down a line card because of insufficient power, it raises a major (red) alarm.

**Power Supply Redundancy**

By default, power management in EX Series switches is configured to manage the power supplies for $N+1$ redundancy, in which one power supply is held in reserve for backup if one of the other power supplies is removed or fails.

You can configure power management to manage the power supplies for $N+N$ redundancy. In $N+N$ redundancy, power management holds $N$ power supplies in reserve for backup. For example, if your switch has six power supplies and you configure $N+N$ redundancy, power management makes three power supplies available for normal operating power and reserves three power supplies for redundancy ($3+3$). If you have an odd number of power supplies, power management allocates one more power supply to normal operating power than to redundant power. For example, if you have five power supplies, the $N+N$ configuration is $3+2$.

Given the same number of power supplies, an $N+N$ configuration usually provides less normal operating power than an $N+1$ configuration because the $N+N$ configuration holds more power in reserve for backup. Table 279 on page 2218 shows the effect on normal operating power in $N+1$ and $N+N$ configurations.

**Table 279: Available Operating Power in N+1 and N+N Redundancy Configurations**

<table>
<thead>
<tr>
<th>Number of Power Supplies at $n$ W Each</th>
<th>Normal Operating Power in $N+1$ Configuration</th>
<th>Normal Operating Power in $N+N$ Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$1 \times (n \ W)$</td>
<td>$1 \times (n \ W)$</td>
</tr>
<tr>
<td>3</td>
<td>$2 \times (n \ W)$</td>
<td>$2 \times (n \ W)$</td>
</tr>
<tr>
<td>4</td>
<td>$3 \times (n \ W)$</td>
<td>$2 \times (n \ W)$</td>
</tr>
<tr>
<td>5 (EX8200 switches only)</td>
<td>$4 \times (n \ W)$</td>
<td>$3 \times (n \ W)$</td>
</tr>
<tr>
<td>6 (EX8200 switches only)</td>
<td>$5 \times (n \ W)$</td>
<td>$3 \times (n \ W)$</td>
</tr>
</tbody>
</table>

To compensate for the reduced normal operating power, power management on EX8200 switches allocates less power to the chassis in an $N+N$ configuration than in an $N+1$ configuration. This reduction in allocated chassis power allows a switch in an $N+N$ configuration to power more line cards than it could without the reduction. For the EX8208 switch, the power allocated for the chassis is reduced to 1200 W from 1600 W; for the EX8216 switch, it is reduced to 1800 W from 2400 W.
NOTE: To achieve the reduction in allocated chassis power in an EX8200 switch, power management reduces the maximum fan speed to 60 percent in an N+N configuration from 80 percent in an N+1 configuration. Because the maximum fan speed is reduced, it is possible that a line card that overheats would be shut down sooner in an N+N configuration than in an N+1 configuration.

On EX6200 switches, the same amount of power is allocated for the chassis in N+N configurations as in N+1 configurations.

Power management automatically recalculates the reserved power and normal operating power as power supplies go online or offline. For example, if you have an N+N configuration with three online 2000 W power supplies, power management allocates 2000 W to reserved power. If you bring a fourth 2000 W power supply online, power management then allocates 4000 W to reserved power. If a power supply goes offline again, power management once again allocates 2000 W to reserved power.

When power is insufficient to meet the budgeted power requirements, power management raises alarms as follows:

- A minor (yellow) alarm is raised when insufficient power exists to maintain the configured N+1 or N+N power reserves, but all line cards are still receiving their base and PoE power allocations. If this condition persists for 5 minutes, the alarm becomes a major (red) alarm. Even though operation of the switch is unaffected in this condition, you should remedy it as quickly as possible because a power supply failure might cause a disruption in switch operation.

- A major (red) alarm is raised when insufficient power exists to provide all the line cards with their base and PoE power allocations. One or more PoE ports might be down or one or more line cards might be down.

Power management clears all alarms when sufficient power is available to meet normal operating and reserved power requirements.

Related Documentation
- Understanding Alarm Types and Severity Levels on EX Series Switches on page 669
- Configuring the Power Priority of Line Cards (CLI Procedure)
- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
- Verifying Power Configuration and Use on page 2247

VRRP Overview
- Understanding VRRP on EX Series Switches on page 2220
Understanding VRRP on EX Series Switches

Juniper Networks EX Series Ethernet Switches support the Virtual Router Redundancy Protocol (VRRP) and VRRP for IPv6. This topic covers:

- Overview of VRRP on EX Series Switches on page 2220
- Examples of VRRP Topologies on page 2221

Overview of VRRP on EX Series Switches

You can configure the Virtual Router Redundancy Protocol (VRRP) or VRRP for IPv6 on Gigabit Ethernet interfaces, 10-Gigabit Ethernet interfaces, and logical interfaces on EX Series switches. When VRRP is configured, the switches act as virtual routing platforms. VRRP enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routing platforms share the IP address corresponding to the default route configured on the hosts. At any time, one of the VRRP routing platforms is the master (active) and the others are backups. If the master routing platform fails, one of the backup routing platforms becomes the new master, providing a virtual default routing platform and enabling traffic on the LAN to be routed without relying on a single routing platform. Using VRRP, a backup EX Series switch can take over a failed default switch within a few seconds. This is done with minimum loss of VRRP traffic and without any interaction with the hosts. Virtual Router Redundancy Protocol is not supported on management interfaces.

VRRP for IPv6 provides a much faster switchover to an alternate default routing platform than IPv6 Neighbor Discovery (ND) procedures. VRRP for IPv6 does not support the `authentication-type` or `authentication-key` statements.

**NOTE:** Do not confuse the VRRP master and backup routing platforms with the master and backup member switches of a Virtual Chassis configuration. The master and backup members of a Virtual Chassis configuration compose a single host. In a VRRP topology, one host operates as the master routing platform and another operates as the backup routing platform, as shown in Figure 35 on page 2221.

Switches running VRRP dynamically elect master and backup routing platforms. You can also force assignment of master and backup routing platforms using priorities from 1 through 255, with 255 being the highest priority. In VRRP operation, the default master routing platform sends advertisements to backup routing platforms at regular intervals. The default interval is 1 second. If the backup routing platforms do not receive an advertisement for a set period, the backup routing platform with the highest priority takes over as master and begins forwarding packets.

**NOTE:** Priority 255 cannot be set for routed VLAN interfaces (RVIs).

VRRP is defined in RFC 3768, *Virtual Router Redundancy Protocol*. 
**Examples of VRRP Topologies**

Figure 34 on page 2221 illustrates a basic VRRP topology with EX Series switches. In this example, Switches A, B, and C are running VRRP and together they make up a virtual routing platform. The IP address of this virtual routing platform is **10.10.0.1** (the same address as the physical interface of Switch A).

**Figure 34: Basic VRRP on EX Series Switches**

Figure 35 on page 2221 illustrates a basic VRRP topology using Virtual Chassis configurations. Switch A, Switch B, and Switch C are each composed of multiple interconnected Juniper Networks EX4200 Ethernet Switches. Each Virtual Chassis configuration operates as a single switch, which is running VRRP, and together they make up a virtual routing platform. The IP address of this virtual routing platform is **10.10.0.1** (the same address as the physical interface of Switch A).

**Figure 35: VRRP on Virtual Chassis Switches**
Because the virtual routing platform uses the IP address of the physical interface of Switch A, Switch A is the master VRRP routing platform, while Switch B and Switch C function as backup VRRP routing platforms. Clients 1 through 3 are configured with the default gateway IP address of 10.10.0.1 as the master router, Switch A, forwards packets sent to its IP address. If the master routing platform fails, the switch configured with the higher priority becomes the master virtual routing platform and provides uninterrupted service for the LAN hosts. When Switch A recovers, it becomes the master virtual routing platform again.

Related Documentation

- For more information on VRRP or VRRP for IPv6, see the Junos OS High Availability Configuration Guide.
- High Availability Features for EX Series Switches Overview
- Configuring VRRP for IPv6 (CLI Procedure) on page 2224
CHAPTER 42

Configuration

- Configuration Tasks on page 2223
- Configuration Statements on page 2225

Configuration Tasks

- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
- Configuring VRRP for IPv6 (CLI Procedure) on page 2224

Configuring Power Supply Redundancy (CLI Procedure)

By default, the power management feature in EX Series switches is configured to manage the power supplies for N+1 redundancy, in which one power supply is held in reserve for backup if any one of the other power supplies is removed or fails.

You can configure power management to manage the power supplies for N+N redundancy. For example, to set up your AC power supplies for dual power feed, N+N redundancy is required. In N+N redundancy, power management allocates half of the online power supplies to normal operating power and half to redundant power. If you have an odd number of online power supplies, power management allocates one more power supply to normal operating power than to redundant power.

This topic describes how to configure power management for N+N redundancy and how to revert back to N+1 redundancy if your deployment needs change.

Before you configure power management for N+N redundancy, ensure that you have sufficient power supplies to meet the power requirements of an N+N configuration. Use the `show chassis power-budget-statistics` command to display your current power budget.
NOTE: To allow more power to be available to line cards in an EX8200 switch, power management compensates for the reduced normal operating power in an N+N configuration by allocating less power to the chassis than it does in an N+1 configuration. For the EX8208 switch, the power allocated to the chassis is reduced to 1200 W from 1600 W. For the EX8216 switch, it is reduced to 1800 W from 2400 W. In determining whether you have enough power for an N+N configuration, take this reduction of allocated chassis power into account.

The reduction in allocated chassis power is achieved by reducing the maximum fan speed to 60 percent in an N+N configuration from 80 percent in an N+1 configuration. Because the maximum fan speed is reduced, it is possible that a line card that overheats would be shut down sooner in an N+N configuration than in an N+1 configuration.

On EX6200 switches, the same amount of power is allocated for the chassis in N+N configurations as in N+1 configurations.

To configure N+N redundancy:

```
[edit chassis]
user@switch# set PSU redundancy n-plus-n
```

To revert back to N+1 redundancy:

```
[edit chassis]
user@switch# delete chassis PSU redundancy n-plus-n
```

Related Documentation

- Configuring the Power Priority of Line Cards (CLI Procedure)
- Verifying Power Configuration and Use on page 2247
- Understanding Power Management on EX Series Switches on page 2213

Configuring VRRP for IPv6 (CLI Procedure)

By configuring the Virtual Router Redundancy Protocol (VRRP) on EX Series switches, you can enable hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. You can configure VRRP for IPv6 on Gigabit Ethernet, 10-Gigabit Ethernet, and logical interfaces.

To configure VRRP for IPv6:
1. Configure VRRP group support on interfaces:

   
   ```
   [edit interfaces interface-name unit logical-unit-number family inet6 address address]
   user@switch# set vrrp-inet6-group group-id priority number virtual-inet6-address address virtual-link-local-address ipv6-address
   ```

   You must explicitly define a virtual link local address for each VRRP for IPv6 group.
   Otherwise, when you attempt to commit the configuration, the commit request fails.
   The virtual link local address must be on the same subnet as the physical interface address.

2. If you want to configure the priority order in which this switch functioning as a backup router becomes the master router if the master router becomes nonoperational, configure a priority for this switch:

   ```
   [edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]
   user@switch# set priority number
   ```

3. Specify the interval in milliseconds in which the master router sends advertisement packets to the members of the VRRP group:

   ```
   [edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]
   user@switch# set inet6-advertise-interval milliseconds
   ```

4. By default, a higher-priority backup router preempts a lower-priority master router.

   - To explicitly enable the master router to be preempted:
     ```
     [edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]
     user@switch# set preempt
     ```
   - To prohibit a higher-priority backup router from preempting a lower priority master router:
     ```
     [edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]
     user@switch# set no-preempt
     ```

Related Documentation
- show vrrp on page 2254
- Understanding VRRP on EX Series Switches on page 2220

Configuration Statements

- [edit chassis] Configuration Statement Hierarchy on EX Series Switches on page 2225
- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2227
- [edit protocols vrrp] Hierarchy Level on page 2228

[edit chassis] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit chassis] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
• *Unsupported* statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

* Supported Statements in the [edit chassis] Hierarchy Level on page 2226

**Supported Statements in the [edit chassis] Hierarchy Level**

The following hierarchy shows the [edit chassis] configuration statements supported on EX Series switches:

```plaintext
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
      lACP {
        link-protection non-revertive;
        system-priority system-priority-number
      }
    }
  }
  alarm {
    ethernet {
      link-down (ignore | red | yellow);
    }
    management-ethernet {
      link-down (ignore | red | yellow);
    }
    container-devices {
      device-count device-count-number;
    }
    disk-partition {
      /config {
        level (full | high) {
          free-space (free-space-threshold-value | mb | percent);
        }
      }
      /var {
        level (full | high) {
          free-space (free-space-threshold-value | mb | percent);
        }
      }
    }
    fpc slot-number{
      pic pic-number {
        no-multi-rate;
        q-pic-large-buffer (large-scale | small-scale);
      }
    }
  }
}
```


```c
}
maximum-ecmp maximum-ecmp-routes;
lcd-menu {
  fpc slot-number {
    menu-item menu-name);
    disable;
  }
  pseudowire-service {
    device-count device-count-number;
  }
}
psu {
  redundancy {
    n-plus-n;
  }
  redundancy {
    graceful-switchover;
  }
  slow-pfe-alarm;
}
```

### Related Documentation

- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504
- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
- Configuring the Power Priority of Line Cards (CLI Procedure)
- Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)

### [edit interfaces] Configuration Statement Hierarchy on EX Series Switches

Each of the following topics lists the statements at a subhierarchy of the [edit interfaces] hierarchy:

- [edit interfaces ae] Configuration Statement Hierarchy on EX Series Switches on page 2354
- [edit interfaces et] Configuration Statement Hierarchy on EX Series Switches on page 2360
- [edit interfaces ge] Configuration Statement Hierarchy on EX Series Switches on page 2365
- [edit interfaces interface-range] Configuration Statement Hierarchy on EX Series Switches on page 2371
- [edit interfaces irb] Configuration Statement Hierarchy on EX Series Switches on page 2379
- [edit interfaces lo] Configuration Statement Hierarchy on EX Series Switches on page 2383
- [edit interfaces me] Configuration Statement Hierarchy on EX Series Switches on page 2386

---

Copyright © 2013, Juniper Networks, Inc.
[edit protocols vrrp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems logical-system-name] hierarchy level.

```conf
protocols {
  vrrp {
    asymmetric-hold-time;
    delegate-processing;
    failover-delay milliseconds;
    global-advertisements-threshold advertisement-value;
    skew-timer-disable;
    startup-silent-period seconds;
    traceoptions {
      file <filename> <files number> <match regular-expression> <microsecond-stamp> <size maximum-file-size> <world-readable | no-world-readable>;
      flag <file <flag>
      no-remote-trace;
    }
    version-3;
  }
}
```

Related Documentation

- Notational Conventions Used in Junos OS Configuration Hierarchies
- [edit protocols] Hierarchy Level
- Junos OS Hierarchy and RFC Reference
- Ethernet Interfaces
- Junos OS Network Interfaces Library for Routing Devices
chassis

Syntax

chassis {
  aggregated-devices {
    ethernet (Aggregated Devices) {
      device-count number;
    }
  }
  auto-image-upgrade;
  fpc slot {
    pic pic-number {
      sfplus {
        pic-mode mode;
      }
      power-budget-priority priority;
    }
  }
  lcd-menu {
    fpc slot-number {
      menu-item (menu-name | menu-option) {
        disable;
      }
    }
  }
  nssu {
    upgrade-group group-name {
      fpcs (NSSU Upgrade Groups) (slot-number | [list-of-slot-numbers]);
    }
  }
  psu {
    redundancy {
      n-plus-n (Power Management);
    }
    redundancy {
      graceful-switchover;
    }
  }
}

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure chassis-specific properties for the switch.

The remaining statements are explained separately.

Required Privilege Interface—to view this statement in the configuration.

Level Interface-control—to add this statement to the configuration.
Related Documentation

- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Upgrading Software Using Automatic Software Download
- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504
- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
- Configuring the Power Priority of Line Cards (CLI Procedure)
- Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)
**synchronize**

**Syntax**

synchronize;

**Hierarchy Level**

[edit system commit]

**Release Information**

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 10.4 for EX Series switches.

**Description**

For devices with multiple Routing Engines only. Configure the `commit` command to automatically perform a **commit synchronize** action between dual Routing Engines within the same chassis. The Routing Engine on which you execute the `commit` command (the requesting Routing Engine) copies and loads its candidate configuration to the other (the responding) Routing Engine. Each Routing Engine then performs a syntax check on the candidate configuration file being committed. If no errors are found, the configuration is activated and becomes the current operational configuration on both Routing Engines.

**NOTE:** When you configure nonstop active routing (NSR), you must configure the **commit synchronize** statement. Otherwise, the commit operation fails.

On the TX Matrix router, synchronization only occurs between the Routing Engines within the same chassis. When synchronization is complete, the new configuration is then distributed to the Routing Engines on the T640 routers. That is, the master Routing Engine on the TX Matrix router distributes the configuration to the master Routing Engine on each T640 router. Likewise, the backup Routing Engine on the TX Matrix router distributes the configuration to the backup Routing Engine on each T640 router.

On the TX Matrix Plus router and TX Matrix Plus router with 3D SIBs, synchronization only occurs between the Routing Engines within the switch-fabric chassis and when synchronization is complete, the new configuration is then distributed to the Routing Engines on the line-card chassis (LCC). That is, the master Routing Engine on the TX Matrix Plus router distributes the configuration to the master Routing Engine on each LCC. Likewise, the backup Routing Engine on the TX Matrix Plus router distributes the configuration to the backup Routing Engine on each LCC.

In EX Series Virtual Chassis configurations:

- On EX4200 switches in Virtual Chassis, synchronization occurs between the switch in the master role and the switch in the backup role.
- On EX8200 switches in a Virtual Chassis, synchronization occurs only between the master and backup XRE200 External Routing Engines.

**Options**

- **and-quit**—(Optional) Quit configuration mode if the commit synchronization succeeds.
- **at**—(Optional) Time at which to activate configuration changes.
- **comment**—(Optional) Write a message to the commit log.
force—(Optional) Force a commit synchronization on the other Routing Engine (ignore warnings).

scripts—(Optional) Push scripts to the other Routing Engine.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Synchronizing the Routing Engine Configuration
- Configuring Multiple Routing Engines to Synchronize Committed Configurations Automatically

**failover (Chassis)**

**Syntax**
```
failover {
  on-disk-failure;
  on-loss-of-keepalives;
}
```

**Hierarchy Level**
[edit chassis redundancy]

**Release Information**
Statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**
Specify conditions on the master Routing Engine that cause the backup router to take mastership.

The remaining statements are explained separately.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- graceful-switchover on page 2234
- On Detection of a Hard Disk Error on the Master Routing Engine
- Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)
- High Availability Features for EX Series Switches Overview
## fpc

**Syntax**

```
fpc slot {
    pic pic-number {
        sfpplus {
            pic-mode mode;
        }
        tunnel-port port-number tunnel-services;
    }
    power (off | on);
    power-budget-priority priority;
}
```

**Hierarchy Level**

```
[edit chassis]
```

**Release Information**

Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

On an EX3200 or an EX4200 switch, specify the port of the SFP+ uplink module for which you want to configure the operating mode.

On an EX6200 or an EX8200 switch, specify the line card slot for which you want to assign a power priority.

---

**NOTE:** On an EX6200 switch, you cannot change the power priority of a slot containing a Switch Fabric and Routing Engine (SRE) module. Although the CLI allows you to set a different power priority for the slot, your change does not go into effect, and the power priority remains 0. A message is sent to the system log to inform you that changing the power priority of the slot is unsupported.

---

For generic routing encapsulation (GRE) tunneling, use the `fpc` statement with the `tunnel-port` statement to specify the port on the switch that you want to convert to a GRE tunnel port.

**Options**

- `slot`—Number of the slot:
  - 0—EX3200 and standalone EX4200 switches. The FPC value refers to the switch itself.
  - 0–9—EX4200 switch in a Virtual Chassis configuration. The value corresponds to the switch’s member ID.
  - 0–3 and 6–9—EX6210 switch. The slot is a line card slot.
  - 4–5—The slot is a line card slot or an SRE module slot.
  - 0–7—EX8208 switch. The slot is a line card slot.
  - 0–15—EX8216 switch. The slot is a line card slot.

The remaining statements are explained separately.
graceful-switchover

Syntax  graceful-switchover;

Hierarchy Level  [edit chassis redundancy]


Description  For switches with more than one Routing Engine, including those in a Virtual Chassis, configure the master Routing Engine to switch over gracefully to a backup Routing Engine without interruption to packet forwarding.

Default  Graceful Routing Engine switchover (GRES) is disabled.

Required Privilege Level  interface—To view this statement in the configuration.

Related Documentation  • Example: Configuring Nonstop Active Routing on EX Series Switches
  • Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504
  • Configuring Nonstop Active Routing on EX Series Switches (CLI Procedure)
  • Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)
**hold-time**

**Syntax**

```
hold-time seconds;
```

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id preempt]

**Release Information**

Statement introduced in Junos OS Release 10.0 for EX Series switches.

**Description**

Configure the time in seconds after which a backup router with the highest priority preempts the master router.

**Options**

`seconds`—Hold-time period.

**Required Privilege**

interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring VRRP for IPv6 (CLI Procedure) on page 2224

---

**inet6-advertise-interval**

**Syntax**

```
inet6-advertise-interval milliseconds;
```

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]

**Release Information**

Statement introduced in Junos OS Release 10.0 for EX Series switches.

**Description**

Configure the interval between Virtual Router Redundancy Protocol (VRRP) IPv6 advertisement packets.

**Options**

`milliseconds`—Interval, in milliseconds, between advertisement packets.

**Range:** 100 to 40,000 ms

**Default:** 1 second

**Required Privilege**

interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring VRRP for IPv6 (CLI Procedure) on page 2224
**keepalive-time**

**Syntax**  
keepalive-time seconds;

**Hierarchy Level**  
[edit chassis redundancy]

**Release Information**  
Statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**  
Configure the time period that must elapse before the backup router takes mastership when it detects loss of the keepalive signal.

**Default**  
The on-loss-of-keepalives statement at the [edit chassis redundancy failover] hierarchy level must be included for failover to occur.

When the on-loss-of-keepalives statement is included and graceful Routing Engine switchover is not configured, failover occurs after 300 seconds (5 minutes).

When the on-loss-of-keepalives statement is included and graceful Routing Engine switchover is configured, the keepalive signal is automatically enabled and the failover time is set to 2 seconds.

**Options**  
seconds—Time before the backup router takes mastership when it detects loss of the keepalive signal. The range of values is 2 through 10,000.

**Required Privilege Level**  
interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

**Related Documentation**  
- failover on page 2232
- graceful-switchover on page 2234
- on-loss-of-keepalives
- High Availability Features for EX Series Switches Overview
**n-plus-n (Power Management)**

**Syntax**

```
n-plus-n;
```

**Hierarchy Level**

```
[edit chassis psu redundancy]
```

**Release Information**

Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Configure $N+N$ power supply redundancy for power management on an EX6200 or EX8200 switch.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Power Supply Redundancy (CLI Procedure) on page 2223

**preempt**

**Syntax**

```
(preempt | no-preempt) {
  hold-time seconds;
}
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family inet6 address address
  vrrp-inet6-group group-id]
```

**Release Information**

Statement introduced in Junos OS Release 10.0 for EX Series switches.

**Description**

Configure whether a backup router can preempt a master router:

- **preempt**—Allow the master router to be preempted.
- **no-preempt**—Prohibit the preemption of the master router.

The remaining statement is explained separately.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring VRRP for IPv6 (CLI Procedure) on page 2224
priority

Syntax  

priority number;

Hierarchy Level  

[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-group group-id],  
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]

Release Information  

Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description  

Configure a switch’s priority for becoming the master default routing platform. The routing platform with the highest priority within the group becomes the master.

Options  

number—Routing platform’s priority for being elected to be the master router in the VRRP group. A larger value indicates a higher priority for being elected.

Range: 1 through 255
Default: 100 (for backup routers)

NOTE: Priority 255 cannot be assigned to routed VLAN interfaces (RVIs).

Required Privilege  

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  

• Configuring VRRP for IPv6 (CLI Procedure) on page 2224
PSU

Syntax

```plaintext
psu {
    redundancy {
        n-plus-n (Power Management);
    }
}
```

Hierarchy Level

`[edit chassis]`

Release Information

Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description

Configure N+N power supply redundancy for power management on an EX6200 or EX8200 switch.

The remaining statements are explained separately.

Required Privilege Level

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

Related Documentation

- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
redundancy (Graceful Switchover)

Syntax

redundancy {
  failover {
    on-disk-failure;
    on-loss-of-keepalives;
  }
  graceful-switchover;
}

Hierarchy Level
[edit chassis]

Release Information
Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description
Enable redundant Routing Engines on a Virtual Chassis with two or more member switches or on a standalone EX6200 or EX8200 switch with more than one Routing Engine.

The remaining statements are explained separately.

Default
Redundancy is enabled for the Routing Engines.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• graceful-switchover on page 2234
• Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504
• Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)
• High Availability Features for EX Series Switches Overview
### redundancy (Power Management)

**Syntax**

```plaintext
redundancy {
    n-plus-n (Power Management);
}
```

**Hierarchy Level**

```
[edit chassis psu]
```

**Release Information**

Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Configure N+N power supply redundancy for power management on an EX6200 or EX8200 switch.

The remaining statement is explained separately.

**Default**

N+1 power supply redundancy is configured by default.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
traceoptions (Routing Options)

Syntax

Syntax: traceoptions { file filename <files number> <size size> <world-readable | no-world-readable>; flag flag <disable>; }

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast],
[edit logical-systems logical-system-name routing-options],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options],
[edit routing-options flow],
[edit routing-options multicast]

Release Information

Statement introduced before Junos OS Release 7.4.
nsr-synchronization flag for BGP, IS-IS, LDP, and OSPF added in Junos OS Release 8.4.
nsr-synchronization and nsr-packet flags for BFD sessions added in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
nsr-synchronization flag for RIP and RIPng added in Junos OS Release 9.0.
nsr-synchronization flag for Layer 2 VPNs and VPLS added in Junos OS Release 9.1.
nsr-synchronization flag for PIM added in Junos OS Release 9.3.
nsr-synchronization flag for MPLS added in Junos OS Release 10.1.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
nsr-synchronization flag for MSDP added in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Define tracing operations that track all routing protocol functionality in the routing device.

To specify more than one tracing operation, include multiple flag statements.

Default

If you do not include this statement, no global tracing operations are performed.

Options

Values:

disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

file filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. We recommend that you place global routing protocol tracing output in the file routing-log.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and
so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. Note that if you specify a maximum number of files, you also must specify a maximum file size with the size option.

**Range:** 2 through 1000 files  
**Default:** 10 files

flag **flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. These are the global routing protocol tracing options:

- **all**—All tracing operations  
- **condition-manager**—Condition-manager events  
- **config-internal**—Configuration internals  
- **general**—All normal operations and routing table changes (a combination of the normal and route trace operations)  
- **graceful-restart**—Graceful restart operations  
- **normal**—All normal operations  
- **nsr-packet**—Detailed trace information for BFD nonstop active routing only  
- **nsr-synchronization**—Tracing operations for nonstop active routing  
- **nsr-synchronization-detail**—(MPLS only) Tracing operations for nonstop active routing in detail  
- **parse**—Configuration parsing  
- **policy**—Routing policy operations and actions  
- **regex-parse**—Regular-expression parsing  
- **route**—Routing table changes  
- **state**—State transitions  
- **task**—Interface transactions and processing  
- **timer**—Timer usage

**no-world-readable**—(Optional) Prevent any user from reading the log file.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. Note that if you specify a maximum file size, you also must specify a maximum number of trace files with the files option.

**Syntax:** xk to specify KB, xm to specify MB, or xg to specify GB  
**Range:** 10 KB through the maximum file size supported on your system  
**Default:** 128 KB
world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level
routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

Related Documentation
• Example: Tracing Global Routing Protocol Operations
• Tracing Nonstop Active Routing Synchronization Events

virtual-inet6-address

Syntax
virtual-inet6-address [addresses];

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number family inet6 address address
vrrp-inet6-group group-id]

Release Information
Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description
Configure the addresses of the virtual routers in a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You can configure up to eight addresses.

NOTE: The address of an aggregated Ethernet interface (a LAG) or a routed VLAN interface (RVI) cannot be assigned as the virtual router address in a VRRP IPv6 group.

Options
addresses—Addresses of one or more virtual routers. Do not include a prefix length. If the address is the same as the interface’s physical address, the interface becomes the master virtual router for the group.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring VRRP for IPv6 (CLI Procedure) on page 2224
virtual-link-local-address

**Syntax**

virtual-link-local-address *ipv6-address*;

**Hierarchy Level**

[edit interfaces interface-name unit logical-unit-number family inet address address vrrp-inet6-group group-id]
[edit interfaces interface-name unit logical-unit-number family inet6 address address vrrp-inet6-group group-id]

**Release Information**

Statement introduced in Junos OS Release 10.0 for EX Series switches.

**Description**

Configure a virtual link local address for a Virtual Router Redundancy Protocol (VRRP) IPv6 group. You must explicitly define a virtual link local address for each VRRP IPv6 group. The virtual link local address must be in the same subnet as the physical interface address.

**Options**

*ipv6-address*—Virtual link local IPv6 address for VRRP for an IPv6 group.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring VRRP for IPv6 (CLI Procedure) on page 2224
vrrp-inet6-group

Syntax
vrrp-inet6-group group-id {
    inet6-advertise-interval milliseconds;
    preempt {
        hold-time seconds;
    }
    priority number;
    virtual-inet6-address;
    virtual-link-local-address
}

Hierarchy Level
[edit interfaces interface-name unit logical-unit-number family inet6 address address]

Release Information
Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description
Configure a Virtual Router Redundancy Protocol (VRRP) IPv6 group.

Options
group-id—VRRP group identifier. If you enable MAC source address filtering on the
interface, you must include the virtual MAC address in the list of source MAC
addresses that you specify in the source-address-filter statement. MAC addresses
ranging from 00:00:5e:00:01:00 through 00:00:5e:00:01:ff are reserved for VRRP,
as defined in RFC 3768. The VRRP group number must be the decimal equivalent
of the last hexadecimal byte of the virtual MAC address.

Range: 0 through 255

The remaining statements are explained separately.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring VRRP for IPv6 (CLI Procedure) on page 2224
CHAPTER 43
Administration

- Verification Tasks on page 2247
- Operational Commands on page 2249

Verification Tasks

- Verifying Power Configuration and Use on page 2247

Verifying Power Configuration and Use

**Purpose** Verify on an EX Series switch:

- The power redundancy and line card priority settings
- The PoE power budgets for line cards that support PoE
- Whether the \(N+1\) or \(N+N\) power requirements are being met
- Whether the switch has sufficient power for a new line card or an \(N+N\) configuration

**Action** Enter the following command:

```
user@switch> show chassis power-budget-statistics
```

Example output for an EX6200 switch:

```
  PSU 0  (EX6200-PWR-AC2500)     :    2500 W   Online
  PSU 1  (EX6200-PWR-AC2500)     :    2500 W   Online
  PSU 2  (EX6200-PWR-AC2500)     :    2500 W   Online
  PSU 3  (EX6200-PWR-AC2500)     :    2500 W   Online
  Total Power supplied by all Online PSUs :   10000 W
  Power Redundancy Configuration :     N+1
  Power Reserved for the Chassis :     500 W

  Fan Tray Statistics
  FTC 0                         :     300 W      43.04 W

  FPC Statistics
  Base power   Power Used   PoE power   Priority
  FPC 1  (EX6200-48P)           :     220 W    49.47 W     1440 W       1
  FPC 2  (EX6200-48P)           :     220 W    47.20 W     800 W        2
  FPC 3  (EX6200-48P)           :     220 W 1493.57 W    1440 W       0
  FPC 4  (EX6200-SRE64-4XS)     :     100 W    51.38 W     0 W         0
  FPC 5  (EX6200-SRE64-4XS)     :     100 W    50.28 W     0 W         0
  FPC 6  (EX6200-48P)           :     220 W    49.38 W     800 W        6
  FPC 7  (EX6200-48P)           :     220 W    61.41 W    1440 W       9
```
**FPC 9 (EX6200-48T)**

- Total (non-PoE) Power allocated: 150 W
- Total Power allocated for PoE: 12.49 W
- Power Available (Redundant case): 0 W
- Total Power Available: 9 W

**Example output for an EX8200 switch:**

- **PSU 0 (EX8200-AC2K)**: 1200 W Online
- **PSU 1 (EX8200-AC2K)**: 1200 W Online
- **PSU 2 (EX8200-AC2K)**: 1200 W Online
- **PSU 3 (EX8200-AC2K)**: 1200 W Online
- Total Power supplied by all Online PSUs: 4800 W
- Power Redundancy Configuration: N+1
- Power Reserved for the Chassis: 1600 W

**FPC Statistics**

<table>
<thead>
<tr>
<th>FPC</th>
<th>Base power</th>
<th>PoE power</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>350 W</td>
<td>0 W</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>387 W</td>
<td>300 W</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>267 W</td>
<td>350 W</td>
<td>15</td>
</tr>
<tr>
<td>4</td>
<td>387 W</td>
<td>300 W</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>230 W</td>
<td>0 W</td>
<td>15</td>
</tr>
<tr>
<td>6</td>
<td>230 W</td>
<td>0 W</td>
<td>15</td>
</tr>
</tbody>
</table>

- Total (non-PoE) Power allocated: 3451 W
- Total Power allocated for PoE: 950 W
- Power Available (Redundant case): 149 W
- Total Power Available: 510 W

**Meaning**

Example output for an EX6200 switch — The online power supplies can supply a total of 10,000 W to the switch. The switch is configured for \( N+1 \) redundancy, which means 7500 W of redundant power can be supplied. The **Power Available (Redundant case)** field shows that the switch is meeting the \( N+1 \) power requirements, with an additional 5750 W available. This value is calculated by subtracting all power allocations except PoE power allocations from redundant power (7500 W).

The total amount of power available on the switch is 2515 W. This value is calculated by subtracting all power allocations, including PoE power allocations, from the total power (10,000 W). On a switch with PoE line cards, if **Total Power Available** is 0, some or all of the PoE line cards might not be allocated their configured PoE power budgets, which means power to some or all PoE ports might be disabled.

The power priority order of the line cards, from highest priority line card to the lowest priority line card, is 4, 5, 3, 1, 2, 6, 8, 9. Slots 4 and 5, which contain the Switch Fabric and Routing Engine (SRE) modules, always have highest priority, even if a lower-numbered slot, such as slot 3 in this example, has a priority of 0. Should two or more 2500 W power supplies fail, power management will remove or reduce the PoE power allocations from the PoE line cards in the following order to balance the power budget: 8, 6, 2, 1, and 3.

The **Power Used** values for the fan tray and line cards shows the actual power being consumed for these components at the time the command was executed. These values are for your information only; power management uses allocated power, which is based on the maximum power the component might consume, and not actual power consumed, in determining its power budget.
Example output for an EX8200 switch—The online power supplies can supply a total of 4800 W to the switch. The switch is configured for N+1 redundancy, which means 3600 W of redundant power can be supplied. The **Power Available (Redundant case)** field shows that the switch is meeting the N+1 power requirements, with an additional 149 W available. This value is calculated by subtracting all power allocations except PoE power allocations from redundant power (3600 W). Because 149 W is insufficient power for a line card, another line card cannot be added to the switch while maintaining N+1 redundancy.

The total amount of power available on the switch is 510 W. This value is calculated by subtracting all power allocations, including PoE power allocations, from the total power (4800 W). On a switch with PoE line cards, if **Total Power Available** is 0, some or all of the PoE line cards might not be allocated their configured PoE power budgets, which means power to some or all PoE ports might be disabled.

The power priority order of the line cards, from highest priority line card to the lowest priority line card, is 1, 4, 0, 2, 5, 6. Should one or more 1200 W power supplies fail, power management will remove or reduce the PoE power allocations from the PoE line cards in the following order to balance the power budget: 2, 4, and 1.

**Related Documentation**
- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
- Configuring the Power Priority of Line Cards (CLI Procedure)

**Operational Commands**
show chassis power-budget-statistics

Syntax
show chassis power-budget-statistics

Release Information
Command introduced in Junos OS Release 10.2 for EX Series switches.

Description
Display the power budget of an EX Series switch.

Required Privilege
view

Related Documentation
- Verifying Power Configuration and Use on page 2247
- Configuring the Power Priority of Line Cards (CLI Procedure)
- Configuring Power Supply Redundancy (CLI Procedure) on page 2223

List of Sample Output
- show chassis power-budget-statistics (EX6200 Switch) on page 2252
- show chassis power-budget-statistics (EX8200 Switch) on page 2252

Output Fields
Table 280 on page 2250 lists the output fields for the show chassis power-budget-statistics command. Output fields are listed in the approximate order in which they appear.

Table 280: show chassis power-budget-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSU n (supply type)</td>
<td>Capacity rating of the power supply and whether the power supply is currently operating (Online) or not (Offline). If a power supply is offline, the capacity is shown as 0 W.</td>
</tr>
<tr>
<td>Total Power supplied by all Online PSUs</td>
<td>Total number of watts supplied by all currently operating power supplies.</td>
</tr>
<tr>
<td>Power Redundancy Configuration</td>
<td>Configured power redundancy setting, either N+1 or N+N.</td>
</tr>
<tr>
<td>Base power reserved</td>
<td>Total number of watts reserved for the switch.</td>
</tr>
<tr>
<td>Non-PoE power being consumed</td>
<td>The amount of power, in W, currently being consumed for PoE.</td>
</tr>
<tr>
<td>Power Reserved for the Chassis</td>
<td>Power reserved for the chassis:</td>
</tr>
<tr>
<td></td>
<td>- For an EX6200 switch, 500 W.</td>
</tr>
<tr>
<td></td>
<td>- For an EX8208 switch: 1600 W in an N+1 configuration; 1200 W in an N+N configuration</td>
</tr>
<tr>
<td></td>
<td>- For an EX8216 switch: 2400 W in an N+1 configuration; 1800 W in an N+N configuration</td>
</tr>
<tr>
<td></td>
<td>The power reserved for the chassis includes the maximum power requirements for the fan tray and Switch Fabric and Routing Engine (SRE), Routing Engine (RE), and Switch Fabric (SF) modules in both base and redundant configurations.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Fan Tray Statistics</strong></td>
<td>(EX6200 switch only) Information about the fan tray:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Base power</strong>—Power allocated to the fan tray in the power budget. This allocation is included in <strong>Power Reserved for the Chassis</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Power Used</strong>—Actual power being used by the fan tray. This value is for informational purposes only: the power budget for the switch is based on allocated power (the theoretical maximum the fan tray might use) rather than used power.</td>
</tr>
<tr>
<td><strong>FPC n (card type)</strong></td>
<td>Information about the line card installed in slot n. For EX6200 switches, information about the SRE modules in slot 4 and slot 5 is also shown.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Base power</strong>—For line cards without PoE ports, the total power allocated to the line card. For line cards with PoE ports, the power allocated to the line card before the PoE power budget is allocated. The base power includes 37 W of PoE power that is always allocated to line cards that support PoE.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Power Used</strong>—(EX6200 switch only) The actual power being consumed by the line card or SRE module, including PoE power. This value is for informational purposes only: the power budget for the switch is based on allocated power (the theoretical maximum the line card might use) rather than used power.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PoE power</strong>—For line cards with PoE ports, the PoE power budget allocated to the line card. This value includes the 37 W of PoE power that is always part of the base power allocation for line cards that support PoE. For line cards without PoE ports, the value is always 0 W.</td>
</tr>
<tr>
<td></td>
<td>• The power priority assigned to the line card slot.</td>
</tr>
<tr>
<td><strong>Total (non-PoE) Power allocated</strong></td>
<td>Power budgeted for all the components in the switch, excluding the PoE power budget allocated to line cards. This value is equal to the power reserved for the chassis plus the base power allocations of all online line cards.</td>
</tr>
<tr>
<td><strong>Total Power allocated for PoE</strong></td>
<td>The total of the PoE power budgets allocated to the line cards in the switch. This figure includes the 37 W of PoE power always included in the base allocation for each line card that supports PoE.</td>
</tr>
<tr>
<td><strong>Total PoE power consumed</strong></td>
<td>The amount of power that has been consumed by PoE.</td>
</tr>
<tr>
<td><strong>Total PoE power remaining</strong></td>
<td>The amount of available power remaining that can be used for PoE.</td>
</tr>
<tr>
<td><strong>Power Available (Redundant case)</strong></td>
<td>Unused power available to the switch in the power budget, not including the power reserved for redundancy. If power is insufficient to meet the N+1 or N+N redundancy requirements, this value is 0. PoE power allocations are not included in the calculation of this value.</td>
</tr>
</tbody>
</table>
Table 280: show chassis power-budget-statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Power Available</td>
<td>Unused power available to the switch in the power budget. This value is derived by subtracting all power allocations, including PoE power allocations, from the total power available on the switch (the Total Power supplied by all Online PSUs value).</td>
</tr>
</tbody>
</table>

Sample Output

show chassis power-budget-statistics (EX6200 Switch)

```
user@switch> show chassis power-budget-statistics

PSU  0     (EX6200-PWR-AC2500)                 :    2500 W   Online
PSU  1     (EX6200-PWR-AC2500)                 :    2500 W   Online
PSU  2     (EX6200-PWR-AC2500)                 :    2500 W   Online
PSU  3     (EX6200-PWR-AC2500)                 :    2500 W   Online
Total Power supplied by all Online PSUs  :   10000 W
Power Redundancy Configuration           :     N+1
Power Reserved for the Chassis           :     500 W

Fan Tray Statistics            Base power    Power Used
FTC  0                         :     300 W      43.04 W
FPC Statistics                  Base power   Power Used   PoE power   Priority
FPC  1   (EX6200-48P)          :     220 W      49.47 W      1440 W       1
FPC  2   (EX6200-48P)          :     220 W      47.20 W       800 W       2
FPC  3   (EX6200-48P)          :     220 W    1493.57 W      1440 W       0
FPC  4   (EX6200-SRE64-4XS)    :     100 W    1493.57 W      1440 W       0
FPC  5   (EX6200-SRE64-4XS)    :     100 W      50.28 W       800 W       0
FPC  6   (EX6200-48P)          :     220 W      49.38 W       800 W       6
FPC  8   (EX6200-48P)          :     220 W      61.41 W      1440 W       9
FPC  9   (EX6200-48T)          :     150 W      12.49 W        0 W       9

Total (non-PoE) Power allocated          :    1750 W
Total Power allocated for PoE            :    5920 W
Power Available (Redundant case)         :    5750 W
Total Power Available                    :    2515 W
```

show chassis power-budget-statistics (EX8200 Switch)

```
user@switch> show chassis power-budget-statistics

PSU  0     (EX8200-AC2K)                 :    2000 W  Online
PSU  1     (EX8200-AC2K)                 :    2000 W  Online
PSU  2     (EX8200-AC2K)                 :    2000 W  Online
PSU  3     (EX8200-AC2K)                 :    2000 W  online
PSU  4     (EX8200-AC2K)                 :    2000 W  Online
Total Power supplied by all Online PSUs  :   10000 W
Power Redundancy Configuration           :     N+1
Power Reserved for the Chassis           :    2400 W

FPC Statistics                  Base power   PoE power  Priority
FPC  1   (EX8200-48T)                    :     350 W          0 W      15
FPC  5   (EX8200-2XS-40P)                :     387 W         792 W       0
FPC  9   (EX8200-48PL)                   :     267 W        915 W      15
FPC 10   (EX8200-2XS-40T)                :     350 W          0 W       1
FPC 12   (EX8200-48T)                    :     350 W          0 W      15

Total (non-PoE) Power allocated          :    4104 W
```
<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Power allocated for PoE</td>
<td>1707 W</td>
</tr>
<tr>
<td>Power Available (Redundant case)</td>
<td>3896 W</td>
</tr>
<tr>
<td>Total Power Available</td>
<td>4263 W</td>
</tr>
</tbody>
</table>
show vrrp

Syntax

show vrrp
  <brief | detail | extensive | summary>
  <interface interface-name>
  <track interfaces>

Release Information
Statement introduced in Junos OS Release 10.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display information and status about VRRP groups.

Options

none—(Same as brief) Display brief status information about all VRRP interfaces.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

interface interface-name—(Optional) Display information and status about the specified VRRP interface.

track interfaces—(Optional) Display information and status about VRRP track interfaces.

Required Privilege
Level view

Related Documentation
  • Configuring VRRP for IPv6 (CLI Procedure) on page 2224

List of Sample Output
  show vrrp on page 2259
  show vrrp brief on page 2259
  show vrrp detail (IPv6) on page 2259
  show vrrp detail (Route Track) on page 2260
  show vrrp extensive on page 2260
  show vrrp interface on page 2261
  show vrrp summary on page 2262
  show vrrp track detail on page 2262
  show vrrp track summary on page 2263

Output Fields
Table 281 on page 2254 lists the output fields for the show vrrp command. Output fields are listed in the approximate order in which they appear.

Table 281: show vrrp Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the logical interface.</td>
<td>none, brief, extensive, summary</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface index number, which reflects its initialization sequence.</td>
<td>extensive</td>
</tr>
<tr>
<td>Groups</td>
<td>Total number of VRRP groups configured on the interface.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 281: show vrrp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Total number of VRRP groups that are active (that is, whose interface state is</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>either up or down).</td>
<td></td>
</tr>
<tr>
<td>Interface VRRP PDU statistics</td>
<td>Nonerrored statistics for the logical interface:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Advertisement sent—Number of VRRP advertisement protocol data units (PDUs) that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that the interface has transmitted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advertisement received—Number of VRRP advertisement PDUs received by the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packets received—Number of VRRP packets received for VRRP groups on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No group match received—Number of VRRP packets received for VRRP groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that do not exist on the interface.</td>
<td></td>
</tr>
<tr>
<td>Interface VRRP PDU error</td>
<td>Errored statistics for the logical interface:</td>
<td>extensive</td>
</tr>
<tr>
<td>statistics</td>
<td>• Invalid IPAH next type received—Number of packets received that use the IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authentication Header protocol (IPAH) and that do not encapsulate VRRP packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalid VRRP ttl value received—Number of packets received whose IP time-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to-live (TTL) value is not 255.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalid VRRP version received—Number of packets received whose VRRP version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is not 2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalid VRRP pdu type received—Number of packets received whose VRRP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDU type is not 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalid VRRP authentication type received—Number of packets received whose</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VRRP authentication is not none, simple, or md5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalid VRRP IP count received—Number of packets received whose VRRP IP count</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exceeds 8.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalid VRRP checksum received—Number of packets received whose VRRP checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>does not match the calculated value.</td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Unit</td>
<td>Logical unit number.</td>
<td>All levels</td>
</tr>
<tr>
<td>Address</td>
<td>Address of the physical interface.</td>
<td>none, brief,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Index</td>
<td>Physical interface index number, which reflects its initialization sequence.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>SNMP ifindex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>VRRP-Traps</td>
<td>Status of VRRP traps: Enabled or Disabled.</td>
<td>detail, extensive</td>
</tr>
</tbody>
</table>
Table 281: show vrrp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type and Address</strong></td>
<td>Identifier for the address and the address itself:</td>
<td>none, brief, summary</td>
</tr>
<tr>
<td></td>
<td>• lcl—Configured local interface address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• mas—Address of the master virtual router. This address is displayed only when the local interface is acting as a backup router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vip—Configured virtual IP addresses.</td>
<td></td>
</tr>
<tr>
<td><strong>Interface state or Int state</strong></td>
<td>State of the physical interface:</td>
<td>none, brief, extensive, summary</td>
</tr>
<tr>
<td></td>
<td>• down—The device is present and the link is unavailable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• not present—The interface is configured, but no physical device is present.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unknown—The VRRP process has not had time to query the kernel about the state of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• up—The device is present and the link is established.</td>
<td></td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td>VRRP group number.</td>
<td>none, brief, extensive, summary</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>VRRP state:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• backup—The interface is acting as the backup router interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• bringup—VRRP is just starting, and the physical device is not yet present.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• idle—VRRP is configured on the interface and is disabled. This can occur when VRRP is first enabled on an interface whose link is established.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• initializing—VRRP is initializing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• master—The interface is acting as the master router interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• transition—The interface is changing between being the backup and being the master router.</td>
<td></td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Configured VRRP priority for the interface.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Advertisement interval</strong></td>
<td>Configured VRRP advertisement interval.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Authentication type</strong></td>
<td>Configured VRRP authentication type: none, simple, or md5.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Preempt</strong></td>
<td>Whether preemption is allowed on the interface: yes or no.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Accept-data mode</strong></td>
<td>Whether the interface is configured to accept packets destined for the virtual IP address: yes or no.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>VIP count</strong></td>
<td>Number of virtual IP addresses that have been configured on the interface.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>VIP</strong></td>
<td>List of virtual IP addresses configured on the interface.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Advertisement timer</strong></td>
<td>Time until the advertisement timer expires.</td>
<td>detail, extensive</td>
</tr>
</tbody>
</table>
### Table 281: show vrrp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Master router</strong></td>
<td>IP address of the interface that is acting as the master. If the VRRP interface is down, the output is N/A.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Virtual router uptime</strong></td>
<td>Time that the virtual router has been up.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Master router uptime</strong></td>
<td>Time that the master router has been up.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Virtual MAC</strong></td>
<td>MAC address associated with the virtual IP address.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Tracking</strong></td>
<td>Whether tracking is <strong>enabled</strong> or <strong>disabled</strong>.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Current priority</strong></td>
<td>Current operational priority for being the VRRP master.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Configured priority</strong></td>
<td>Configured base priority for being the VRRP master.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Priority hold-time</strong></td>
<td>Minimum time interval, in seconds, between successive changes to the current priority. <strong>Disabled</strong> indicates no minimum interval.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Remaining-time</strong></td>
<td><em>(track option only)</em> Displays the time remaining in the priority hold-time interval.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Interface tracking</strong></td>
<td>Whether interface tracking is enabled or disabled. When enabled, the output also displays the number of tracked interfaces.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Interface/Tracked interface</strong></td>
<td>Name of the tracked interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Int state/Interface state</strong></td>
<td>Current operational state of the tracked interface: <strong>up</strong> or <strong>down</strong>.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Int speed/Speed</strong></td>
<td>Current operational speed, in bits per second, of the tracked interface.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Incurred priority cost</strong></td>
<td>Operational priority cost incurred due to the state and speed of this tracked interface. This cost is applied to the configured priority to obtain the current priority.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Threshold</strong></td>
<td>Speed below which the corresponding priority cost is incurred. In other words, when the speed of the interface drops below the threshold speed, the corresponding priority cost is incurred. An entry of <strong>down</strong> means that the corresponding priority cost is incurred when the interface is down.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Route tracking</strong></td>
<td>Whether route tracking is enabled or disabled. When enabled, the output also displays the number of tracked routes.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Route count</strong></td>
<td>The number of routes being tracked.</td>
<td>detail, extensive</td>
</tr>
</tbody>
</table>
Table 281: show vrrp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route</td>
<td>The IP address of the route being tracked.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>VRF name</td>
<td>The VPN routing and forwarding (VRF) routing instance that the tracked route is in.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Route state</td>
<td>The state of the route being tracked: up, down, or unknown.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Priority cost</td>
<td>Configured priority cost. This value is incurred when the interface speed drops below the corresponding threshold or when the tracked route goes down.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the threshold is active (*). If the threshold is active, the corresponding priority cost is incurred.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Group VRRP PDU statistics</td>
<td>Number of VRRP advertisements sent and received by the group.</td>
<td>extensive</td>
</tr>
<tr>
<td>Group VRRP PDU error statistics</td>
<td>Errored statistics for the VRRP group:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Bad authentication type received—Number of VRRP PDUs received with an invalid authentication type. The received authentication can be none, simple, or md5 and must be the same for all routers in the VRRP group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bad password received—Number of VRRP PDUs received with an invalid key (password). The password for simple authentication must be the same for all routers in the VRRP group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bad MD5 digest received—Number of VRRP PDUs received for which the MD5 digest computed from the VRRP PDU differs from the digest expected by the VRRP instance configured on the router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bad advertisement timer received—Number of VRRP PDUs received with an advertisement time interval that is inconsistent with the one in use among the routers in the VRRP group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bad VIP count received—Number of VRRP PDUs whose virtual IP address counts differ from the count that has been configured on the VRRP instance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bad VIPADDR received—Number of VRRP PDUs whose virtual IP addresses differ from the list of virtual IP addresses configured on the VRRP instance.</td>
<td></td>
</tr>
<tr>
<td>Group state transition statistics</td>
<td>State transition statistics for the VRRP group:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Idle to master transitions—Number of times that the VRRP instance transitioned from the idle state to the master state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Idle to backup transitions—Number of times that the VRRP instance transitioned from the idle state to the backup state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Backup to master transitions—Number of times that the VRRP instance transitioned from the backup state to the master state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Master to backup transitions—Number of times that the VRRP instance transitioned from the master state to the backup state.</td>
<td></td>
</tr>
<tr>
<td>Vlan-id</td>
<td>ID of Vlan</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 281: show vrrp Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>VR state</td>
<td>VRRP information:</td>
<td>none, brief</td>
</tr>
<tr>
<td></td>
<td>• backup—The interface is acting as the backup router interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• bringup—VRRP is just starting, and the physical device is not yet present.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• idle—VRRP is configured on the interface and is disabled. This can occur when VRRP is first enabled on an interface whose link is established.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• initializing—VRRP is initializing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• master—The interface is acting as the master router interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• transition—The interface is changing between being the backup and being the master router.</td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>VRRP timer information:</td>
<td>none, brief</td>
</tr>
<tr>
<td></td>
<td>• A—Time, in seconds, until the advertisement timer expires.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• D—Time, in seconds, until the Master is Dead timer expires.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

**show vrrp**

```
user@host> show vrrp
Interface        State        Group    VR state    Timer   Type  Address
ge-0/0/0.121     up               1     master      A 1.052  lcl   gec0::12:1:1:1
                      vip   ge80::12:1:1:99
                      vip   gec0::12:1:1:99

ge-0/0/2.131     up                1   master      A 0.364  lcl   gec0::13:1:1:1
                      vip   ge80::13:1:1:99
                      vip   gec0::13:1:1:99
```

**show vrrp brief**

The output for the `show vrrp brief` command is identical to that for the `show vrrp` command. For sample output, see show vrrp on page 2259.

**show vrrp detail (IPv6)**

```
user@host> show vrrp detail
Physical interface: ge-0/0/0, Unit: 121, Vlan-id: 212, Address: gec0::12:1:1/120

Index: 67, SNMP ifIndex: 45, VRRP-Traps: enabled
Interface state: up, Group: 1, State: master
Priority: 200, Advertisement interval: 1, Authentication type: none
Advertisement timer: 1.121s, Master router: ge80::12:1:1:1
Virtual router uptime: 00:03:47, Master router uptime: 00:03:41
Virtual MAC: 00:00:5e:00:02:01
Tracking: disabled
```
show vrrp detail (Route Track)

show vrrp extensive

Physical interface: ge-0/0/2, Unit: 131, Vlan-id: 213, Address: gec0::13:1:1:1/120

Index: 69, SNMP ifIndex: 47, VRRP-Traps: enabled
Interface state: up, Group: 1, State: master
Priority: 200, Advertisement interval: 1, Authentication type: none
Advertisement timer: 0.327s, Master router: ge80::13:1:1:1
Virtual router uptime: 00:03:47, Master router uptime: 00:03:41
Virtual MAC: 00:00:5e:00:02:01
Tracking: disabled

Interface state: up, Group: 1, State: master
Priority: 200, Advertisement interval: 1, Authentication type: none
Advertisement timer: 0.327s, Master router: ge80::13:1:1:1
Virtual router uptime: 00:03:47, Master router uptime: 00:03:41
Virtual MAC: 00:00:5e:00:02:01
Tracking: disabled

Tracking: disabled

show vrrp extensive

Interface: ge-0/0/0.121, Interface index: 67, Groups: 1, Active : 1
Interface VRRP PDU statistics
Advertisement sent : 188
Advertisement received : 0
Packets received : 0
No group match received : 0
Interface VRRP PDU error statistics
Invalid IPAH next type received : 0
Invalid VRRP TTL value received : 0
Invalid VRRP version received : 0
Invalid VRRP PDU type received : 0
Invalid VRRP authentication type received: 0
Invalid VRRP IP count received : 0
Invalid VRRP checksum received : 0

Physical interface: ge-0/0/0, Unit: 121, Vlan-id: 212, Address: gec0::12:1:1:1/120

Index: 67, SNMP ifIndex: 45, VRRP-Traps: enabled
Interface state: up, Group: 1, State: master
Priority: 200, Advertisement interval: 1, Authentication type: none
Advertisement timer: 1.034s, Master router: ge80::12:1:1:1
Virtual router uptime: 00:03:47, Master router uptime: 00:03:41
Virtual MAC: 00:00:5e:00:02:01
Tracking: disabled
Group VRRP PDU statistics
Advertisement sent              :          188
Advertisement received          :            0

Group VRRP PDU error statistics
Bad authentication type received:            0
Bad password received             :            0
Bad MD5 digest received           :            0
Bad advertisement timer received:            0
Bad VIP count received            :            0
Bad VIPADDR received              :            0

Group state transition statistics
Idle to master transitions       :            0
Idle to backup transitions       :            1
Backup to master transitions     :            1
Master to backup transitions     :            0

Interface: ge-0/0/2.131, Interface index: 69, Groups: 1, Active: 1

Interface VRRP PDU statistics
Advertisement sent               :          186
Advertisement received           :            0
Packets received                 :            0
No group match received          :            0

Interface VRRP PDU error statistics
Invalid IPAH next type received  :            0
Invalid VRRP TTL value received  :            0
Invalid VRRP version received    :            0
Invalid VRRP PDU type received   :            0
Invalid VRRP authentication type received:            0
Invalid VRRP IP count received   :            0
Invalid VRRP checksum received   :            0

Physical interface: ge-0/0/2, Unit: 131, Vlan-id: 213, Address: gec0::13:1:1:1/120
Index: 69, SNMP ifIndex: 47, VRRP-Traps: enabled
Interface state: up, Group: 1, State: master
Priority: 200, Advertisement interval: 1, Authentication type: none
Preempt: yes, Accept-data mode: no, VIP count: 2, VIP: ge80::13:1:1:99,
gec0::13:1:1:99
Advertisement timer: 0.396s, Master router: ge80::13:1:1:1
Virtual router uptime: 00:04:04, Master router uptime: 00:03:58
Virtual MAC: 00:00:5e:00:02:01
Tracking: disabled

Group VRRP PDU statistics
Advertisement sent               :          186
Advertisement received           :            0

Group VRRP PDU error statistics
Bad authentication type received:            0
Bad password received             :            0
Bad MD5 digest received           :            0
Bad advertisement timer received:            0
Bad VIP count received            :            0
Bad VIPADDR received              :            0

Group state transition statistics
Idle to master transitions       :            0
Idle to backup transitions       :            1
Backup to master transitions     :            1
Master to backup transitions     :            0

show vrrp interface

user@host> show vrrp interface
Interface: ge-0/0/0.121, Interface index: 67, Groups: 1, Active: 1

Interface VRRP PDU statistics
  Advertisement sent : 205
  Advertisement received : 0
  Packets received : 0
  No group match received : 0

Interface VRRP PDU error statistics
  Invalid IP AH next type received : 0
  Invalid VRRP TTL value received : 0
  Invalid VRRP version received : 0
  Invalid VRRP PDU type received : 0
  Invalid VRRP authentication type received : 0
  Invalid VRRIP IP count received : 0
  Invalid VRRP checksum received : 0

Physical interface: ge-0/0/0, Unit: 121, Vlan-id: 212, Address: gec0::12:1:1:1/120
  Index: 67, SNMP ifIndex: 45, VRRP-Traps: enabled
  Interface state: up, Group: 1, State: master
  Priority: 200, Advertisement interval: 1, Authentication type: none
  Advertisement timer: 0.789s, Master router: ge80::12:1:1:1
  Virtual router uptime: 00:04:26, Master router uptime: 00:04:20
  Virtual MAC: 00:00:5e:00:02:01
  Tracking: disabled

Group VRRP PDU statistics
  Advertisement sent : 205
  Advertisement received : 0

Group VRRP PDU error statistics
  Bad authentication type received : 0
  Bad password received : 0
  Bad MD5 digest received : 0
  Bad advertisement timer received : 0
  Bad VIP count received : 0
  Bad VIPADDR received : 0

Group state transition statistics
  Idle to master transitions : 0
  Idle to backup transitions : 1
  Backup to master transitions : 1
  Master to backup transitions : 0

show vrrp summary

user@host> show vrrp summary
  Interface     State       Group   VR state      Type   Address
  ge-4/1/0.0    up              1   backup        lcl    10.57.0.2
  vip    10.57.0.100

show vrrp track detail

user@host> show vrrp track detail
  Tracked interface: ae1.211
  State: up, Speed: 400m
  Incurred priority cost: 0
  Threshold Priority cost Active
  400m      10
  300m      60
  200m      110
  100m      160
  down     190
Tracking VRRP interface: ae0.210, Group: 1
  VR State: master
  Current priority: 200, Configured priority: 200
  Priority hold-time: disabled, Remaining-time: 50.351

show vrrp track summary

user@host> show vrrp track summary
Track if     State  Speed VRRP if  Group  VR State  Current priority
ae1.211     up     400m  ae0.210  1 master  200
PART 15

Interfaces

• Overview on page 2267
• Configuration on page 2285
• Administration on page 2463
• Troubleshooting Procedures on page 2545
CHAPTER 44

Overview

• Interfaces Overview on page 2267

Interfaces Overview

• EX Series Switches Interfaces Overview on page 2267
• Understanding Interface Naming Conventions on EX Series Switches on page 2270
• Understanding Aggregated Ethernet Interfaces and LACP on page 2272
• Understanding Layer 3 Subinterfaces on page 2275
• Understanding Unicast RPF for EX Series Switches on page 2276
• Understanding IP Directed Broadcast for EX Series Switches on page 2280
• Understanding Interface Ranges on EX Series Switches on page 2281
• 802.1Q VLANs Overview on page 2283

EX Series Switches Interfaces Overview

Juniper Networks EX Series Ethernet Switches have two types of interfaces: network interfaces and special interfaces. This topic provides brief information about these interfaces. For additional information, see the Junos OS Interfaces Fundamentals Configuration Guide.

For information about interface-naming conventions on EX Series switches, see “Understanding Interface Naming Conventions on EX Series Switches” on page 2270.

This topic describes:

• Network Interfaces on page 2267
• Special Interfaces on page 2268

Network Interfaces

Network interfaces connect to the network and carry network traffic. Table 282 on page 2268 lists the types of network interfaces supported on EX Series switches.
Table 282: Network Interface Types and Purposes

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Ethernet interfaces</td>
<td>All EX Series switches allow you to group Ethernet interfaces at the physical layer to form a single link layer interface, also known as a link aggregation group (LAG) or bundle. These aggregated Ethernet interfaces help to balance traffic and increase the uplink bandwidth.</td>
</tr>
<tr>
<td>LAN access interfaces</td>
<td>Use these EX Series switch interfaces to connect a personal computer, laptop, file server, or printer to the network. When you power on an EX Series switch and use the factory-default configuration, the software automatically configures interfaces in access mode for each of the network ports. The default configuration also enables autonegotiation for both speed and link mode.</td>
</tr>
<tr>
<td>Power over Ethernet (PoE) interfaces</td>
<td>EX Series switches provide PoE network ports with various switch models. These ports can be used to connect voice over IP (VoIP) telephones, wireless access points, video cameras, and point-of-sale devices to safely receive power from the same access ports that are used to connect personal computers to the network. PoE interfaces are enabled by default in the factory configuration.</td>
</tr>
<tr>
<td>Trunk interfaces</td>
<td>EX Series access switches can be connected to a distribution switch or customer-edge (CE) switches or routers. To use a port for this type of connection, you must explicitly configure the network interface for trunk mode. The interfaces from the distribution switch or CE switch to the access switches must also be configured for trunk mode.</td>
</tr>
</tbody>
</table>

Special Interfaces
Table 283 on page 2268 lists the types of special interfaces supported on EX Series switches.

Table 283: Special Interface Types and Purposes

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console port</td>
<td>Each EX Series switch has a serial port, labeled CON or CONSOLE, for connecting tty-type terminals to the switch using standard PC-type tty cables. The console port does not have a physical address or IP address associated with it. However, it is an interface in the sense that it provides access to the switch. On an EX3300 Virtual Chassis, an EX4200 Virtual Chassis, or an EX4500 Virtual Chassis, you can access the master and configure all members of the Virtual Chassis through any member’s console port. For more information about the console port in a Virtual Chassis, see “Understanding Global Management of an EX Series Virtual Chassis” on page 4469.</td>
</tr>
<tr>
<td>Loopback</td>
<td>All EX Series switches have this software-only virtual interface that is always up. The loopback interface provides a stable and consistent interface and IP address on the switch.</td>
</tr>
<tr>
<td>Management interface</td>
<td>The Juniper Networks Junos operating system (Junos OS) for EX Series switches automatically creates the switch’s management Ethernet interface, me0. The management Ethernet interface provides an out-of-band method for connecting to the switch. To use me0 as a management port, you must configure its logical port, me0.0, with a valid IP address. You can connect to the management interface over the network using utilities such as SSH or Telnet. SNMP can use the management interface to gather statistics from the switch. (The management interface me0 is analogous to the fxp0 interfaces on routers running Junos OS.)</td>
</tr>
</tbody>
</table>
### Table 283: Special Interface Types and Purposes (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Routing and Bridging (IRB) Interface or Routed VLAN Interface (RVI)</td>
<td>EX Series switches use an integrated routing and bridging (IRB) interface or Routed VLAN Interface (RVI) to route traffic from one broadcast domain to another and to perform other Layer 3 functions such as traffic engineering. These functions are typically performed by a router interface in a traditional network. The IRB interface or RVI functions as a logical router, eliminating the need for having both a switch and a router. These interfaces must be configured as part of a broadcast domain or virtual private LAN service (VPLS) routing instance for Layer 3 traffic to be routed from.</td>
</tr>
<tr>
<td>Virtual Chassis port (VCP) interfaces</td>
<td>Virtual Chassis ports (VCPs) are used to interconnect switches in a Virtual Chassis:</td>
</tr>
<tr>
<td></td>
<td>• EX3300 switches—Port 2 and port 3 of the SFP+ uplink ports are preconfigured as VCPs and can be used to interconnect up to six EX3300 switches in an EX3300 Virtual Chassis. See “Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure)” on page 4497.</td>
</tr>
<tr>
<td></td>
<td>• EX4200 and EX4500 switches—Each EX4200 switch or each EX4500 switch with a Virtual Chassis module installed has two dedicated VCPs on its rear panel. These ports can be used to interconnect up to ten EX4200 switches in an EX4200 Virtual Chassis, up to ten EX4500 switches in an EX4500 Virtual Chassis, and up to ten switches in a mixed EX4200 and EX4500 Virtual Chassis. When you power on switches that are interconnected in this manner, the software automatically configures the VCP interfaces for the dedicated ports that have been interconnected. These VCP interfaces are not configurable or modifiable. See Understanding the High-Speed Interconnection of the Dedicated Virtual Chassis Ports Connecting EX4200, EX4500, and EX4550 Member Switches. You can also interconnect EX4200 and EX4500 switches by using uplink module ports. Using uplink ports allows you to connect switches over longer distances than you can by using the dedicated VCPs. To use the uplink ports as VCPs, you must explicitly configure the uplink module ports on the members you want to connect as VCPs. See “Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure)” on page 4497 or Setting an Uplink Port as a Virtual Chassis Port on an EX4500 or EX4550 Switch (CLI Procedure).</td>
</tr>
<tr>
<td></td>
<td>• EX4300 switches—All QSFP+ ports are configured as VCPs, by default. See “Understanding EX4300 Virtual Chassis” on page 4459. You can also interconnect EX4300 switches into a Virtual Chassis by using SFP+ uplink module ports as VCPs. Using uplink ports as VCPs allows you to connect switches over longer distances than you can by using the QSFP+ ports as VCPs. To use the uplink ports as VCPs, you must explicitly configure the uplink module ports on the members you want to connect as VCPs. See “Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure)” on page 4497.</td>
</tr>
<tr>
<td></td>
<td>• EX8200 switches—EX8200 switches can be connected to an XRE200 External Routing Engine to create an EX8200 Virtual Chassis. The XRE200 External Routing Engine has dedicated VCPs that connect to ports on the internal Routing Engines of the EX8200 switches and can connect to another XRE200 External Routing Engine for redundancy. These ports require no configuration. You can also connect two members of an EX8200 Virtual Chassis so that they can exchange Virtual Chassis Control Protocol (VCCP) traffic. To do so, you explicitly configure network ports on the EX8200 switches as VCPs. See Understanding Virtual Chassis Ports in an EX8200 Virtual Chassis.</td>
</tr>
<tr>
<td>Virtual management Ethernet (VME) interface</td>
<td>EX3300, EX4200, EX4300, and EX4500 switches have a VME interface. This is a logical interface that is used for Virtual Chassis configurations and allows you to manage all the members of the Virtual Chassis through the master. For more information about the VME interface, see “Understanding Global Management of an EX Series Virtual Chassis” on page 4469. EX8200 switches do not use a VME interface. An EX8200 Virtual Chassis is managed through the management Ethernet (me0) interface on the XRE200 External Routing Engine.</td>
</tr>
</tbody>
</table>
Understanding Interface Naming Conventions on EX Series Switches

Juniper Networks EX Series Ethernet Switches use a naming convention for defining the interfaces that is similar to that of other platforms running under Juniper Networks Junos operating system (Junos OS). This topic provides brief information about the naming conventions used for interfaces on EX Series switches. For additional information, see the Junos OS Network Interfaces Configuration Guide.

This topic describes:

- Physical Part of an Interface Name on page 2270
- Logical Part of an Interface Name on page 2272
- Wildcard Characters in Interface Names on page 2272

Physical Part of an Interface Name

Network interfaces in Junos OS are specified as follows:

`type-fpc / pic / port`

EX Series switches apply this convention as follows:

- **type**—EX Series interfaces use the following media types:
  
  - `ge`—Gigabit Ethernet interface
  
  - `xe`—10 Gigabit Ethernet interface
  
  - `et`—40 Gigabit Ethernet interface

- **fpc**—Flexible PIC Concentrator. EX Series interfaces use the following convention for the FPC number in interface names:
- On an EX2200 switch, an EX3200 switch, a standalone EX3300 switch, a standalone EX4200 switch, a standalone EX4300 switch, a standalone EX4500, and a standalone EX4550 switch, FPC refers to the switch itself. The FPC number is 0 by default on these switches.

- On an EX3300 Virtual Chassis, an EX4200 Virtual Chassis, an EX4300 Virtual Chassis, an EX4500 Virtual Chassis, an EX4550 Virtual Chassis, or a mixed Virtual Chassis, the FPC number indicates the member ID of the switch in the Virtual Chassis.

- On an EX6200 switch and a standalone EX8200 switch, the FPC number indicates the slot number of the line card that contains the physical interface. On an EX6200 switch, the FPC number also indicates the slot number of the Switch Fabric and Routing Engine (SRE) module that contains the uplink port.

- On an EX8200 Virtual Chassis, the FPC number indicates the slot number of the line card on the Virtual Chassis. The line card slots on Virtual Chassis member 0 are numbered 0 through 15; on member 1, they are numbered 16 through 31, and so on.

- **pic**—EX Series interfaces use the following convention for the PIC (Physical Interface Card) number in interface names:
  - On EX2200, EX3200, EX3300, EX4200, EX4500 switch, and EX4550 switches, the PIC number is 0 for all built-in interfaces (interfaces that are not uplink ports).
  - On EX2200, EX3200, EX3300, and EX4200 switches, the PIC number is 1 for uplink ports.
  - On EX4300 switches, the PIC number is 0 for built-in network ports, 1 for built-in QSFP+ ports (located on the rear panel of the switch), and 2 for uplink module ports.
  - On EX4500 switches, the PIC number is 1 for ports on the left-hand uplink module and 2 for ports on the right-hand uplink module.
  - On EX4550 switches, the PIC number is 1 for ports in the expansion module or Virtual Chassis module installed in the module slot on the front panel of the switch and 2 for those in the expansion module or Virtual Chassis module installed in the module slot on the rear panel of the switch.
  - On EX6200 and EX8200 switches, the PIC number is always 0.

- **port**—EX Series interfaces use the following convention for port numbers:
  - On EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, and EX4550 switches, built-in network ports are numbered from left to right. On models that have two rows of ports, the ports on the top row start with 0 followed by the remaining even-numbered ports, and the ports on the bottom row start with 1 followed by the remaining odd-numbered ports.
  - Uplink ports in EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, and EX4550 switches are labeled from left to right, starting with 0.
  - On EX6200 and EX8200 switches, the network ports are numbered from left to right on each line card. On line cards that have two rows of ports, the ports on the top row...
start with 0 followed by the remaining even-numbered ports, and the ports on the bottom row start with 1 followed by the remaining odd-numbered ports.

- Uplink ports on an SRE module in an EX6200 switch are labeled from left to right, starting with 0.

Logical Part of an Interface Name

The logical unit part of the interface name corresponds to the logical unit number, which can be a number from 0 through 16384. In the virtual part of the name, a period (.) separates the port and logical unit numbers: `type-fpc/pic/port.logical-unit-number`. For example, if you issue the `show ethernet-switching interfaces` command on a system with a default VLAN, the resulting display shows the logical interfaces associated with the VLAN:

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>down</td>
<td>remote-analyzer</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/10.0</td>
<td>down</td>
<td>default</td>
<td>unblocked</td>
</tr>
</tbody>
</table>

Wildcard Characters in Interface Names

In the `show interfaces` and `clear interfaces` commands, you can use wildcard characters in the `interface-name` option to specify groups of interface names without having to type each name individually. You must enclose all wildcard characters except the asterisk (*) in quotation marks (" ").

Related Documentation

- EX Series Switches Interfaces Overview on page 2267
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286

Understanding Aggregated Ethernet Interfaces and LACP

IEEE 802.3ad link aggregation enables you to group Ethernet interfaces to form a single link layer interface, also known as a link aggregation group (LAG) or bundle.

Aggregating multiple links between physical interfaces creates a single logical point-to-point trunk link or a LAG. The LAG balances traffic across the member links within an aggregated Ethernet bundle and effectively increases the uplink bandwidth. Another advantage of link aggregation is increased availability, because the LAG is composed of multiple member links. If one member link fails, the LAG continues to carry traffic over the remaining links.

Link Aggregation Control Protocol (LACP), a component of IEEE 802.3ad, provides additional functionality for LAGs.

This topic describes:

- Link Aggregation Group (LAG) on page 2273
- Link Aggregation Control Protocol (LACP) on page 2274
Link Aggregation Group (LAG)

You configure a LAG by specifying the link number as a physical device and then associating a set of interfaces (ports) with the link. All the interfaces must have the same speed and be in full-duplex mode. Juniper Networks Junos operating system (Junos OS) for EX Series Ethernet Switches assigns a unique ID and port priority to each interface. The ID and priority are not configurable.

The number of interfaces that can be grouped into a LAG and the total number of LAGs supported on a switch varies according to switch model. Table 284 on page 2273 lists the EX Series switches and the maximum number of interfaces per LAG and the maximum number of LAGs they support. MX Series devices can support up to 64 LAGs.

Table 284: Maximum Interfaces per LAG and Maximum LAGs per Switch

<table>
<thead>
<tr>
<th>Switch</th>
<th>Maximum Interfaces per LAG</th>
<th>Maximum LAGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200</td>
<td>8</td>
<td>32</td>
</tr>
<tr>
<td>EX3200</td>
<td>8</td>
<td>32</td>
</tr>
<tr>
<td>EX3300 and EX3300 Virtual Chassis</td>
<td>8</td>
<td>111</td>
</tr>
<tr>
<td>EX4200 and EX4200 Virtual Chassis</td>
<td>8</td>
<td>111</td>
</tr>
<tr>
<td>EX4300 and EX4300 Virtual Chassis</td>
<td>8</td>
<td>112</td>
</tr>
<tr>
<td>EX4500, EX4500 Virtual Chassis, EX4550, and EX4550 Virtual Chassis</td>
<td>8</td>
<td>111</td>
</tr>
<tr>
<td>EX6200</td>
<td>8</td>
<td>111</td>
</tr>
<tr>
<td>EX8200</td>
<td>12</td>
<td>255</td>
</tr>
<tr>
<td>EX8200 Virtual Chassis</td>
<td>12</td>
<td>239</td>
</tr>
</tbody>
</table>

When configuring LAGs, consider the following guidelines:

- You must configure the LAG on both sides of the link.
- You must set the interfaces on either side of the link to the same speed.
- You can configure and apply firewall filters on a LAG.
- You can optionally configure LACP for link negotiation.
- You can optionally configure LACP for link protection.
You can combine physical Ethernet ports belonging to different member switches of a Virtual Chassis configuration to form a LAG. See “Understanding EX Series Virtual Chassis Port Link Aggregation” on page 4472 and Understanding Link Aggregation in an EX8200 Virtual Chassis.

NOTE: The interfaces that are included within a LAG are sometimes referred to as member interfaces. Do not confuse this term with member switches, which refers to switches that are interconnected as a Virtual Chassis. It is possible to create a LAG that is composed of member interfaces that are located in different member switches of a Virtual Chassis.

A LAG creates a single logical point-to-point connection. A typical deployment for a LAG would be to aggregate trunk links between an access switch and a distribution switch or customer edge (CE) router.

**Link Aggregation Control Protocol (LACP)**

When LACP is configured, it detects misconfigurations on the local end or the remote end of the link. Thus, LACP can help prevent communication failure:

- When LACP is not enabled, a local LAG might attempt to transmit packets to a remote single interface, which causes the communication to fail.
- When LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.

By default, Ethernet links do not exchange LACP protocol data units (PDUs), which contain information about the state of the link. You can configure Ethernet links to actively transmit LACP PDUs, or you can configure the links to passively transmit them, sending out LACP PDUs only when the Ethernet link receives them from the remote end. The transmitting link is known as the actor and the receiving link is known as the partner.

In a scenario where a dual-homed server is deployed with a switch, the network interface cards form a LAG with the switch. During a server upgrade, the server might not be able to exchange LACP PDUs. In such a situation, you can configure an interface to be in the up state even if no PDUs are exchanged. Use the force-up statement to configure an interface when the peer has limited LACP capability. The interface selects the associated LAG by default, whether the switch and peer are both in active or passive mode. When PDUs are not received, the partner is considered to be working in the passive mode. Therefore, LACP PDU transmissions are controlled by the transmitting link.

If the remote end of the LAG link is a security device, LACP might not be supported because security devices require a deterministic configuration. In such a scenario, do not configure LACP. All links in the LAG are permanently operational unless the switch detects a link failure within the Ethernet physical layer or data link layers.

### Related Documentation

- Understanding EX Series Virtual Chassis Port Link Aggregation on page 4472
- Understanding Link Aggregation in an EX8200 Virtual Chassis
- Understanding Redundant Trunk Links on EX Series Switches on page 2068
Understanding Layer 3 Subinterfaces

A Layer 3 subinterface is a logical division of a physical interface that operates at the network level and therefore can receive and forward 802.1Q VLAN tags. You can use Layer 3 subinterfaces to route traffic among multiple VLANs along a single trunk line that connects a Juniper Networks EX Series Ethernet Switch to a Layer 2 switch. Only one physical connection is required between the switches. This topology is often called a router on a stick or a one-armed router when the Layer 3 device is a router.

To create Layer 3 subinterfaces on an EX Series switch, you enable VLAN tagging, partition the physical interface into logical partitions, and bind the VLAN ID to the logical interface.

You can partition one physical interface into up to 4094 different subinterfaces, one for each VLAN. We recommend that you use the VLAN ID as the subinterface number when you configure the subinterface. Juniper Networks Junos operating system (Junos OS) reserves VLAN IDs 0 and 4095.

VLAN tagging places the VLAN ID in the frame header, allowing each physical interface to handle multiple VLANs. When you configure multiple VLANs on an interface, you must also enable tagging on that interface. Junos OS on EX Series switches supports a subset of the 802.1Q standard for receiving and forwarding routed or bridged Ethernet frames with single VLAN tags and running Virtual Router Redundancy Protocol (VRRP) over 802.1Q-tagged interfaces. Double-tagging is not supported.
Understanding Unicast RPF for EX Series Switches

Unicast reverse-path forwarding (RPF) helps protect the switch against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by verifying the unicast source address of each packet that arrives on an ingress interface where unicast RPF is enabled. It also helps ensure that traffic arriving on ingress interfaces comes from a network source that the receiving interface can reach.

When you enable unicast RPF, the switch forwards a packet only if the receiving interface is the best return path to the packet's unicast source address. This is known as strict mode unicast RPF.

**NOTE:** On Juniper Networks EX3200, EX4200, and EX4300 Ethernet Switches, the switch applies unicast RPF *globally* to all interfaces when unicast RPF is configured on any interface. For additional information, see “Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches” on page 2279.

This topic covers:
- Unicast RPF for EX Series Switches Overview on page 2276
- Unicast RPF Implementation for EX Series Switches on page 2277
- When to Enable Unicast RPF on page 2277
- When Not to Enable Unicast RPF on page 2278
- Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches on page 2279

**Unicast RPF for EX Series Switches Overview**

Unicast RPF functions as an ingress filter that reduces the forwarding of IP packets that might be spoofing an address. By default, unicast RPF is disabled on the switch interfaces.

The type of unicast RPF provided on the switches—that is, strict mode unicast RPF—is especially useful on untrusted interfaces. An untrusted interface is an interface where untrusted users or processes can place packets on the network segment.

The switch supports only the active paths method of determining the best return path back to a unicast source address. The active paths method looks up the best reverse path entry in the forwarding table. It does not consider alternate routes specified using routing-protocol-specific methods when determining the best return path.

If the forwarding table lists the receiving interface as the interface to use to forward the packet back to its unicast source, it is the best return path interface. Strict mode unicast RPF recognizes only one best return path to a unicast source address.

Use strict mode unicast RPF only on symmetrically routed interfaces. (For information about symmetrically routed interfaces, see “When to Enable Unicast RPF” on page 2277.)
For more information about strict unicast RPF, see RFC 3704, Ingress Filtering for Multihomed Networks at http://www.ietf.org/rfc/rfc3704.txt.

Unicast RPF Implementation for EX Series Switches

This section includes:

- Unicast RPF Packet Filtering on page 2277
- Bootstrap Protocol (BOOTP) and DHCP Requests on page 2277
- Default Route Handling on page 2277

Unicast RPF Packet Filtering

When you enable unicast RPF on the switch, the switch handles traffic in the following manner:

- If the switch receives a packet on the interface that is the best return path to the unicast source address of that packet, the switch forwards the packet.
- If the best return path from the switch to the packet's unicast source address is not the receiving interface, the switch discards the packet.
- If the switch receives a packet that has a source IP address that does not have a routing entry in the forwarding table, the switch discards the packet.

Bootstrap Protocol (BOOTP) and DHCP Requests

Bootstrap protocol (BOOTP) and DHCP request packets are sent with a broadcast MAC address and therefore the switch does not perform unicast RPF checks on them. The switch forwards all BOOTP packets and DHCP request packets without performing unicast RPF checks.

Default Route Handling

If the best return path to the source is the default route (0.0.0.0) and the default route points to reject, the switch discards all unicast RPF packets. If the default route points to a valid network interface, the switch performs a normal unicast RPF check on the packets.

When to Enable Unicast RPF

Enable unicast RPF when you want to ensure that traffic arriving on a network interface comes from a source that resides on a network that that interface can reach. You can enable unicast RPF on untrusted interfaces to filter spoofed packets. For example, a common application for unicast RPF is to help defend an enterprise network from DoS/DDoS attacks coming from the Internet.

Enable unicast RPF only on symmetrically routed interfaces. A symmetrically routed interface uses the same route in both directions between the source and the destination, as shown in Figure 36 on page 2278. Symmetrical routing means that if an interface receives a packet, the switch uses the same interface to send a reply to the packet source (the receiving interface matches the forwarding-table entry for the best return path to the source).
Enabling unicast RPF on asymmetrically routed interfaces (where different interfaces receive a packet and reply to its source) results in packets from legitimate sources being filtered (discarded) because the best return path is not the same interface that received the packet.

The following switch interfaces are most likely to be symmetrically routed and thus are candidates for unicast RPF enabling:

- The service provider edge to a customer
- The customer edge to a service provider
- A single access point out of the network (usually on the network perimeter)
- A terminal network that has only one link

**NOTE:** Because unicast RPF is enabled globally on EX3200, EX4200, and EX4300 switches, ensure that all interfaces are symmetrically routed before you enable unicast RPF on these switches. Enabling unicast RPF on asymmetrically routed interfaces results in packets from legitimate sources being filtered.

**TIP:** Enabling unicast RPF as close as possible to the traffic source stops spoofed traffic before it can proliferate or reach interfaces that do not have unicast RPF enabled.

**When Not to Enable Unicast RPF**

Typically, you will not enable unicast RPF if:

- Switch interfaces are multihomed.
- Switch interfaces are trusted interfaces.
- BGP is carrying prefixes and some of those prefixes are not advertised or are not accepted by the ISP under its policy. (The effect in this case is the same as filtering an interface by using an incomplete access list.)
- Switch interfaces face the network core. Core-facing interfaces are usually asymmetrically routed.

An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination, as shown in Figure 37 on page 2279. This means
that if an interface receives a packet, that interface does not match the forwarding table entry as the best return path back to the source. If the receiving interface is not the best return path to the source of a packet, unicast RPF causes the switch to discard the packet even though it comes from a valid source.

**Figure 37: Asymmetrically Routed Interfaces**

![Diagram of Asymmetrically Routed Interfaces]

**NOTE:** Do not enable unicast RPF on EX3200, EX4200, and EX4300 switches if any switch interfaces are asymmetrically routed, because unicast RPF is enabled globally on all interfaces of these switches. All switch interfaces must be symmetrically routed for you to enable unicast RPF without the risk of the switch discarding traffic that you want to forward.

**Limitations of the Unicast RPF Implementation on EX3200, EX4200, and EX4300 Switches**

On EX3200, EX4200, and EX4300 switches, the switch implements unicast RPF on a global basis. You cannot enable unicast RPF on a per-interface basis. Unicast RPF is globally disabled by default.

- When you enable unicast RPF on any interface, it is automatically enabled on all switch interfaces, including link aggregation groups (LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs).
- When you disable unicast RPF on the interface (or interfaces) on which you enabled unicast RPF, it is automatically disabled on all switch interfaces.

**NOTE:** You must explicitly disable unicast RPF on every interface on which it was explicitly enabled or unicast RPF remains enabled on all switch interfaces.

The EX3200 and EX4200 switches do not perform unicast RPF filtering on equal-cost multipath (ECMP) traffic. The unicast RPF check examines only one best return path to the packet source, but ECMP traffic employs an address block consisting of multiple paths.

Using unicast RPF to filter ECMP traffic on EX3200 and EX4200 switches can result in the switch discarding packets that you want to forward because the unicast RPF filter does not examine the entire ECMP address block.
Understanding IP Directed Broadcast for EX Series Switches

IP directed broadcast helps you implement remote administration tasks such as backups and wake-on-LAN (WOL) application tasks by sending broadcast packets targeted at the hosts in a specified destination subnet. IP directed broadcast packets traverse the network in the same way as unicast IP packets until they reach the destination subnet. When they reach the destination subnet and IP directed broadcast is enabled on the receiving switch, the switch translates (explodes) the IP directed broadcast packet into a broadcast that floods the packet on the target subnet. All hosts on the target subnet receive the IP directed broadcast packet.

This topic covers:

- IP Directed Broadcast for EX Series Switches Overview on page 2280
- IP Directed Broadcast Implementation for EX Series Switches on page 2280
- When to Enable IP Directed Broadcast on page 2281
- When Not to Enable IP Directed Broadcast on page 2281

IP Directed Broadcast for EX Series Switches Overview

IP directed broadcast packets have a destination IP address that is a valid broadcast address for the subnet that is the target of the directed broadcast (the target subnet). The intent of an IP directed broadcast is to flood the target subnet with the broadcast packets without broadcasting to the entire network. IP directed broadcast packets cannot originate from the target subnet.

When you send an IP directed broadcast packet, as it travels to the target subnet, the network forwards it in the same way as it forwards a unicast packet. When the packet reaches a switch that is directly connected to the target subnet, the switch checks to see whether IP directed broadcast is enabled on the interface that is directly connected to the target subnet:

- If IP directed broadcast is enabled on that interface, the switch broadcasts the packet on that subnet by rewriting the destination IP address as the configured broadcast IP address for the subnet. The switch converts the packet to a link-layer broadcast packet that every host on the network processes.
- If IP directed broadcast is disabled on the interface that is directly connected to the target subnet, the switch drops the packet.

IP Directed Broadcast Implementation for EX Series Switches

You configure IP directed broadcast on a per-subnet basis by enabling IP directed broadcast on the Layer 3 interface of the subnet’s VLAN. When the switch that is
connected to that subnet receives a packet that has the subnet’s broadcast IP address as the destination address, the switch broadcasts the packet to all hosts on the subnet.

By default, IP directed broadcast is disabled.

**When to Enable IP Directed Broadcast**

IP directed broadcast is disabled by default. Enable IP directed broadcast when you want to perform remote management or administration services such as backups or WOL tasks on hosts in a subnet that does not have a direct connection to the Internet.

Enabling IP directed broadcast on a subnet affects only the hosts within that subnet. Only packets received on the subnet’s Layer 3 interface that have the subnet’s broadcast IP address as the destination address are flooded on the subnet.

**When Not to Enable IP Directed Broadcast**

Typically, you do not enable IP directed broadcast on subnets that have direct connections to the Internet. Disabling IP directed broadcast on a subnet’s Layer 3 interface affects only that subnet. If you disable IP directed broadcast on a subnet and a packet that has the broadcast IP address of that subnet arrives at the switch, the switch drops the broadcast packet.

If a subnet has a direct connection to the Internet, enabling IP directed broadcast on it increases the network’s susceptibility to denial-of-service (DoS) attacks.

For example, a malicious attacker can spoof a source IP address (use a source IP address that is not the actual source of the transmission to deceive a network into identifying the attacker as a legitimate source) and send IP directed broadcasts containing Internet Control Message Protocol (ICMP) echo (ping) packets. When the hosts on the network with IP directed broadcast enabled receive the ICMP echo packets, they all send replies to the victim that has the spoofed source IP address. This creates a flood of ping replies in a DoS attack that can overwhelm the spoofed source address; this is known as a smurf attack. Another common DoS attack on exposed networks with IP directed broadcast enabled is a fraggle attack, which is similar to a smurf attack except that the malicious packet is a User Datagram Protocol (UDP) echo packet instead of an ICMP echo packet.

**Related Documentation**

- Example: Configuring IP Directed Broadcast on an EX Series Switch
- Configuring IP Directed Broadcast (CLI Procedure)
- Configuring IP Directed Broadcast (CLI Procedure) on page 2349

**Understanding Interface Ranges on EX Series Switches**

**NOTE:** This concept uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Understanding Interface Ranges on EX Series Switches. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Copyright © 2013, Juniper Networks, Inc. 2281
You can use the interface ranges to group interfaces of the same type that share a common configuration profile. This helps reduce the time and effort in configuring interfaces on Juniper Networks EX Series Ethernet Switches. The configurations common to all the interfaces can be included in the interface range definition.

The interface range definition contains the name of the interface range defined, the names of the individual member interfaces that do not fall in a series of interfaces, a range of interfaces defined in the member range, and the configuration statements common to all the interfaces. An interface range defined with member ranges and individual members but without any common configurations, is also a valid definition.

**NOTE:** The interface range definition is supported only for Gigabit, 10-Gigabit, 40-Gigabit, and Fast Ethernet interfaces.

The common configurations defined in the interface range will be overridden by the local configuration.

The defined interface ranges can be used at places where the `interface` node is used in the following configuration hierarchies:

- `forwarding-options analyzer name input egress interface`
- `forwarding-options analyzer name input ingress interface`
- `poe interface`
- `protocols dot1x authenticator interface`
- `protocols igmp interface`
- `protocols isis interface`
- `protocols layer2-control bpdu-block interface`
- `protocols link-management peer name lmp-control-channel`
- `protocols link-management te-link name interface`
- `protocols lldp interface`
- `protocols lldp-med interface`
- `protocols mstp interface`
- `protocols oam ethernet link-fault-management interface`
- `protocols ospf area area-id interface`
- `protocols pim interface`
- `protocols router-advertisement interface`
- `protocols router-discovery interface`
- `protocols rsvp interface`
- `protocols sflow interfaces`
Related Documentation:

- protocols vstp vlan vlan-id interface
- switch-options redundant-trunk-group group-name interface
- switch-options voip interface

802.1Q VLANs Overview

For Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet interfaces supporting VPLS, the Junos OS supports a subset of the IEEE 802.1Q standard for channelizing an Ethernet interface into multiple logical interfaces, allowing many hosts to be connected to the same Gigabit Ethernet switch, but preventing them from being in the same routing or bridging domain.

For more information, visit the following related documentation:

- Configuring Dynamic 802.1Q VLANs
- 802.1Q VLAN IDs and Ethernet Interface Types
- Enabling VLAN Tagging
- Binding VLAN IDs to Logical Interfaces
- Configuring VLAN Encapsulation
- Configuring Extended VLAN Encapsulation
- Guidelines for Configuring VLAN ID List-Bundled Logical Interfaces That Connect CCCs
- Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface
- Configuring a VLAN-Bundled Logical Interface to Support a Layer 2 VPN Routing Instance
- Specifying the Interface Over Which VPN Traffic Travels to the CE Router
- Specifying the Interface to Handle Traffic for a CCC
- Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface
- Configuring a VLAN-Bundled Logical Interface to Support a Layer 2 VPN Routing Instance
- Specifying the Interface to Handle Traffic for a CCC Connected to the Layer 2 Circuit
- Example: Configuring a Layer 2 VPN Routing Instance on a VLAN-Bundled Logical Interface
- Example: Configuring a Layer 2 Circuit on a VLAN-Bundled Logical Interface
- Configuring a Logical Interface for Access Mode
- Configuring a Logical Interface for Trunk Mode
• Configuring the VLAN ID List for a Trunk Interface
• Configuring a Trunk Interface on a Bridge Network
• Ethernet Interfaces
CHAPTER 45

Configuration

- Configuration Tasks on page 2285
- Configuration Statements on page 2351

Configuration Tasks

- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
- Port Role Configuration with the J-Web Interface (with CLI References) on page 2295
- Adding a Logical Unit Description to the Configuration on page 2299
- Disabling a Physical Interface on page 2299
- Disabling a Logical Interface on page 2301
- Configuring Flow Control on page 2301
- Configuring the Interface Address on page 2302
- Configuring the Interface Bandwidth on page 2306
- Configuring the Media MTU on page 2307
- Setting the Protocol MTU on page 2318
- Interface Ranges on page 2319
- Configuring Accounting for the Physical Interface on page 2327
- Configuring Accounting for the Logical Interface on page 2329
- Configuring Ethernet Loopback Capability on page 2330
- Configuring Gratuitous ARP on page 2331
- Configuring Static ARP Table Entries on page 2332
- Disabling the Transmission of Redirect Messages on an Interface on page 2333
- Configuring Restricted and Unrestricted Proxy ARP on page 2333
- Enabling or Disabling SNMP Notifications on Logical Interfaces on page 2334
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring Aggregated Ethernet Interfaces (J-Web Procedure) on page 2336
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
An Ethernet interface must be configured for optimal performance in a high-traffic network. EX Series switches include a factory default configuration that:

- Enables all the network interfaces on the switch
- Sets a default interface mode (access)
- Sets default link settings
- Specifies a logical unit (unit 0) and assigns it to `family ethernet-switching` (except on EXB200 switches and Virtual Chassis)
- Specifies Rapid Spanning Tree Protocol (RSTP) and Link Layer Discovery Protocol (LLDP)

This topic describes:

- Configuring VLAN Options and Interface Mode
- Configuring the Link Settings
- Configuring the IP Options

**Configuring VLAN Options and Interface Mode**

By default, when you boot a switch and use the factory default configuration, or when you boot the switch and do not explicitly configure a port mode, all interfaces on the switch are in access mode and accept only untagged packets from the VLAN named `default`. You can optionally configure another VLAN and use that instead of `default`. You
can also configure a port to accept untagged packets from the user-configured VLAN. For details on this concept (native VLAN), see “Understanding Bridging and VLANs on EX Series Switches” on page 2049.

If you are connecting either a desktop phone, wireless access point or a security camera to a Power over Ethernet (PoE) port, you can configure some parameters for the PoE interface. PoE interfaces are enabled by default. For detailed information about PoE settings, see “Configuring PoE (CLI Procedure)” on page 3942.

If you are connecting a device to other switches and to routers on the LAN, you need to assign the interface to a logical port and configure the logical port as a trunk port. See “Port Role Configuration with the J-Web Interface (with CLI References)” on page 2295 for more information about port configuration.

If you are connecting to a server that contains virtual machines and a VEPA for packet aggregation from those virtual machines, configure the port as a tagged-access port. See “Understanding Bridging and VLANs on EX Series Switches” on page 2049 for more information about tagged access.

To configure a Gigabit Ethernet interface or 10-Gigabit Ethernet interface for trunk port mode:

```
[edit]
user@switch# set interfaces interface-name unit logical-unit-number family ethernet-switching interface-mode trunk
```

**Configuring the Link Settings**

EX Series switches include a factory default configuration that enables interfaces with the following link settings:

- All Gigabit Ethernet interfaces are set to auto-negotiation.
- The speed for Gigabit Ethernet interfaces is set to auto, allowing the interface to operate at 10m, 100m, or 1g. The link operates at the highest possible speed, depending on the capabilities of the remote end.
- The flow control for Gigabit Ethernet interfaces and 10-Gigabit Ethernet interfaces is set to enabled.
- The link mode is set to auto, allowing the interface to operate as either full duplex or half duplex. The link operates as full duplex unless this mode is not supported at the remote end.
- The 10-Gigabit Ethernet interfaces default to no auto-negotiation. The default speed is 10g and the default link mode is full duplex.
To configure the link settings:

- Set link settings for a Gigabit Ethernet interface:
  
  ```
  [edit]
  user@switch# set interfaces ge-fpc/pic/port ether-options
  ```

- Set link settings for a 10-Gigabit Ethernet interface:
  
  ```
  [edit]
  user@switch# set interfaces xe-fpc/pic/port ether-options
  ```

- Set link settings for a 40-Gigabit Ethernet interface:
  
  ```
  [edit]
  user@switch# set interfaces et-fpc/pic/port ether-options
  ```

For detailed information about the FPC, PIC, and port numbers used for EX Series switches, see “Understanding Interface Naming Conventions on EX Series Switches” on page 2270.

The `ether-options` statement allows you to modify the configuration:

- 802.3ad—Specify an aggregated Ethernet bundle. See “Configuring Aggregated Ethernet Links (CLI Procedure)” on page 2335.
- auto-negotiation—Enable or disable autonegotiation of flow control, link mode, and speed.
- flow-control—Enable or disable flow control.
- loopback—Enable or disable loopback mode.

### Configuring the IP Options

To specify an IP address for the logical unit using IPv4:

```
[edit]
user@switch# set interfaces interface-name unit logical-unit-number family inet address ip-address
```

To specify an IP address for the logical unit using IPv6:

```
[edit]
user@switch# set interfaces interface-name unit logical-unit-number family inet6 address ip-address
```

**NOTE:** Access interfaces on EX2200, EX3200, EX3300, EX4200, EX4300, and EX4500 switches are set to family ethernet-switching by default. You might have to delete this or any other user-configured family setting before changing the setting to family inet or family inet6.

**Related Documentation**

- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
- Monitoring Interface Status and Traffic on page 2463
- `show interfaces ge-` on page 2493
- `show interfaces xe-` on page 2524
- Understanding Interface Naming Conventions on EX Series Switches on page 2270
Configuring Gigabit Ethernet Interfaces (J-Web Procedure)

You can configure specific properties on your Ethernet interface to ensure optimal performance of your network in a high-traffic environment.

To configure properties on a Gigabit Ethernet interface, a 10-Gigabit Ethernet interface, and a 40-Gigabit Ethernet interface on an EX Series switch:

1. Select Interfaces > Ports.

The page that is displayed lists Gigabit Ethernet, 10-Gigabit Ethernet interfaces, and 40-Gigabit Ethernet interfaces, and their link statuses.

NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See “Using the Commit Options to Commit Configuration Changes (J-Web Procedure)” on page 511 for details about all commit options.

2. Select the interface you want to configure. For an EX8200 Virtual Chassis configuration, select the member and the FPC slot if the interface you want to configure is not listed under Ports in the top table on the page.

Details for the selected interface, such as administrative status, link status, speed, duplex, and flow control, are displayed in the Details of port table on the page.

NOTE: You can select multiple interfaces and modify their settings at the same time. However, while doing this, you cannot modify the IP address or enable or disable the administrative status of the selected interfaces.

NOTE: In the J-Web interface, you cannot configure interface ranges and interface groups.

3. Click Edit and select the set of options you want to configure first:
• Port Role—Enables you to assign a profile for the selected interface.

NOTE: When you select a particular port role, preconfigured port security parameters are set for the VLAN that the interface belongs to. For example, if you select the port role Desktop, the port security options examine-dhcp and arp-inspection are enabled on the VLAN that the interface belongs to. If there are interfaces in the VLAN that have static IP addresses, those interfaces might lose connectivity because those static IP addresses might not be present in the DHCP pool. Therefore, when you select a port role, ensure that the corresponding port security settings for the VLAN are applicable to the interface.

For basic information about port security features such as DHCP snooping (CLI option examine-dhcp) or dynamic ARP inspection (DAI) (CLI option arp-inspection), see “Configuring Port Security (J-Web Procedure)” on page 4024. For detailed descriptions of port security features, see the Port Security topics in the EX Series documentation at http://www.juniper.net/techpubs/.

Click Details to view the configuration parameters for the selected port role.

• VLAN—Enables you to configure VLAN options for the selected interface.

• Link—Enables you to modify the following link options for the selected interface:
  - Speed
  - MTU
  - Autonegotiation
  - Flow Control
  - Duplex
  - Media Type

• IP—Enables you to configure an IP address for the interface.

4. Configure the interface by configuring options in the selected option set. See Table 285 on page 2291 for details of the options.

5. Repeat Steps 3 and 4 for the remaining option sets that you want to configure for the interface.

NOTE: To enable or disable the administrative status of a selected interface, click Enable Port or Disable Port.
### Table 285: Port Edit Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Role Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Role</td>
<td>Specifies a profile (role) to assign to the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> After a port role is configured on the interface, you cannot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>specify VLAN options or IP options.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Port roles are not supported by the et interfaces (40-Gigabit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ethernet interfaces) on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only the following port roles can be applied on EX8200 switch</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interfaces:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Layer 2 uplink</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Routed uplink</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Applies the default role.</td>
<td>1. Click <strong>Details</strong> to view CLI commands for this role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>The interface family is set to <strong>ethernet-switching</strong>, port mode is set</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to <strong>access</strong>, and RSTP is enabled.</td>
<td></td>
</tr>
<tr>
<td>Desktop</td>
<td>Applies the desktop role.</td>
<td>1. Select an existing VLAN configuration or type the name of a new VLAN</td>
</tr>
<tr>
<td></td>
<td>The interface family is set to <strong>ethernet-switching</strong>, port mode is set</td>
<td>configuration to be associated with the interface.</td>
</tr>
<tr>
<td></td>
<td>to <strong>access</strong>, RSTP is enabled with the <strong>edge</strong> and <strong>point-to-point</strong></td>
<td>2. Click <strong>Details</strong> to view CLI commands for this role.</td>
</tr>
<tr>
<td></td>
<td>options, and port security parameters (MAC limit =1; dynamic ARP</td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>inspection and DHCP snooping enabled) are set.</td>
<td></td>
</tr>
<tr>
<td>Desktop and Phone</td>
<td>Applies the desktop and phone role.</td>
<td>1. Select an existing VLAN configuration or type the name of a new VLAN</td>
</tr>
<tr>
<td></td>
<td>The interface family is set to <strong>ethernet-switching</strong>, port mode is set</td>
<td>configuration to be associated with the interface.</td>
</tr>
<tr>
<td></td>
<td>to <strong>access</strong>, port security parameters (MAC limit =1; dynamic ARP TCP/IP</td>
<td>You can also select an existing VoIP VLAN configuration or a new VoIP VLAN</td>
</tr>
<tr>
<td></td>
<td>inspection and DHCP snooping enabled) are set, and recommended class-of-</td>
<td>configuration to be associated with the interface.</td>
</tr>
<tr>
<td></td>
<td>service (CoS) parameters (MAC limit =1; dynamic ARP inspection and DHCP</td>
<td><strong>NOTE:</strong> VoIP is not supported on EX8200 switches.</td>
</tr>
<tr>
<td></td>
<td>snooping enabled) are set, and recommended class-of-service (CoS)</td>
<td>2. Click <strong>Details</strong> to view CLI commands for this role.</td>
</tr>
<tr>
<td></td>
<td>parameters are specified for forwarding classes, schedulers,</td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>and classifiers. See <strong>Table 286 on page 2294</strong> for more CoS information.</td>
<td></td>
</tr>
<tr>
<td>Wireless Access</td>
<td>Applies the wireless access point role.</td>
<td>1. Select an existing VLAN configuration or type the name of a new VLAN</td>
</tr>
<tr>
<td>Access Point</td>
<td>The interface family is set to <strong>ethernet-switching</strong>, port mode is set</td>
<td>configuration to be associated with the interface.</td>
</tr>
<tr>
<td></td>
<td>to <strong>access</strong>, and RSTP is enabled with the <strong>edge</strong> and <strong>point-to-point</strong></td>
<td>Type the VLAN ID for a new VLAN.</td>
</tr>
<tr>
<td></td>
<td>options.</td>
<td>2. Click <strong>Details</strong> to view CLI commands for this role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
### Table 285: Port Edit Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed Uplink</td>
<td>Applies the routed uplink role.</td>
<td>To specify an IPv4 address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select the <strong>IPv4 address</strong> check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Type an IP address—for example: <strong>10.10.10.10</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the subnet mask or address prefix. For example, 24 bits represents <strong>255.255.255.0</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> IPv6 is not supported on EX2200 VC switches.</td>
</tr>
<tr>
<td>Layer 2 Uplink</td>
<td>Applies the Layer 2 uplink role.</td>
<td>To specify an IPv6 address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select the <strong>IPv6 address</strong> check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Type an IP address—for example: <strong>2001:ab8:85a3::8a2e:370:7334</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the subnet mask or address prefix.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> IPv6 is not supported on EX2200 VC switches.</td>
</tr>
<tr>
<td>None</td>
<td>Specifies that no port role is configured for the selected interface.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** For an EX8200 switch, dynamic ARP inspection and DHCP snooping parameters are not configured.
Table 285: Port Edit Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Mode</td>
<td>Specifies the mode of operation for the interface: trunk or access.</td>
<td>If you select <strong>Trunk</strong>, you can:&lt;br&gt;1. Click <strong>Add</strong> to add a VLAN member.&lt;br&gt;2. Select the VLAN and click <strong>OK</strong>.&lt;br&gt;3. (Optional) Associate a native VLAN with the interface.&lt;br&gt;4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Link Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmission unit size (MTU) for the interface.</td>
<td>Type a value from 256 through 9216. The default MTU size for Gigabit Ethernet interfaces is 1514.</td>
</tr>
<tr>
<td>Speed</td>
<td>Specifies the speed for the mode.</td>
<td>Select one of the following values: <strong>10 Mbps</strong>, <strong>100 Mbps</strong>, <strong>1000 Mbps</strong>, or <strong>Auto-Negotiation</strong>.&lt;br&gt;&lt;br&gt;<strong>NOTE:</strong> EX4300 switches supports <strong>Auto-Negotiation 10M-100M</strong> apart from the values mentioned above.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Specifies the link mode.</td>
<td>Select one: <strong>automatic</strong>, <strong>half</strong>, or <strong>full</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> Link mode <strong>half</strong> is not supported on EX4300 switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the link.</td>
<td>Enter a brief description for the link.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If the interface is part of a link aggregation group (LAG), only the Description option is enabled. Other Port Edit options are unavailable.</td>
</tr>
<tr>
<td>Enable Auto</td>
<td>Enables or disables autonegotiation.</td>
<td>Select the check box to enable autonegotiation, or clear the check box to disable it. By default, autonegotiation is enabled.</td>
</tr>
<tr>
<td>Negotiation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable Flow</td>
<td>Enables or disables flow control.</td>
<td>Select the check box to enable flow control to regulate the amount of traffic sent out of the interface, or clear the check box to disable flow control and permit unrestricted traffic. Flow control is enabled by default.</td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Type</td>
<td>Specifies the media type selected.</td>
<td>Select the check box to enable the media type. Then select <strong>Copper</strong> or <strong>Fiber</strong>.</td>
</tr>
</tbody>
</table>
Table 285: Port Edit Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Options</td>
<td></td>
<td>1. Select the IPv4 address check box to specify an IPv4 address.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>Specifies an IPv4 address for the interface.</td>
<td>2. Type an IP address—for example: 10.10.10.10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the subnet mask or address prefix. For example, 24 bits represents 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click OK.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Specifies an IPv6 address for the interface.</td>
<td>1. Select the IPv6 address check box to specify an IPv6 address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Type an IP address—for example: 2001:ab8:85a3::8a2e:370:7334.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the subnet mask or address prefix.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click OK.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If the IPv6 Address check box is cleared, the interface still belongs to the inet family.</td>
<td></td>
</tr>
</tbody>
</table>

Table 286: Recommended CoS Settings for Port Roles

<table>
<thead>
<tr>
<th>CoS Parameter</th>
<th>Recommended Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Classes</td>
<td>There are four forwarding classes:</td>
</tr>
<tr>
<td></td>
<td>• voice—Queue number is set to 7.</td>
</tr>
<tr>
<td></td>
<td>• expedited-forwarding—Queue number is set to 5.</td>
</tr>
<tr>
<td></td>
<td>• assured-forwarding—Queue number is set to 1.</td>
</tr>
<tr>
<td></td>
<td>• best-effort—Queue number is set to 0.</td>
</tr>
<tr>
<td>Schedulers</td>
<td>The schedulers and their settings are:</td>
</tr>
<tr>
<td></td>
<td>• Strict-priority—Transmission rate is set to 10 percent and buffer size to 5 percent.</td>
</tr>
<tr>
<td></td>
<td>• Expedited-scheduler—Transmission rate is set to 30 percent, buffer size to 30 percent, and priority to low.</td>
</tr>
<tr>
<td></td>
<td>• Assured-scheduler—Transmission rate is set to 25 percent, buffer size to 25 percent, and priority to low.</td>
</tr>
<tr>
<td></td>
<td>• Best-effort scheduler—Transmission rate is set to 35 percent, buffer size to 40 percent, and priority to low.</td>
</tr>
<tr>
<td>Scheduler maps</td>
<td>When a desktop and phone, routed uplink, or Layer 2 uplink role is applied on an interface, the forwarding classes and schedulers are mapped using the scheduler map.</td>
</tr>
<tr>
<td>ieee-802.1 classifier</td>
<td>Imports the default ieee-802.1 classifier configuration and sets the loss priority to low for the code point 101 for the voice forwarding class.</td>
</tr>
<tr>
<td>dscp classifier</td>
<td>Imports the default dscp classifier configuration and sets the loss priority to low for the code point 101110 for the voice forwarding class.</td>
</tr>
</tbody>
</table>
Port Role Configuration with the J-Web Interface (with CLI References)

When you configure Gigabit Ethernet interface properties with the J-Web interface (Configure > Interfaces) you can optionally select pre-configured port roles for those interfaces. When you select a role from the Port Role field and apply it to a port, the J-Web interface modifies the switch configuration using CLI commands. Table 287 on page 2295 lists the CLI commands applied for each port role.

**NOTE:** If there is an existing port role configuration, it is cleared before the new port role configuration is applied.

### Table 287: Port Role Configuration Summary

<table>
<thead>
<tr>
<th>Configuration Description</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Port Role</strong></td>
<td></td>
</tr>
<tr>
<td>Set the port role to <strong>Default</strong>.</td>
<td><code>set interfaces interface apply-macro juniper-port-profile Default</code></td>
</tr>
<tr>
<td>Set port family to <strong>ethernet-switching</strong>.</td>
<td><code>set interfaces interface unit 0 family ethernet-switching port-mode access</code></td>
</tr>
<tr>
<td>Set port mode to <strong>access</strong>.</td>
<td></td>
</tr>
<tr>
<td>Enable RSTP if redundant trunk groups are not configured.</td>
<td><code>delete protocols rstp interface interface disable</code></td>
</tr>
<tr>
<td>Disable RSTP if redundant trunk groups are configured.</td>
<td><code>set protocols rstp interface interface disable</code></td>
</tr>
<tr>
<td><strong>Desktop Port Role</strong></td>
<td></td>
</tr>
<tr>
<td>Set the port role to desktop.</td>
<td><code>set interfaces interface apply-macro juniper-port-profile Desktop</code></td>
</tr>
<tr>
<td>Set VLAN if new VLAN is specified.</td>
<td><code>set vlans &lt;vlan name&gt; vlan-id &lt;vlan-id&gt;</code></td>
</tr>
<tr>
<td>Set port family to <strong>ethernet-switching</strong>.</td>
<td><code>set interfaces interface unit 0 family ethernet-switching port-mode access</code></td>
</tr>
<tr>
<td>Set Port Mode to <strong>Access</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Table 287: Port Role Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Configuration Description</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set VLAN if new VLAN is specified.</td>
<td>set interfaces interface unit 0 family ethernet-switching vlan members vlan-members</td>
</tr>
<tr>
<td>Set port security parameters.</td>
<td>set ethernet-switching-options secure-access-port vlan MacTest arp-inspection</td>
</tr>
<tr>
<td>Set RSTP protocol with edge option.</td>
<td>set protocols rstp interface interface edge</td>
</tr>
<tr>
<td>RSTP protocol is disabled if redundant trunk groups are configured.</td>
<td>set protocols rstp interface interface disable</td>
</tr>
<tr>
<td>Desktop and Phone Port Role</td>
<td></td>
</tr>
<tr>
<td>Set the port role to desktop and phone.</td>
<td>set interfaces interface apply-macro juniper-port-profile Desktop and Phone</td>
</tr>
<tr>
<td>Set data VLAN if new VLAN is specified.</td>
<td>set vlans vlan-name vlan-id vlan id</td>
</tr>
<tr>
<td>Set voice VLAN if new voice VLAN is specified.</td>
<td></td>
</tr>
<tr>
<td>Set port family to ethernet-switching.</td>
<td>set interfaces interface unit 0 family ethernet-switching port-mode access</td>
</tr>
<tr>
<td>Set Port Mode to access.</td>
<td></td>
</tr>
<tr>
<td>Set data VLAN on port stanza.</td>
<td>set interfaces interface unit 0 family ethernet-switching vlan members vlan-members</td>
</tr>
<tr>
<td>Set port security parameters.</td>
<td>set ethernet-switching-options secure-access-port vlan MacTest arp-inspection</td>
</tr>
<tr>
<td>Set VOIP VLAN.</td>
<td>set ethernet-switching-options voip interface interface.0 vlan vlan vlan name</td>
</tr>
<tr>
<td>Set class of service parameters</td>
<td>set class-of-service interfaces scheduler-map juniper-port-profile-map</td>
</tr>
<tr>
<td>SCHEDULER_MAP=juniper-port-profile-map</td>
<td>set class-of-service interfaces interface unit 0 classifiers ieee-802.1 juniper_ieee_classifier</td>
</tr>
<tr>
<td>IEEE_CLASSIFIER=juniper-ieee-classifier</td>
<td>set class-of-service interfaces interface unit 0 classifiers dscp juniper-dscp-classifier</td>
</tr>
<tr>
<td>DSCP_CLASSIFIER=juniper-dscp-classifier</td>
<td></td>
</tr>
<tr>
<td>Set CoS Configuration</td>
<td>Refer Table 288 on page 2298 for details.</td>
</tr>
<tr>
<td>Wireless Access Point Port Role</td>
<td></td>
</tr>
<tr>
<td>Set the port role to wireless access point.</td>
<td>set interfaces interface apply-macro juniper-port-profile Wireless Access Point</td>
</tr>
<tr>
<td>Set VLAN on VLANs stanza.</td>
<td>set vlans vlan name vlan-id vlan-id</td>
</tr>
<tr>
<td>Set port family to ethernet-switching</td>
<td>set interfaces interface unit 0 family ethernet-switching port-mode access</td>
</tr>
<tr>
<td>Set port mode to Access.</td>
<td></td>
</tr>
<tr>
<td>Set VLAN on port stanza.</td>
<td>set interfaces interface unit 0 family ethernet-switching vlan members vlan-members</td>
</tr>
</tbody>
</table>
### Table 287: Port Role Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Configuration Description</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set RSTP protocol with edge option.</td>
<td><code>set protocols rstp interface interface edge</code></td>
</tr>
<tr>
<td>RSTP protocol is disabled if redundant trunk groups are configured.</td>
<td><code>set protocols rstp interface interface disable</code></td>
</tr>
</tbody>
</table>

**Routed Uplink Port Role**

<table>
<thead>
<tr>
<th>CLI Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>apply-macro juniper-port-profile</code></td>
<td>Set the port role to Routed Uplink.</td>
</tr>
<tr>
<td><code>set interfaces unit 0 family inet address ipaddress</code></td>
<td>Set port family to inet. Set IP address on the port.</td>
</tr>
<tr>
<td><code>set class-of-service interfaces scheduler-map juniper-port-profile-map</code></td>
<td>Set class-of-service parameters.</td>
</tr>
<tr>
<td><code>set class-of-service interfaces unit 0 classifiers ieee-802.1 juniper_ieee_classifier</code></td>
<td></td>
</tr>
<tr>
<td><code>set class-of-service interfaces unit 0 classifiers dscp juniper_dscp-classifier</code></td>
<td></td>
</tr>
</tbody>
</table>

Set CoS configuration: Refer Table 288 on page 2298 for details.

**Layer 2 Uplink Port Role**

<table>
<thead>
<tr>
<th>CLI Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>apply-macro juniper-port-profile</code></td>
<td>Set the port role to Layer 2 Uplink.</td>
</tr>
<tr>
<td><code>set interfaces unit 0 family ethernet-switching port-mode trunk</code></td>
<td>Set port family to ethernet-switching. Set port mode to trunk.</td>
</tr>
<tr>
<td><code>set interfaces unit 0 family ethernet-switching native-vlan-id vlan-name</code></td>
<td>Set Native VLAN name.</td>
</tr>
<tr>
<td><code>set interfaces unit 0 family ethernet-switching vlan members vlan-members</code></td>
<td>Set the port as part of all valid VLANs; &quot;valid&quot; refers to all VLANs except native VLAN and voice VLANs.</td>
</tr>
<tr>
<td><code>set ethernet-switching-options secure-access-port dhcp-trusted</code></td>
<td>Set port security parameter.</td>
</tr>
<tr>
<td><code>set protocols rstp interface interface mode point-to-point</code></td>
<td>Set RSTP protocol with point-to-point option.</td>
</tr>
<tr>
<td><code>set protocols rstp interface interface disable</code></td>
<td>Disable RSTP if redundant trunk groups are configured.</td>
</tr>
<tr>
<td><code>set class-of-service interfaces scheduler-map juniper-port-profile-map</code></td>
<td>Set class-of-service parameters.</td>
</tr>
<tr>
<td><code>set class-of-service interfaces unit 0 classifiers ieee-802.1 juniper_ieee_classifier</code></td>
<td></td>
</tr>
<tr>
<td><code>set class-of-service interfaces unit 0 classifiers dscp juniper_dscp-classifier</code></td>
<td></td>
</tr>
</tbody>
</table>
Table 287: Port Role Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Configuration Description</th>
<th>CLI Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set CoS configuration</td>
<td>Refer to Table 288 on page 2298 for details.</td>
</tr>
</tbody>
</table>

Table 288 on page 2298 lists the CLI commands for the recommended CoS settings that are committed when the CoS configuration is set.

Table 288: Recommended CoS Settings for Port Roles

<table>
<thead>
<tr>
<th>CoS Parameter</th>
<th>CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forwarding Classes</strong></td>
<td></td>
</tr>
<tr>
<td>voice</td>
<td>set class-of-service forwarding-classes class voice queue-num 7</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>set class-of-service forwarding-classes class expedited-forwarding queue-num 5</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>set class-of-service forwarding-classes class assured-forwarding queue-num 1</td>
</tr>
<tr>
<td>best-effort</td>
<td>set class-of-service forwarding-classes class best-effort queue-num 0</td>
</tr>
<tr>
<td><strong>Schedulers</strong></td>
<td></td>
</tr>
<tr>
<td>strict-priority-scheduler</td>
<td>The CLI commands are:</td>
</tr>
<tr>
<td></td>
<td>• set class-of-service schedulers strict-priority-scheduler transmit-rate percent 10</td>
</tr>
<tr>
<td></td>
<td>• set class-of-service schedulers strict-priority-scheduler buffer-size percent 5</td>
</tr>
<tr>
<td></td>
<td>• set class-of-service schedulers strict-priority-scheduler priority strict-high</td>
</tr>
<tr>
<td>expedited-scheduler</td>
<td>The CLI commands are:</td>
</tr>
<tr>
<td></td>
<td>• set class-of-service schedulers expedited-scheduler transmit-rate percent 30</td>
</tr>
<tr>
<td></td>
<td>• set class-of-service schedulers expedited-scheduler buffer-size percent 30</td>
</tr>
<tr>
<td></td>
<td>• set class-of-service schedulers expedited-scheduler priority low</td>
</tr>
<tr>
<td>assured-scheduler</td>
<td>The CLI commands are:</td>
</tr>
<tr>
<td></td>
<td>set class-of-service schedulers assured-scheduler transmit-rate percent 25</td>
</tr>
<tr>
<td></td>
<td>set class-of-service schedulers assured-scheduler buffer-size percent 25</td>
</tr>
<tr>
<td>best-effort-scheduler</td>
<td>The CLI commands are:</td>
</tr>
<tr>
<td></td>
<td>set class-of-service schedulers best-effort-scheduler transmit-rate percent 35</td>
</tr>
<tr>
<td></td>
<td>set class-of-service schedulers best-effort-scheduler buffer-size percent 40</td>
</tr>
<tr>
<td></td>
<td>set class-of-service schedulers best-effort-scheduler priority low</td>
</tr>
</tbody>
</table>
Table 288: Recommended CoS Settings for Port Roles (continued)

<table>
<thead>
<tr>
<th>CoS Parameter</th>
<th>CLI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifiers</td>
<td>The classifiers are:</td>
</tr>
<tr>
<td></td>
<td>set class-of-service classifiers ieee-802.1 juniper_ieee_classifier import default forwarding-class voice loss-priority low code-points 101</td>
</tr>
<tr>
<td></td>
<td>set class-of-service classifiers dscp juniper_dscp_classifier import default forwarding-class voice loss-priority low code-points 101110</td>
</tr>
</tbody>
</table>

Related Documentation
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286

Adding a Logical Unit Description to the Configuration

You can include a text description of each logical unit in the configuration file. Any descriptive text you include is displayed in the output of the `show interfaces` commands, and is also exposed in the `ifAlias` Management Information Base (MIB) object. It has no impact on the interface’s configuration. To add a text description, include the `description` statement:

```
description text;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

The description can be a single line of text. If the text contains spaces, enclose it in quotation marks.

**NOTE:** You can configure the extended DHCP relay to include the interface description in the option 82 Agent Circuit ID suboption. See “Enabling and Disabling Insertion of Option 82 Information” on page 1303” in the Junos OS Subscriber Management and Services Library.

For information about describing physical interfaces, see Configuring Interface Description.

Disabling a Physical Interface

You can disable a physical interface, marking it as being down, without removing the interface configuration statements from the configuration. To do this, include the `disable` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
disable;
```
**CAUTION:** Dynamic subscribers and logical interfaces use physical interfaces for connection to the network. The Junos OS allows you to set the interface to disable and commit the change while dynamic subscribers and logical interfaces are still active. This action results in the loss of all subscriber connections on the interface. Use care when disabling interfaces.

**NOTE:** On the router, when you use the `disable` statement at the `edit interfaces` hierarchy level, depending on the PIC type, the interface might or might not turn off the laser. Older PIC transceivers do not support turning off the laser, but newer Gigabit Ethernet PICs with SFP and XFP transceivers do support it and the laser will be turned off when the interface is disabled.

**WARNING:** Do not stare into the laser beam or view it directly with optical instruments even if the interface has been disabled.

**Example: Disabling a Physical Interface**

Sample interface configuration:

```plaintext
[edit interfaces]
user@host# show
ge-0/3/2 {
  unit 0 {
    description CE2-to-PE1;
    family inet {
      address 20.1.1.6/24;
    }
  }
}
```

Disabling the interface:

```plaintext
[edit interfaces]
user@host# set ge-0/3/2 disable
```

Verifying the interface configuration:

```plaintext
[edit interfaces]
user@host# show
ge-0/3/2 {
  disable; # Interface is marked as disabled.
  unit 0 {
    description CE2-to-PE1;
    family inet {
      address 20.1.1.6/24;
    }
  }
}
```
Disabling a Logical Interface

You can unconfigure a logical interface, effectively disabling that interface, without removing the logical interface configuration statements from the configuration. To do this, include the `disable` statement:

```
disable;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

When an interface is disabled, a route (pointing to the reserved target "REJECT") with the IP address of the interface and a 32-bit subnet mask is installed in the routing table. See Routing Protocols.

Configuring Flow Control

By default, the router or switch imposes flow control to regulate the amount of traffic sent out on a Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interface. Flow control is not supported on the 4-port Fast Ethernet PIC. This is useful if the remote side of the connection is a Fast Ethernet or Gigabit Ethernet switch.

You can disable flow control if you want the router or switch to permit unrestricted traffic. To disable flow control, include the `no-flow-control` statement:

```
no-flow-control;
```

To explicitly reinstate flow control, include the `flow-control` statement:

```
flow-control;
```

You can include these statements at the following hierarchy levels:

- `[edit interfaces interface-name aggregated-ether-options]`
- `[edit interfaces interface-name ether-options]`
- `[edit interfaces interface-name fastether-options]`
- `[edit interfaces interface-name gigether-options]`

**NOTE:** On the Type 5 FPC, to prioritize control packets in case of ingress oversubscription, you must ensure that the neighboring peers support MAC flow control. If the peers do not support MAC flow control, then you must disable flow control.

Related Documentation

- flow-control on page 2426
- Ethernet Interfaces Overview
You assign an address to an interface by specifying the address when configuring the protocol family. For the inet or inet6 family, configure the interface IP address. For the iso family, configure one or more addresses for the loopback interface. For the ccc, ethernet-switching, tcc, mpls, tnp, and vpls families, you never configure an address.

NOTE: The point-to-point (PPP) address is taken from the loopback interface address that has the primary attribute. When the loopback interface is configured as an unnumbered interface, it takes the primary address from the donor interface.

To assign an address to an interface, include the address statement:

```
address address {
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    preferred;
    primary;
}
```

You can include these statements at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family family]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]

In the address statement, specify the network address of the interface.

For each address, you can optionally configure one or more of the following:

- Broadcast address for the interface subnet—Specify this in the broadcast statement; this applies only to Ethernet interfaces, such as the management interface fxp0, em0, or me0 the Fast Ethernet interface, and the Gigabit Ethernet interface.
- Address of the remote side of the connection (for point-to-point interfaces only)—Specify this in the destination statement.
- PPP properties to the remote end—Specify this in the destination-profile statement. You define the profile at the [edit access group-profile name ppp] hierarchy level (for point-to-point interfaces only).
- Whether the router or switch automatically generates the host number portion of interface addresses—The eui-64 statement applies only to interfaces that carry IPv6 traffic, in which the prefix length of the address is 64 bits or less, and the low-order 64
bits of the address are zero. This option does not apply to the loopback interface (lo0) because IPv6 addresses configured on the loopback interface must have a 128-bit prefix length.

• Whether this address is the preferred address—Each subnet on an interface has a preferred local address. If you configure more than one address on the same subnet, the preferred local address is chosen by default as the source address when you originate packets to destinations on the subnet.

By default, the preferred address is the lowest-numbered address on the subnet. To override the default and explicitly configure the preferred address, include the preferred statement when configuring the address.

• Whether this address is the primary address—Each interface has a primary local address. If an interface has more than one address, the primary local address is used by default as the source address when you send packets from an interface where the destination provides no information about the subnet (for example, some ping commands).

By default, the primary address on an interface is the lowest-numbered non-127 (in other words, non-loopback) preferred address on the interface. To override the default and explicitly configure the preferred address, include the primary statement when configuring the address.

• Configuring Interface IPv4 Addresses on page 2303
  • Configuring Interface IPv6 Addresses on page 2305

**Configuring Interface IPv4 Addresses**

You can configure router or switch interfaces with a 32-bit IP version 4 (IPv4) address and optionally with a destination prefix, sometimes called a subnet mask. An IPv4 address utilizes a 4-octet dotted decimal address syntax (for example, 192.16.1.1). An IPv4 address with destination prefix utilizes a 4-octet dotted decimal address syntax with a destination prefix appended (for example, 192.16.1.1/30).

To configure an IPv4 address on routers and switches running Junos OS, use the edit interface interface-name unit number family inet address a.b.c.d/nn statement at the [edit interfaces] hierarchy level.

**NOTE:** Juniper Networks routers and switches support /31 destination prefixes when used in point-to-point Ethernet configurations; however, they are not supported by many other devices, such as hosts, hubs, routers, or switches. You must determine if the peer system also supports /31 destination prefixes before configuration.

**Operational Behavior of Interfaces when the Same IPv4 Address is Assigned to Them**

You can configure the same IPv4 address on multiple physical interfaces. When you assign the same IPv4 address to multiple physical interfaces, the operational behavior of those interfaces differs, depending on whether they are implicitly or explicitly point-to-point.
NOTE: By default, all interfaces are assumed to be point-to-point (PPP) interfaces. For all interfaces except aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet, you can explicitly configure an interface to be a point-to-point connection.

The following examples show the sample configuration of assigning the same IPv4 address to implicitly and explicitly point-to-point interfaces, and their corresponding `show interfaces terse` command outputs to see their operational status.

**Configuring same IPv4 address on implicitly PPP interfaces:**

```plaintext
[edit]
user@host# show
ge-0/1/0 {
    unit 0 {
        family inet {
            address 200.1.1.1/24;
        }
    }
}
ge-3/0/1 {
    unit 0 {
        family inet {
            address 200.1.1.1/24;
        }
    }
}
```

The sample output shown below for the above configuration reveals that only `ge-0/1/0.0` was assigned the same IPv4 address `200.1.1.1/24` and its link state was up, while `ge-3/0/1.0` was not assigned the IPv4 address, though its link state was up, which means that it will be operational only when it gets a unique IPv4 address other than `200.1.1.1/24`.

```plaintext
user@host> show interfaces terse ge*
Interface         Admin Link  Proto Local       Remote
ge-0/1/0          up       up    inet      200.1.1.1/24
ge-0/1/0.0        up       up    inet      200.1.1.1/24 multiservice
ge-0/1/1          up       down
ge-3/0/0          up       down
ge-3/0/1          up       up
ge-3/0/1.0        up       up    inet      200.1.1.1/24 multiservice
```

**Configuring same IPv4 address on explicitly PPP interfaces:**

```plaintext
[edit]
user@host# show
so-0/0/0 {
    unit 0 {
        family inet {
            address 200.1.1.1/24;
        }
    }
}
```

```plaintext
Copyright © 2013, Juniper Networks, Inc.
```
The sample output shown below for the above configuration reveals that both
so-0/0/0.0 and so-0/0/3.0 were assigned the same IPv4 address 200.1.1.1/24
and that their link states were down, which means that to make them operational at least
one of them will have be configured with a unique IPv4 address other than 200.1.1.1/24.

user@host> show interfaces terse so*

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>up</td>
<td>down</td>
<td>inet</td>
<td>200.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>so-0/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/2</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-0/0/3.0</td>
<td>up</td>
<td>down</td>
<td>inet</td>
<td>200.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>so-1/1/0</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-1/1/1</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-1/1/2</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-1/1/3</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/0/1</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/0/2</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>so-2/0/3</td>
<td>up</td>
<td>down</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configuring Interface IPv6 Addresses

NOTE: IPv6 is not currently supported for the QFX Series.

You represent IP version 6 (IPv6) addresses in hexadecimal notation using a colon-separated list of 16-bit values.

You assign a 128-bit IPv6 address to an interface by including the address statement:

address aaaa:bbbb:....:zzzz/nn;

NOTE: You cannot configure a subnet zero IPv6 address because RFC 2461 reserves the subnet-zero address for anycast addresses, and Junos OS complies with the RFC.

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family inet6]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6]
The double colon (::) represents all bits set to 0, as shown in the following example:

```plaintext
interfaces fe-0/0/1 {
  unit 0 {
    family inet6 {
      address fec0:1:1:1::2/64;
    }
  }
}
```

**NOTE:** You must manually configure the router or switch advertisement and advertise the default prefix for autoconfiguration to work on a specific interface.

### Configuring the Interface Bandwidth

By default, the Junos OS uses the physical interface’s speed for the MIB-II object, `ifSpeed`. You can configure the logical unit to populate the `ifSpeed` variable by configuring a bandwidth value for the logical interface. The `bandwidth` statement sets an informational-only parameter; you cannot adjust the actual bandwidth of an interface with this statement.

**NOTE:** We recommend that you be careful when setting this value. Any interface bandwidth value that you configure using the `bandwidth` statement affects how the interface cost is calculated for a dynamic routing protocol, such as OSPF. By default, the interface cost for a dynamic routing protocol is calculated using the following formula:

\[
\text{cost} = \frac{\text{reference-bandwidth}}{\text{bandwidth}},
\]

where `bandwidth` is the physical interface speed. However, if you specify a value for bandwidth using the `bandwidth` statement, that value is used to calculate the interface cost, rather than the actual physical interface bandwidth.

To configure the bandwidth value for a logical interface, include the `bandwidth` statement:

```plaintext
bandwidth rate;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`
rate is the peak rate, in bps or cps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation c; values expressed in cells per second are converted to bits per second using the formula 1 cps = 384 bps. The value can be any positive integer. The bandwidth statement is valid for all logical interfaces, except multilink interfaces.

Configuring the Media MTU

The media maximum transmission unit (MTU) is the largest data unit that can be forwarded without fragmentation.

This topic contains the following sections:

- Media MTU Overview on page 2307
- How to Configure the Media MTU on page 2308
- Encapsulation Overhead by Encapsulation Type on page 2309
- Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers on page 2310
- Media MTU Sizes by Interface Type for M40e Routers on page 2311
- Media MTU Sizes by Interface Type for M160 Routers on page 2312
- Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers on page 2312
- Media MTU Sizes by Interface Type for MX Series Routers on page 2313
- Media MTU Sizes by Interface Type for T320 Routers on page 2314
- Media MTU Sizes by Interface Type for T640 Platforms on page 2314
- Media MTU Sizes by Interface Type for J2300 Platforms on page 2315
- Media MTU Sizes by Interface Type for J4300 and J6300 Platforms on page 2315
- Media MTU Sizes by Interface Type for J4350 and J6350 Platforms on page 2316
- Media MTU Sizes by Interface Type for EX Series Switches and ACX Series Routers on page 2318
- Media MTU Sizes by Interface Type for PTX Series Packet Transport Routers on page 2318

Media MTU Overview

The default media MTU size used on a physical interface depends on the encapsulation used on that interface. In some cases, the default IP Protocol MTU depends on whether the protocol used is IP version 4 (IPv4) or International Organization for Standardization (ISO).

The default media MTU is calculated as follows:

Default media MTU = Default IP MTU + encapsulation overhead

When you are configuring point-to-point connections, the MTU sizes on both sides of the connections must be the same. Also, when you are configuring point-to-multipoint
connections, all interfaces in the subnet must use the same MTU size. For details about encapsulation overhead, see “Encapsulation Overhead by Encapsulation Type” on page 2309.

**NOTE:** The actual frames transmitted also contain cyclic redundancy check (CRC) bits, which are not part of the media MTU. For example, the media MTU for a Gigabit Ethernet Version 2 interface is specified as 1514 bytes, but the largest possible frame size is actually 1518 bytes; you need to consider the extra bits in calculations of MTUs for interoperability.

The physical MTU for Ethernet interfaces does not include the 4-byte frame check sequence (FCS) field of the Ethernet frame.

A SONET/SDH interface operating in concatenated mode has a “c” added to the rate descriptor. For example, a concatenated OC48 interface is referred to as OC48c.

If you do not configure an MPLS MTU, the Junos OS derives the MPLS MTU from the physical interface MTU. From this value, the software subtracts the encapsulation-specific overhead and space for the maximum number of labels that might be pushed in the Packet Forwarding Engine. Currently, the software provides for three labels of four bytes each, for a total of 12 bytes.

In other words, the formula used to determine the MPLS MTU is the following:

\[
\text{MPLS MTU} = \text{physical interface MTU} - \text{encapsulation overhead} - 12
\]

If you configure an MTU value by including the `mtu` statement at the [edit interfaces interface-name unit logical-unit-number family mpls] hierarchy level, the configured value is used.

**How to Configure the Media MTU**

To modify the default media MTU size for a physical interface, include the `mtu` statement at the [edit interfaces interface-name] hierarchy level:

```plaintext
[edit interfaces interface-name]
mtu bytes;
```

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead.

**NOTE:** Changing the media MTU or protocol MTU causes an interface to be deleted and added again.

You configure the protocol MTU by including the `mtu` statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
Because tunnel services interfaces are considered logical interfaces, you cannot configure the MTU setting for the physical interface. This means you cannot include the `mtu` statement at the `[edit interfaces interface-name]` hierarchy level for the following interface types: generic routing encapsulation (gr-), IP-IP (ip-), loopback (lo-), link services (ls-), multilink services (ml-), and multicast (pe-, pd-). You can, however, configure the protocol MTU on tunnel interfaces, as described in “Setting the Protocol MTU” on page 2318.

### Encapsulation Overhead by Encapsulation Type

<table>
<thead>
<tr>
<th>Interface Encapsulation</th>
<th>Encapsulation Overhead (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 802.3</td>
<td>21</td>
</tr>
<tr>
<td>Ethernet Subnetwork Access Protocol (SNAP)</td>
<td>26</td>
</tr>
<tr>
<td>Ethernet version 2</td>
<td>18</td>
</tr>
<tr>
<td>ATM Cell Relay</td>
<td>4</td>
</tr>
<tr>
<td>ATM permanent virtual connection (PVC)</td>
<td>12</td>
</tr>
<tr>
<td>Cisco HDLC</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet 802.3 CCC and virtual private LAN service (VPLS)</td>
<td>4</td>
</tr>
<tr>
<td>Ethernet over ATM</td>
<td>32</td>
</tr>
<tr>
<td>Ethernet SNAP</td>
<td>22</td>
</tr>
<tr>
<td>Ethernet translational cross-connect (TCC)</td>
<td>18</td>
</tr>
<tr>
<td>Ethernet version 2</td>
<td>14</td>
</tr>
<tr>
<td>Extended virtual local area network (VLAN) CCC and VPLS</td>
<td>4</td>
</tr>
<tr>
<td>Extended VLAN TCC</td>
<td>22</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>4</td>
</tr>
<tr>
<td>PPP</td>
<td>4</td>
</tr>
<tr>
<td>VLAN CCC</td>
<td>4</td>
</tr>
</tbody>
</table>
### Table 289: Encapsulation Overhead by Encapsulation Type (continued)

<table>
<thead>
<tr>
<th>Interface Encapsulation</th>
<th>Encapsulation Overhead (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN VPLS</td>
<td>4</td>
</tr>
<tr>
<td>VLAN TCC</td>
<td>22</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers

### Table 290: Media MTU Sizes by Interface Type for M5 and M7i Routers with CFEB, M10 and M10i Routers with CFEB, and M20 and M40 Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Services</td>
<td>9192</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(MTU size not configurable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533 (4-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (8-port)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (12-port)</td>
<td></td>
</tr>
<tr>
<td>NOTE: The maximum MTU for two 100Base-TX Fast Ethernet port FIC is 9192 bytes.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>
### Media MTU Sizes by Interface Type for M40e Routers

#### Table 291: Media MTU Sizes by Interface Type for M40e Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Services</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(MTU size not</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>configurable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (4-port)</td>
<td></td>
</tr>
<tr>
<td>E3/DS3 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192 (1- or 2-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (4-port)</td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>4500 (1-port</td>
<td>4470</td>
</tr>
<tr>
<td></td>
<td></td>
<td>nonconcatenated)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (4-port OC3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (4-port OC3c)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (1-port OC12)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (4-port OC12)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (4-port OC12c)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (1-port OC4B)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (2-port OC3)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (2-port OC3c)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1-port OC12c)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1-port OC4Bc)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (1-port OC192)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1-port OC192c)</td>
<td></td>
</tr>
</tbody>
</table>
### Media MTU Sizes by Interface Type for M160 Routers

**Table 292: Media MTU Sizes by Interface Type for M160 Routers**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive Services</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>(MTU size not configurable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATM</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>E1/T1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>E3/T3</td>
<td>4474</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>E3/DS3 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192 (1- or 2-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (4-port)</td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>4500 (1-port nonconcatenated)</td>
<td>4470</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9192 (1- or 2-port)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4500 (4-port)</td>
<td></td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers

**Table 293: Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers**

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM2 IQ</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized DS3 IQ</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized E1 IQ</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>Channelized OC12 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>
Table 293: Media MTU Sizes by Interface Type for M7i Routers with CFEB-E, M10i Routers with CFEB-E, and M320 and M120 Routers (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channelized STM1 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>DS3</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>E1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>E3 IQ</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533 (4-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (8-, 12- and 48-port)</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>T1</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>CT3 IQ (excluding M120)</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

Table 294: Media MTU Sizes by Interface Type for MX Series Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>Multi-Rate Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>Tri-Rate Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
</tbody>
</table>
### Table 294: Media MTU Sizes by Interface Type for MX Series Routers (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channelized SONET/SDH OC3/STM1 (Multi-Rate)</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>DS3/E3 (Multi-Rate)</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for T320 Routers

### Table 295: Media MTU Sizes by Interface Type for T320 Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM</td>
<td>4470</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>ATM2 IQ</td>
<td>4470</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized OC12 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>Channelized STM1 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>DS3</td>
<td>4471</td>
<td>4500</td>
<td>4470</td>
</tr>
<tr>
<td>Fast Ethernet</td>
<td>1514</td>
<td>1533 (4-port)</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1532 (12- and 48-port)</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>CT3 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for T640 Platforms

### Table 296: Media MTU Sizes by Interface Type for T640 Platforms

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM2 IQ</td>
<td>4482</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>48-port Fast Ethernet</td>
<td>1514</td>
<td>1532</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
</tbody>
</table>
Table 296: Media MTU Sizes by Interface Type for T640 Platforms (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SONET/SDH</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>CT3 IQ</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

Media MTU Sizes by Interface Type for J2300 Platforms

Table 297: Media MTU Sizes by Interface Type for J2300 Platforms

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Ethernet (10/100)</td>
<td>1514</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>G.SHDSL</td>
<td>4482</td>
<td>9150</td>
<td>4470</td>
</tr>
<tr>
<td>ISDN BRI</td>
<td>1504</td>
<td>4092</td>
<td>1500</td>
</tr>
<tr>
<td>Serial</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>T1 or E1</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
</tbody>
</table>

Media MTU Sizes by Interface Type for J4300 and J6300 Platforms

Table 298: Media MTU Sizes by Interface Type for J4300 and J6300 Platforms

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL2+ PIM</td>
<td>4482</td>
<td>9150</td>
<td>4470</td>
</tr>
<tr>
<td>Dual-port Fast Ethernet (10/100) PIM</td>
<td>1514</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-port Serial PIM</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-port T1 or E1 PIM</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-port Channelized T1/E1 PIM (channelized to DS0s)</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
</tbody>
</table>
Table 298: Media MTU Sizes by Interface Type for J4300 and J6300 Platforms (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual-port Channelized T1/E1 PIM (clear channel T1 or E1)</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>Fast Ethernet (10/100) built-in interface</td>
<td>1514</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>G.SHDSL PIM</td>
<td>4482</td>
<td>9150</td>
<td>4470</td>
</tr>
<tr>
<td>4-port ISDN BRI PIM</td>
<td>1504</td>
<td>4092</td>
<td>1500</td>
</tr>
<tr>
<td>T3 (DS3) or E3 PIM</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

Media MTU Sizes by Interface Type for J4350 and J6350 Platforms

Table 299: Media MTU Sizes by Interface Type for J4350 and J6350 Platforms

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-port ISDN BRI PIM</td>
<td>1504</td>
<td>4092</td>
<td>1500</td>
</tr>
<tr>
<td>ADSL2+ PIM</td>
<td>4482</td>
<td>9150</td>
<td>4470</td>
</tr>
<tr>
<td>Dual-port Fast Ethernet (10/100) PIM</td>
<td>1514</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-port Serial PIM</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-port T1 or E1 PIM</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-port Channelized T1/E1 PIM (channelized to DS0s)</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-port Channelized T1/E1 PIM (clear channel T1 or E1)</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>4-port Fast Ethernet (10/100) ePIM</td>
<td>1518</td>
<td>1518</td>
<td>1500</td>
</tr>
</tbody>
</table>
Table 299: Media MTU Sizes by Interface Type for J4350 and J6350 Platforms (continued)

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet (10/100/1000) built-in interface</td>
<td>1514</td>
<td>9018</td>
<td>1500</td>
</tr>
<tr>
<td>Gigabit Ethernet (10/100/1000) Enhanced Physical Interface Module (ePIM)</td>
<td>1514</td>
<td>9018</td>
<td>1500</td>
</tr>
<tr>
<td>Gigabit Ethernet (10/100/1000) SFP ePIM</td>
<td>1514</td>
<td>9018</td>
<td>1500</td>
</tr>
<tr>
<td>G.SHDSL PIM</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
</tbody>
</table>

**NOTE:** On Gigabit Ethernet ePIMs in J4350 and J6350 Services Routers, you can configure a maximum transmission unit (MTU) size of only 9018 bytes even though the CLI indicates that you can configure an MTU of up to 9192 bytes. If you configure an MTU greater than 9018 bytes, the router does not accept the configuration and generates a system log error message similar to the following:

```
/kernel: ge-0/0/0: Illegal media change. MTU invalid: 9192. Max MTU supported on this PIC: 9018
```

On 4-port Fast Ethernet ePIMs in J4350 and J6350 Services Routers, you can configure a maximum transmission unit (MTU) size of only 1518 bytes even though the CLI indicates that you can configure an MTU of up to 9192 bytes. If you configure an MTU greater than 1518 bytes, the router does not accept the configuration and generates a system log error message similar to the following:

```
/kernel: fe-3/0/1: Illegal media change. MTU invalid: 9192. Max MTU supported on this PIC: 1518
```
### Media MTU Sizes by Interface Type for EX Series Switches and ACX Series Routers

Table 300: Media MTU Sizes by Interface Type for EX Series Switches and ACX Series Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1514</td>
<td>9192</td>
<td>1500 (IPv4), 1497 (ISO)</td>
</tr>
</tbody>
</table>

### Media MTU Sizes by Interface Type for PTX Series Packet Transport Routers

Table 301: Media MTU Sizes by Interface Type for PTX Series Packet Transport Routers

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Default Media MTU (Bytes)</th>
<th>Maximum MTU (Bytes)</th>
<th>Default IP Protocol MTU (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-Gigabit Ethernet</td>
<td>1514</td>
<td>9500</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>40-Gigabit Ethernet</td>
<td>1514</td>
<td>9500</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
<tr>
<td>100-Gigabit Ethernet</td>
<td>1514</td>
<td>9500</td>
<td>1500 (IPv4), 1488 (MPLS), 1497 (ISO)</td>
</tr>
</tbody>
</table>

### Setting the Protocol MTU

When you initially configure an interface, the protocol maximum transmission unit (MTU) is calculated automatically. If you subsequently change the media MTU, the protocol MTU on existing address families automatically changes.

For a list of default protocol MTU values, see "Configuring the Media MTU" on page 2307.

To modify the MTU for a particular protocol family, include the `mtu` statement:

```
mtu bytes;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
If you increase the size of the protocol MTU, you must ensure that the size of the media MTU is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. For a list of encapsulation overhead values, see Table 289 on page 2309. If you reduce the media MTU size, but there are already one or more address families configured and active on the interface, you must also reduce the protocol MTU size. (You configure the media MTU by including the \texttt{mtu} statement at the \texttt{[edit interfaces interface-name]} hierarchy level, as discussed in “Configuring the Media MTU” on page 2307.)

\textbf{NOTE:} Changing the media MTU or protocol MTU causes an interface to be deleted and added again.

The maximum number of data-link connection identifiers (DLCIs) is determined by the MTU on the interface. If you have keepalives enabled, the maximum number of DLCIs is 1000, with the MTU set to 5012.

The actual frames transmitted also contain cyclic redundancy check (CRC) bits, which are not part of the MTU. For example, the default protocol MTU for a Gigabit Ethernet interface is 1500 bytes, but the largest possible frame size is actually 1504 bytes; you need to consider the extra bits in calculations of MTUs for interoperability.

\subsection*{Interface Ranges}

\textbf{NOTE:} This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Interface Ranges. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Junos OS allows you to group a range of identical interfaces into an \textit{interface range}. You first specify the group of identical interfaces in the interface range. Then you can apply a common configuration to the specified interface range, reducing the number of configuration statements required and saving time while producing a compact configuration.

- Configuring Interface Ranges on page 2320
- Expanding Interface Range Member and Member Range Statements on page 2322
- Configuration Inheritance for Member Interfaces on page 2323
- Member Interfaces Inheriting Configuration from Configuration Groups on page 2324
- Interfaces Inheriting Common Configuration on page 2326
- Configuring Inheritance Range Priorities on page 2326
- Configuration Expansion Where Interface Range Is Used on page 2326
Configuring Interface Ranges

To configure an interface range, include the `interface-range` statement at the [edit interfaces] hierarchy level.

The `interface-range` statement accepts only physical networking interface names in its definition.

Interfaces can be grouped either as a range of interfaces or using a number range under the `interface-range` statement definition.

Interfaces in an `interface-range` definition can be added as part of a member range or as individual members or multiple members using a number range.

To specify a member range, use the `member-range` statement at the [edit interfaces interface-range name] hierarchy level.

To specify interfaces in lexical order, use the `member-range start-range to end-range` statement.

A range for a member statement must contain the following:

- `*`—All, specifies sequential interfaces from 0 through 47.

  **CAUTION:** The wildcard `*` in a member statement does not take into account the interface numbers supported by a specific interface type. Irrespective of the interface type, `*` includes interface numbers ranging from 0 through 47 to the interface group. Therefore, use `*` in a member statement with caution.

- `num`—Number; specifies one specific interface by its number.

- `[low-high]`—Numbers between low to high; specifies a range of sequential interfaces.

- `[num1, num2, num3]`—Numbers `num1`, `num2`, and `num3` specify multiple specific interfaces.

**Example:** Specifying an Interface Range Member Range

```plaintext
member-range ge-0/0/0 to ge-4/0/40;
```

To specify one or multiple members, use the `member` statement at the [edit interfaces interface-range name] hierarchy level.

To specify the list of interface range members individually or for multiple interfaces using regex, use the `member list of interface names` statement.

**Example:** Specifying an Interface Range Member

```plaintext
member ge-0/0/0;
member ge-0/*/*/
member ge-0/[1-10]/0;
member ge-0/[1,2,3]/3;
```
Regex or wildcards are not supported for interface-type prefixes. For example, prefixes `ge`, `fe`, and `xe` must be mentioned explicitly.

An **interface-range** definition can contain both **member** and **member-range** statements within it. There is no maximum limit on the number of **member** or **member-range** statements within an interface-range. However, at least one **member** or **member-range** statement must exist within an **interface-range** definition.

**Example: Interface Range Common Configuration**

Configuration common to an interface range can be added as a part of the **interface-range** definition, as follows:

```
[edit]
interfaces {
    + interface-range foo {
        + member-range ge-1/0/0 to ge-4/0/40;
        + member ge-0/1/1;
        + member ge-5/[1-10]/*

        /* Common configuration is added as part of interface-range definition */
        mtu 256;
        hold-time up 10;
        ether-options {
            flow-control;
            speed {
                100m;
            }
            802.3ad primary;
        }
    }
}
```

An **interface-range** definition having just **member** or **member-range** statements and no common configurations statements is valid.

These defined interface ranges can be used in other configuration hierarchies, in places where an **interface** node exists.

**Example: Interface-Range foo Used Under the Protocols Hierarchy**

```
protocols {
    dot1x {
        authenticator {
            interface foo{
                retries 1;
            }
        }
    }
}
```

`foo` should be an **interface-range** defined at the [interfaces] hierarchy level. In the above example, the **interface** node can accept both individual interfaces and interface ranges.

**TIP:** To view an interface range in expanded configuration, use the (show | display inheritance) command. For more information, see the **CLI User Guide**.
The defined interface ranges can be used at places where the interface node is used in the following configuration hierarchies:

- forwarding-options analyzer name input egress interface
- forwarding-options analyzer name input ingress interface
- poe interface
- protocols dot1x authenticator interface
- protocols igmp interface
- protocols isis interface
- protocols layer2-control bpdu-block interface
- protocols link-management peer name lmp-control-channel
- protocols link-management te-link name interface
- protocols lldp interface
- protocols lldp-med interface
- protocols mstp interface
- protocols oam ethernet link-fault-management interface
- protocols ospf area area-id interface
- protocols pim interface
- protocols router-advertisement interface
- protocols router-discovery interface
- protocols rsvp interface
- protocols sflow interfaces
- protocols vstp vlan vlan-id interface
- switch-options redundant-trunk-group group-name interface
- switch-options voip interface

**Expanding Interface Range Member and Member Range Statements**

All member and member-range statements in an interface range definition are expanded to generate the final list of interface names for the specified interface range.

```
[edit]
interfaces {
    interface-range range-1 {
        member-range ge-0/0/0 to ge-4/0/20;
        member ge-10/1/1;
        member ge-5/0-5)*;
        /*Common configuration is added part of the interface-range definition*/
        mtu 256;
        hold-time up 10;
        ether-options {
```
flow-control;
speed {
  100m;
}
802.3ad primary;
}
}
}

For the **member-range** statement, all possible interfaces between **start-range** and **end-range** are considered in expanding the members. For example, the following **member-range** statement:

**member-range** ge-0/0/0 to ge-4/0/20

expands to:

```
[ge-0/0/0, ge-0/0/1 ... ge-0/0/max_ports
 ge-0/1/0  ge-0/1/1 ... ge-0/1/max_ports
 ge-0/2/0  ge-0/2/1 ... ge-0/2/max_ports
  ...
 ge-0/MAX_PICS/0 ... ge-0/max_pics/max_ports
 ge-1/0/0  ge-1/0/1 ... ge-1/0/max_ports
  ...
 ge-1/MAX_PICS/0 ... ge-1/max_pics/max_ports
  ...
 ge-4/0/0 ge-4/0/1 ... ge-4/0/max_ports]
```

The following **member** statement:

**ge-5/[0-5]/**

expands to:

```
ge-5/0/0 ... ge-5/0/max_ports
 ge-5/1/0 ... ge-5/0/max_ports
  ...
 ge-5/5/0 ... ge-5/5/max_ports
```

The following **member** statement:

**ge-5/1/[2,3,6,10]***

expands to:

```
ge-5/1/2
 ge-5/1/3
 ge-5/1/6
 ge-5/1/10
```

**Configuration Inheritance for Member Interfaces**

When Junos OS expands the **member** and **member-range** statements present in an **interface-range**, it creates **interface objects** if they are not explicitly defined in the configuration. The common configuration is copied to all its member interfaces in the **interface-range**.
Example: Configuration Priorities

Foreground interface configuration takes priority over configuration inherited by the interface through the interface-range.

```
interfaces {
  interface-range range-1 {
    member-range ge-1/0/0/ to ge-10/0/47;
    mtu 256;
  }
  ge-1/0/1 {
    mtu 1024;
  }
}
```

In the preceding example, interface `ge-1/0/1` will have an MTU value of 1024.

This can be verified with output of the `show interfaces | display inheritance` command, as follows:

```
user@host: # show interfaces | display inheritance
## 'ge-1/0/0' was expanded from interface-range 'range-1'
##
ge-1/0/0 {
  ##
  ## '256' was expanded from interface-range 'range-1'
  ##
  mtu 256;
}
ge-1/0/1 {
  mtu 1024;
}
##
## 'ge-1/0/2' was expanded from interface-range 'range-1'
##
ge-1/0/2 {
  ##
  ## '256' was expanded from interface-range 'range-1'
  ##
  mtu 256;
}
```

Member Interfaces Inheriting Configuration from Configuration Groups

Interface range member interfaces inherit the config-groups configuration like any other foreground configuration. `interface-range` is similar to any other foreground configuration statement. The only difference is that the `interface-range` goes through a member interfaces expansion before Junos OS reads this configuration.

```
groups {
```
global {
    interfaces {
        <*> {
            hold-time up 10;
        }
    }
} apply-groups [global];

interfaces {
    interface-range range-1 {
        member-range ge-1/0/0 to ge-10/0/47;
        mtu 256;
    }
}

The **hold-time** configuration is applied to all members of **interface-range range-1**.

This can be verified with **show interfaces | display inheritance** as follows:

```plaintext
user@host# show interfaces | display inheritance
ge-1/0/0 {
    ##
    ## '256' was expanded from interface-range 'range-1'
    ##
    mtu 256;
    ##
    ## 'hold-time' was inherited from group 'global'
    ## '10' was inherited from group 'global'
    ##
    hold-time up 10;
}

ge-1/0/1 {
    ##
    ## '256' was expanded from interface-range 'range-1'
    ##
    mtu 256;
    ##
    ## 'hold-time' was inherited from group 'global'
    ## '10' was inherited from group 'global'
    ##
    hold-time up 10;
}

ge-10/0/47 {
    ##
    ## '256' was expanded from interface-range 'range-1'
    ##
    mtu 256;
    ##
    ## 'hold-time' was inherited from group 'global'
    ## '10' was inherited from group 'global'
    ##
    hold-time up 10;
}
```
**Interfaces Inheriting Common Configuration**

If an interface is a member of several interface ranges, that interface will inherit the common configuration from all of those interface ranges.

```plaintext
[edit]
interfaces {
  interface-range range-1 {
    member-range ge-1/0/0 to ge-10/0/47;
    mtu 256;
  }
}
```

In this example, interfaces ge-10/0/0 through ge-10/0/47 will have both `hold-time` and `mtu`.

**Configuring Inheritance Range Priorities**

The interface ranges are defined in the order of inheritance priority, with the first interface range configuration data taking priority over subsequent interface ranges.

```plaintext
[edit]
interfaces {
  interface-range int-grp-one {
    member-range ge-0/0/0 to ge-4/0/40;
    member ge-1/1/1;
    /*Common config is added part of the interface-range definition*/
    mtu 256;
    hold-time up 10;
  }
}
```

Interface `ge-1/1/1` exists in both `interface-range int-grp-one` and `interface-range int-grp-two`. This interface inherits `mtu 256` from `interface-range int-grp-one` because it was defined first.

**Configuration Expansion Where Interface Range Is Used**

In this example, `interface-range range-1` is used under the `protocols` hierarchy:

```plaintext
[edit]
interfaces {
  interface-range range-1 {
    member ge-10/1/1;
  }
}
```
member ge-5/5/1;
mTU 256;
hold-time up 10;
ether-options {
  flow-control;
speed {
    100m;
  }
  802.3ad primary;
}
}
protocols {
  dot1x {
    authenticator {
      interface range-1 {
        retries 1;
      }
    }
  }
}

The interface node present under authenticator is expanded into member interfaces of the interface-range range-1 as follows:

protocols {
  dot1x {
    authenticator {
      interface ge-10/1/1 {
        retries 1;
      }
      interface ge-5/5/1 {
        retries 1;
      }
    }
  }
}

The interface range-1 statement is expanded into two interfaces, ge-10/1/1 and ge-5/5/1, and configuration retries 1 is copied under those two interfaces.

This configuration can be verified using the show protocols dot1x | display inheritance command.

Configuring Accounting for the Physical Interface

Juniper Networks routers and switches can collect various kinds of data about traffic passing through the router and switch. You can set up one or more accounting profiles that specify some common characteristics of this data, including the following:

- The fields used in the accounting records
- The number of files that the router or switch retains before discarding, and the number of bytes per file
- The polling period that the system uses to record the data
You configure the profiles and define a unique name for each profile using statements at the [edit accounting-options] hierarchy level. There are two types of accounting profiles: interface profiles and filter profiles. You configure interface profiles by including the interface-profile statement at the [edit accounting-options] hierarchy level. You configure filter profiles by including the filter-profile statement at the [edit accounting-options] hierarchy level. For more information, see the Network Management Administration Guide for Routing Devices.

You apply filter profiles by including the accounting-profile statement at the [edit firewall filter filter-name] and [edit firewall family family filter filter-name] hierarchy levels. For more information, see the Routing Policy Feature Guide for Routing Devices.

**Applying an Accounting Profile to the Physical Interface**

To enable accounting on an interface, include the accounting-profile statement at the [edit interfaces interface-name] hierarchy level:

```plaintext
[edit interfaces interface-name]
accounting-profile name;
```

You can also reference profiles by logical unit; for more information, see “Configuring Accounting for the Logical Interface” on page 2329.

**Example: Applying an Accounting Profile to the Physical Interface**

Configure an accounting profile for an interface and apply it to a physical interface:

```plaintext
[edit]
accounting-options {
  file_if_stats {
    size 4m files 10 transfer-interval 15;
    archive-sites {
      "ftp://login:password@host/path";
    }
  }
  interface-profile if_profile {
    interval 15;
    file_if_stats {
      fields {
        input-bytes;
        output-bytes;
        input-packets;
        output-packets;
        input-errors;
        output-errors;
      }
    }
  }
}
[edit interfaces ge-1/0/1]
accounting-profile if_profile;
```
Configuring Accounting for the Logical Interface

Juniper Networks routers or switches can collect various kinds of data about traffic passing through the router or switch. You can set up one or more accounting profiles that specify some common characteristics of this data, including the following:

- The fields used in the accounting records
- The number of files that the router or switch retains before discarding, and the number of bytes per file
- The period that the system uses to record the data

You configure the profiles and define a unique name for each profile using statements at the [edit accounting-options] hierarchy level. There are two types of accounting profiles: interface profiles and filter profiles. You configure interface profiles by including the interface-profile statement at the [edit accounting-options] hierarchy level. You configure filter profiles by including the filter-profile statement at the [edit accounting-options] hierarchy level. For more information, see the Network Management Administration Guide for Routing Devices.

You apply filter profiles by including the accounting-profile statement at the [edit firewall filter filter-name] and [edit firewall family family filter filter-name] hierarchy levels. For more information, see the Routing Policy Feature Guide for Routing Devices.

Applying an Accounting Profile to the Logical Interface

To enable accounting on a logical interface, include the accounting-profile statement:

```
accounting-profile name;
```

You can include this statement at the following hierarchy level:

- [edit interfaces interface-name unit logical-unit-number]

You can also reference profiles for the physical interface; for more information, see “Configuring Accounting for the Physical Interface” on page 2327.

**Example: Applying an Accounting Profile to the Logical Interface**

Configure an accounting profile for an interface and apply it to a logical interface:

```
[edit]
accounting-options {
    file if_stats {
        size 4m files 10 transfer-interval 15;
        archive-sites {
            "ftp://login:password@host/path";
        }
    }
    interface-profile if_profile {
        interval 15;
        file if_stats {
            fields {
                input-bytes;
```
output-bytes;
input-packets;
output-packets;
input-errors;
output-errors;
}
}
}
[edit interfaces ge-1/0/1 unit 1]
accounting-profile if_profile;

To reference profiles by physical interface, see “Applying an Accounting Profile to the Physical Interface” on page 2328. For information about configuring a firewall filter accounting profile, see the Routing Policy Feature Guide for Routing Devices.

Configuring Ethernet Loopback Capability

By default, local aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system. To place an interface in loopback mode, include the loopback statement:

```
loopback;
```

**NOTE:** If you configure a local loopback on a 1-port 10-Gigabit IQ2 and IQ2-E PIC using the loopback statement at the [edit interfaces interface-name gigether-options] hierarchy level, the transmit-path stops working, causing the remote end to detect a link down.

To return to the default—that is, to disable loopback mode—delete the loopback statement from the configuration:

```
[edit]
user@host# delete interfaces fe-fpc/pic/port fastether-options loopback
```

To explicitly disable loopback mode, include the no-loopback statement:

```
noloopback;
```

You can include the loopback and no-loopback statements at the following hierarchy levels:

- [edit interfaces interface-name aggregated-ether-options]
- [edit interfaces interface-name ether-options]
- [edit interfaces interface-name fastether-options]
- [edit interfaces interface-name gigether-options]

**Related Documentation**
- loopback on page 2439
- Ethernet Interfaces Overview
- EX Series Switches Interfaces Overview on page 2267
Configuring Gratuitous ARP

Gratuitous Address Resolution Protocol (ARP) requests provide duplicate IP address detection. A gratuitous ARP request is a broadcast request for a router’s own IP address. If a router or switch sends an ARP request for its own IP address and no ARP replies are received, the router- or switch-assigned IP address is not being used by other nodes. If a router or switch sends an ARP request for its own IP address and an ARP reply is received, the router- or switch-assigned IP address is already being used by another node.

By default, the router or switch responds to gratuitous ARP requests. On Ethernet interfaces, you can disable responses to gratuitous ARP requests. To disable responses to gratuitous ARP requests, include the `no-gratuitous-arp-request` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
no-gratuitous-arp-request;
```

To return to the default—that is, to respond to gratuitous ARP requests—delete the `no-gratuitous-arp-request` statement from the configuration:

```
[edit]
user@host# delete interfaces interface-name no-gratuitous-arp-request
```

Gratuitous ARP replies are reply packets sent to the broadcast MAC address with the target IP address set to be the same as the sender’s IP address. When the router or switch receives a gratuitous ARP reply, the router or switch can insert an entry for that reply in the ARP cache.

By default, updating the ARP cache on gratuitous ARP replies is disabled on the router or switch. On Ethernet interfaces, you can enable handling of gratuitous ARP replies on a specific interface by including the `gratuitous-arp-reply` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
gratuitous-arp-reply;
```

To restore the default behavior, include the `no-gratuitous-arp-reply` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
no-gratuitous-arp-reply;
```
Configuring Static ARP Table Entries

To configure static ARP table entries, include the `arp` statement:

```
arp ip-address (mac | multicast-mac) mac-address <publish>;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number family inet address address]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet address address]

The IP address that you specify must be part of the subnet defined in the enclosing `address` statement.

To associate a multicast MAC address with a unicast IP address, include the `multicast-mac` statement.

Specify the MAC address as six hexadecimal bytes in one of the following formats: `nnnn.nnnn.nnnn` or `nn:nn:nn:nn:nn:nn`, for example, `0011:2233:4455` or `00:11:22:33:44:55`.

For unicast MAC addresses only, if you include the `publish` option, the router or switch replies to proxy ARP requests.

---

**NOTE:** By default, an ARP policer is installed that is shared among all the Ethernet interfaces on which you have configured the family inet statement. By including the `arp` statement at the [edit interfaces interface-name unit logical-unit-number family inet policer] hierarchy level, you can apply a specific ARP-packet policer to an interface. This feature is not available on EX Series switches.

When you need to conserve IP addresses, you can configure an Ethernet interface to be unnumbered by including the unnumbered-address statement at the [edit interfaces interface-name unit logical-unit-number family inet] hierarchy level.

---

**NOTE:** The Junos OS supports the IPv6 static neighbor discovery cache entries, similar to the static ARP entries in IPv4.

---

### Example: Configuring Static ARP Table Entries

Configure two static ARP table entries on the router or switch's management interface:

```
[edit interfaces]
fxp0 {
    unit 0 {
        family inet {
            address 10.10.0.11/24 {
                arp 10.10.0.99 mac 0001.0002.0003;
            }
        }
    }
}
```
Disabling the Transmission of Redirect Messages on an Interface

By default, the interface sends protocol redirect messages. To disable the sending of these messages on an interface, include the `no-redirects` statement:

```
no-redirects;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number family family]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]`

To disable the sending of protocol redirect messages for the entire router or switch, include the `no-redirects` statement at the `[edit system]` hierarchy level.

Configuring Restricted and Unrestricted Proxy ARP

To configure restricted or unrestricted proxy ARP, include the `proxy-arp` statement:

```
proxy-arp (restricted |unrestricted);
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number ]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number ]`

To return to the default—that is, to disable restricted or unrestricted proxy ARP—delete the `proxy-arp` statement from the configuration:

```
[edit]
user@host# delete interfaces interface-name unit logical-unit-number proxy-arp
```

You can track the number of restricted or unrestricted proxy ARP requests processed by the router or switch by issuing the `show system statistics arp` operational mode command.
NOTE: When proxy ARP is enabled as default or unrestricted, the router or switch responds to any ARP request as long as the device has an active route to the target address of the ARP request. This gratuitous ARP behavior can result in an error when the receiving interface and target response interface are the same and the end device (for example, a client) performs a duplicate address check. To prevent this error, configure the router or switch interface with the no-gratuitous-arp-reply statement. See “Configuring Gratuitous ARP” on page 2331 for information about how to disable responses to gratuitous ARP requests.

Related Documentation
- proxy-arp on page 2168
- Restricted and Unrestricted Proxy ARP Overview
- Configuring Gratuitous ARP on page 2331
- Ethernet Interfaces

Enabling or Disabling SNMP Notifications on Logical Interfaces

By default, Simple Network Management Protocol (SNMP) notifications are sent when the state of an interface or a connection changes. To explicitly enable these notifications on the logical interface, include the traps statement; to disable these notifications on the logical interface, include the no-traps statement:

(traps | no-traps);

You can include these statements at the following hierarchy levels:

- [edit interfaces interface-name unit logical-unit-number]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

NOTE: Gigabit Ethernet interfaces on J Series routers do not support SNMP.
Configuring Aggregated Ethernet Links (CLI Procedure)

Use the link aggregation feature to aggregate one or more links to form a virtual link or link aggregation group (LAG). The MAC client can treat this virtual link as if it were a single link to increase bandwidth, provide graceful degradation as failure occurs, and increase availability.

**NOTE:** An interface with an already configured IP address cannot form part of the aggregation group.

To configure aggregated Ethernet interfaces, using the CLI:

1. Specify the number of aggregated Ethernet interfaces to be created:
   
   ```
   [edit chassis]
   user@switch# set aggregated-devices ethernet device-count number
   ```

2. Specify the minimum number of links for the aggregated Ethernet interface (ae), that is, the defined bundle, to be labeled up:
   
   **NOTE:** By default, only one link must be up for the bundle to be labeled up.

   ```
   [edit interfaces]
   user@switch# set ae0 aggregated-ether-options minimum-links number
   ```

3. Specify the link speed for the aggregated Ethernet bundle:
   
   ```
   [edit interfaces]
   user@switch# set ae0 aggregated-ether-options link-speed speed
   ```

4. Specify the members to be included within the aggregated Ethernet bundle:
   
   ```
   [edit interfaces]
   user@switch# set xe-fpc/pic/port ether-options 802.3ada ae0
   user@switch# set xe-fpc/pic/port ether-options 802.3ada ae0
   ```

5. Specify an interface family for the aggregated Ethernet bundle:
   
   ```
   [edit interfaces]
   user@switch# set ae0 unit 0 family inet address address
   ```

For information about adding LACP to a LAG, see “Configuring Aggregated Ethernet LACP (CLI Procedure)” on page 2339.

**Related Documentation**

- Configuring Aggregated Ethernet Interfaces (J-Web Procedure) on page 2336
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
Verifying the Status of a LAG Interface on page 2465
Understanding Aggregated Ethernet Interfaces and LACP on page 2272

Configuring Aggregated Ethernet Interfaces (J-Web Procedure)

Use the link aggregation feature to aggregate one or more Ethernet interfaces to form a virtual link or link aggregation group (LAG) on an EX Series switch. The MAC client can treat this virtual link as if it were a single link. Link aggregation increases bandwidth, provides graceful degradation as failure occurs, and increases availability. You can use the J-Web interface to configure aggregated Ethernet interfaces, or a LAG, on the switch.

NOTE: Interfaces that are already configured with MTU, duplex, flow control, or logical interfaces are listed but are not available for aggregation.

To configure an aggregated Ethernet interface (also referred to as a LAG):

1. Select Configure > Interfaces > Link Aggregation.
   The list of aggregated interfaces is displayed.

   NOTE: After you make changes to the configuration on this page, you must commit the changes immediately for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following:
   - **Add**—Creates an aggregated Ethernet interface, or LAG. Enter information as specified in Table 302 on page 2337.
   - **Edit**—Modifies a selected LAG.
     - **Aggregation**—Modifies settings for the selected LAG. Enter information as specified in Table 302 on page 2337.
     - **VLAN**—Specifies VLAN options for the selected LAG. Enter information as specified in Table 303 on page 2338.
     - **IP Option**—Specifies IP options for the selected LAG. Enter information as specified in Table 304 on page 2338.
   - **Delete**—Deletes the selected LAG.
   - **Disable Port or Enable Port**—Disables or enables the administrative status on the selected interface.
   - **Device Count**—Configures the number of aggregated logical devices available to the switch. Select the number and click OK.
### Table 302: Aggregated Ethernet Interface Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Interface</td>
<td>Specifies the name of the aggregated interface.</td>
<td>None. The name is supplied by the software.</td>
</tr>
<tr>
<td>LACP Mode</td>
<td>Specifies the mode in which LACP packets are exchanged between the interfaces. The modes are:</td>
<td>Select from the list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—Indicates that no mode is applicable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—Indicates that the interface initiates transmission of LACP packets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Passive</strong>—Indicates that the interface responds only to LACP packets.</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description for the LAG.</td>
<td>Enter a description.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interfaces in the LAG.</td>
<td>To add interfaces to the LAG, select the interfaces and click <strong>Add</strong>. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. Click <strong>OK</strong>. To remove an interface from the LAG, select the interface and click <strong>Remove</strong>. <strong>NOTE</strong>: Only interfaces that are configured with the same speed can be selected together for a LAG.</td>
</tr>
<tr>
<td>Enable Log</td>
<td>Specifies whether to enable generation of log entries for the LAG.</td>
<td>Select the check box to enable log generation, or clear the check box to disable log generation.</td>
</tr>
</tbody>
</table>
Table 303: VLAN Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Mode</td>
<td>Specifies the mode of operation</td>
<td>If you select <strong>Trunk</strong>, you can:</td>
</tr>
<tr>
<td></td>
<td>for the port: trunk or access.</td>
<td>1. Click <strong>Add</strong> to add a VLAN member.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the VLAN and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. (Optional) Associate a native VLAN ID with the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select <strong>Access</strong>, you can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select the VLAN member to be associated with the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. (Optional) Associate a VoIP VLAN with the interface. Only a VLAN with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a VLAN ID can be associated as a VoIP VLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

Table 304: IP Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address</td>
<td>Specifies an IPv4 address for the selected LAG.</td>
<td>1. Select the check box <strong>IPv4 address</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Type an IP address—for example, 10.10.10.10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the subnet mask or address prefix. For example, 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Specifies an IPv6 address for the selected LAG.</th>
<th>1. Select the check box <strong>IPv6 address</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Type an IP address—for example, 2001:ab8:85a3:c:8a2e:370:7334.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the subnet mask or address prefix.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

Related Documentation

- [Configuring Aggregated Ethernet Links (CLI Procedure)](page 2335)
  - Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
  - Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- [Verifying the Status of a LAG Interface](page 2465)
- [Configuring Aggregated Ethernet LACP (CLI Procedure)](page 2339)
Configuring Aggregated Ethernet LACP (CLI Procedure)

For aggregated Ethernet interfaces on EX Series switches, you can configure the Link Aggregation Control Protocol (LACP). LACP is one method of bundling several physical interfaces to form one logical interface. You can configure aggregated Ethernet interfaces with or without LACP enabled.

LACP was designed to achieve the following:

- Automatic addition and deletion of individual links to the bundle without user intervention
- Link monitoring to check whether both ends of the bundle are connected to the correct group

NOTE: You can also configure LACP link protection on aggregated Ethernet interfaces. For information, see “Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure)” on page 2340.

The Junos OS implementation of LACP provides link monitoring but not automatic addition and deletion of links.

Before you configure LACP, be sure you have:

- Configured the aggregated Ethernet bundles—also known as link aggregation groups (LAGs). See “Configuring Aggregated Ethernet Links (CLI Procedure)” on page 2335

When LACP is enabled, the local and remote sides of the aggregated Ethernet links exchange protocol data units (PDUs), which contain information about the state of the link. You can configure Ethernet links to actively transmit PDUs, or you can configure the links to passively transmit them (sending out LACP PDUs only when they receive them from another link). One side of the link must be configured as active for the link to be up.

NOTE: Do not add LACP to a LAG if the remote end of the LAG link is a security device, unless the security device supports LACP. Security devices often do not support LACP because they require a deterministic configuration.

To configure LACP:

1. Configure at least one side of the aggregated Ethernet link as active:

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options lACP active
   ```

2. Specify the interval at which the interfaces send LACP packets:

   ```
   [edit interfaces]
   user@switch# set aeX aggregated-ether-options lACP periodic interval
   ```
The LACP process exists in the system only if you configure the system in either active or passive LACP mode.

Related Documentation
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
- Configuring Aggregated Ethernet Interfaces (J-Web Procedure) on page 2336
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Verifying the Status of a LAG Interface on page 2465
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272

**Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure)**

You can configure LACP link protection and system priority at the global level on the switch or for a specific aggregated Ethernet interface. When using LACP link protection, you can configure only two member links for an aggregated Ethernet interface: one active and one standby. LACP link protection ensures that only one link—the link with the higher priority—is used for traffic. The other link is forced to stay in a waiting state.

By default LACP link protection reverts to a higher-priority (lower-numbered) link when the higher-priority link becomes operational or when a higher-priority link is added to the aggregated Ethernet bundle. However, you can suppress link calculation by adding the non-revertive statement to the link protection configuration. In nonrevertive mode, when a link is active in sending and receiving LACP packets, adding a higher-priority link to the bundle does not change the status of the currently active link. It remains active.

If LACP link configuration is specified to be nonrevertive at the global [edit chassis] hierarchy level, you can specify the revertive statement in the LACP link protection configuration at the aggregated Ethernet interface level to override the nonrevertive setting for the interface. In revertive mode, adding a higher-priority link to the aggregated Ethernet bundle results in LACP recalculating the priority and switching the status from the currently active link to the newly added, higher-priority link.

**NOTE:** When LACP link protection is enabled on both local and remote sides of the link, both sides must use the same mode (either revertive or nonrevertive).

Configuring LACP link configuration at the aggregated Ethernet level results in only the configured interfaces using the defined configuration. LACP interface configuration also enables you to override global (chassis) LACP settings.
Before you configure LACP link protection, be sure you have:

- Configured the aggregated Ethernet bundles—also known as link aggregation groups (LAGs). See "Configuring Aggregated Ethernet Links (CLI Procedure)" on page 2335.
- Configured LACP for the interface. See "Configuring Aggregated Ethernet LACP (CLI Procedure)" on page 2339.

You can configure LACP link protection for all aggregated Ethernet interfaces on the switch by enabling it at the global level on the switch or configure it for a specific aggregated Ethernet interface by enabling it on that interface.

- Configuring LACP Link Protection at the Global Level on page 2341
- Configuring LACP Link Protection at the Aggregated Interface Level on page 2341

**Configuring LACP Link Protection at the Global Level**

To configure LACP link protection for aggregated Ethernet interfaces at the global level:

1. Enable LACP link protection on the switch:
   ```
   [edit chassis aggregated-devices ethernet lacp]
   user@switch# set link-protection
   ```

2. (Optional) Configure the LACP link protection for the aggregated Ethernet interfaces to be in nonrevertive mode:
   ```
   [edit chassis aggregated-devices ethernet lacp link-protection]
   user@switch# set non-revertive
   ```

3. (Optional) To configure LACP system priority for the aggregated Ethernet interfaces:
   ```
   [edit chassis aggregated-devices ethernet lacp]
   user@switch# set system-priority
   ```

**Configuring LACP Link Protection at the Aggregated Interface Level**

To enable LACP link protection for a specific aggregated Ethernet interface:

1. Enable LACP link protection for the interface:
   ```
   [edit interfaces aeX aggregated-ether-options lacp]
   user@switch# set link-protection
   ```

2. (Optional) Configure the LACP link protection for the aggregated Ethernet interface to be in revertive or nonrevertive mode:

   - To specify revertive mode:
     ```
     [edit interfaces aeX aggregated-ether-options lacp link-protection]
     user@switch# set revertive
     ```
   - To specify nonrevertive mode:
     ```
     [edit interfaces aeX aggregated-ether-options lacp link-protection]
     user@switch# set non-revertive
     ```

3. (Optional) To configure LACP system priority for an aggregated Ethernet interface:
Related Documentation

- Understanding Aggregated Ethernet Interfaces and LACP on page 2272

Configuring Aggregated Ethernet Link Protection

You can configure link protection for aggregated Ethernet interfaces to provide QoS on the links during operation.

On aggregated Ethernet interfaces, you designate a primary and backup link to support link protection. Egress traffic passes only through the designated primary link. This includes transit traffic and locally generated traffic on the router or switch. When the primary link fails, traffic is routed through the backup link. Because some traffic loss is unavoidable, egress traffic is not automatically routed back to the primary link when the primary link is reestablished. Instead, you manually control when traffic should be diverted back to the primary link from the designated backup link.

NOTE: Link protection is not supported on MX80.

- Configuring Link Protection for Aggregated Ethernet Interfaces on page 2342
- Configuring Primary and Backup Links for Link Aggregated Ethernet Interfaces on page 2342
- Reverting Traffic to a Primary Link When Traffic is Passing Through a Backup Link on page 2343
- Disabling Link Protection for Aggregated Ethernet Interfaces on page 2343

Configuring Link Protection for Aggregated Ethernet Interfaces

Aggregated Ethernet interfaces support link protection to ensure QoS on the interface.

To configure link protection:

1. Specify that you want to configure the options for an aggregated Ethernet interface.
   
   `user@host# edit interfaces aex aggregated-ether-options`

2. Configure the link protection mode.
   
   `[edit interfaces aex aggregated-ether-options]
   user@host# set link-protection`

Configuring Primary and Backup Links for Link Aggregated Ethernet Interfaces

To configure link protection, you must specify a primary and a secondary, or backup, link.
To configure a primary link and a backup link:

1. Configure the primary logical interface.

```
[edit interfaces interface-name]
user@host# set (fastether-options | gigether-options) 802.3adae primary
```

2. Configure the backup logical interface.

```
[edit interfaces interface-name]
user@host# set (fastether-options | gigether-options) 802.3adae backup
```

**Reverting Traffic to a Primary Link When Traffic is Passing Through a Backup Link**

On aggregated Ethernet interfaces, you designate a primary and backup link to support link protection. Egress traffic passes only through the designated primary link. This includes transit traffic and locally generated traffic on the router or switch. When the primary link fails, traffic is routed through the backup link. Because some traffic loss is unavoidable, egress traffic is not automatically routed back to the primary link when the primary link is reestablished. Instead, you manually control when traffic should be diverted back to the primary link from the designated backup link.

To manually control when traffic should be diverted back to the primary link from the designated backup link, enter the following operational command:

```
user@host> request interface revert aex
```

**Disabling Link Protection for Aggregated Ethernet Interfaces**

To disable link protection, issue the `delete interface revert aex` configuration command.

```
user@host# delete interfaces aex aggregated-ether-options link-protection
```

**Configuring Aggregated Ethernet Link Speed**

On aggregated Ethernet interfaces, you can set the required link speed for all interfaces included in the bundle. Generally, all interfaces that make up a bundle must have the same speed. If you include in the aggregated Ethernet interface an individual link that has a speed different from the speed that you specify in the `link-speed` parameter, an error message is logged. However, starting with Junos OS Release 13.2, aggregated Ethernet supports the following mixed rates and mixed modes on T640, T1600, T4000, and TX Matrix Plus routers:

- Member links of different modes (WAN and LAN) for 10-Gigabit Ethernet links.
- Member links of different rates: 10-Gigabit Ethernet, 40-Gigabit Ethernet, 50-Gigabit Ethernet, 100-Gigabit Ethernet, and OC192 (10-Gigabit Ethernet WAN mode)
NOTE:

- Member links of 50-Gigabit Ethernet can only be configured using the 50-Gigabit Ethernet interfaces of 100-Gigabit Ethernet PIC with CFP (PD-ICE-CFP-FPC4).
- Starting with Junos OS Release 13.2, 100-Gigabit Ethernet member links can be configured using the two 50-Gigabit Ethernet interfaces of 100-Gigabit Ethernet PIC with CFP. This 100-Gigabit Ethernet member link can be included in an aggregated Ethernet link that includes member links of other interfaces as well. In releases before Junos OS Release 13.2, the 100-Gigabit Ethernet member link configured using the two 50-Gigabit Ethernet interfaces of 100-Gigabit Ethernet PIC with CFP cannot be included in an aggregated Ethernet link that includes member links of other interfaces.

To configure member links of mixed rates and mixed modes on T640, T1600, T4000, and TX Matrix Plus routers, you need to configure the `mixed` option for the `[edit interfaces aex aggregated-ether-options link-speed]` statement.

To set the required link speed:

1. Specify that you want to configure the aggregated Ethernet options.
   ```
   user@host# edit interfaces interface-name aggregated-ether-options
   ```
2. Configure the link speed.
   ```
   user@host# set link-speed speed
   ```
   
   The `speed` can be in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation `k` (1000), `m` (1,000,000), or `g` (1,000,000,000).

   Aggregated Ethernet interfaces on the M120 router can have one of the following speeds:
   - `100m`—Links are 100 Mbps.
   - `10g`—Links are 10 Gbps.
   - `1g`—Links are 1 Gbps.
   - `oc192`—Links are OC192 or STM64c.

   Aggregated Ethernet links on EX Series switches can be configured to operate at one of the following speeds:
   - `10m`—Links are 10 Mbps.
   - `100m`—Links are 100 Mbps.
   - `1g`—Links are 1 Gbps.
   - `10g`—Links are 10 Gbps.
   - `50g`—Links are 50 Gbps.
Aggregated Ethernet links on T Series routers can be configured to operate at one of the following speeds:

- **100g**—Links are 100 Gbps.
- **100m**—Links are 100 Mbps.
- **10g**—Links are 10 Gbps.
- **1g**—Links are 1 Gbps.
- **40g**—Links are 40 Gbps.
- **50g**—Links are 50 Gbps.
- **80g**—Links are 80 Gbps.
- **8g**—Links are 8 Gbps.
- **mixed**—Links are of various speeds.
- **oc192**—Links are OC192.

**Related Documentation**
- aggregated-ether-options
- Configuring Mixed Aggregated Ethernet Links
- Ethernet Interfaces

**Configuring Aggregated Ethernet Minimum Links**

On aggregated Ethernet interfaces, you can configure the minimum number of links that must be up for the bundle as a whole to be labeled up. By default, only one link must be up for the bundle to be labeled up.

To configure the minimum number of links:

1. Specify that you want to configure the aggregated Ethernet options.
   
   user@host# edit interfaces interface-name aggregated-ether-options

2. Configure the minimum number of links.
   
   [edit interfaces interface-name aggregated-ether-options]
   
   user@host# set minimum-links number

On MX120, MX320, MX Series, T Series, and TX Matrix routers with Ethernet interfaces, and EX 9200 switches, the valid range for **minimum-links number** is 1 through 16. When the maximum value (16) is specified, all configured links of a bundle must be up for the bundle to be labeled up.

On all other routers and on EX Series switches, other than EX8200 switches, the range of valid values for **minimum-links number** is 1 through 8. When the maximum value (8) is specified, all configured links of a bundle must be up for the bundle to be labeled up.

On EX8200 switches, the range of valid values for **minimum-links number** is 1 through 12. When the maximum value (12) is specified, all configured links of a bundle must be up for the bundle to be labeled up.
If the number of links configured in an aggregated Ethernet interface is less than the minimum link value configured under the `aggregated-ether-options` statement, the configuration commit fails and an error message is displayed.

**Related Documentation**
- `aggregated-ether-options`
- `minimum-links`
- `Ethernet Interfaces`

### Configuring Tagged Aggregated Ethernet Interfaces

To specify aggregated Ethernet interfaces, include the `vlan-tagging` statement at the `[edit interfaces ae X]` hierarchy level:

```
[edit interfaces ae X]
vlan-tagging;
```

You must also include the `vlan-id` statement:

```
vlan-id number;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

For more information about the `vlan-tagging` and `vlan-id` statements, see “802.1Q VLANs Overview” on page 2283.

**Related Documentation**
- `vlan-id`
- `vlan-tagging on page 2461`

### Configuring a Layer 3 Subinterface (CLI Procedure)

EX Series switches use Layer 3 subinterfaces to divide a physical interface into multiple logical interfaces, each corresponding to a VLAN. The switch uses the Layer 3 subinterfaces to route traffic between subnets.

To configure Layer 3 subinterfaces, you enable VLAN tagging and partition one or more physical ports into multiple logical interfaces, each corresponding to a VLAN ID.

Before you begin, make sure you set up your VLANs. See *Configuring VLANs for EX Series Switches (CLI Procedure)* or “Configuring VLANs for EX Series Switches (J-Web Procedure)” on page 2117.

To configure Layer 3 subinterfaces:

1. Enable VLAN tagging:
   ```
   [edit interfaces interface-name]
   user@switch# set vlan-tagging
   ```
2. Bind each VLAN ID to a logical interface:

```
[edit interfaces interface-name]
user@switch# set unit logical-unit-number vlan-id (Layer 3 Subinterfaces) vlan-id-number
```

Related Documentation

- Example: Configuring Layer 3 Subinterfaces for a Distribution Switch and an Access Switch
- Verifying That Layer 3 Subinterfaces Are Working on page 2466
- Understanding Layer 3 Subinterfaces on page 2275

Configuring Unicast RPF (CLI Procedure)

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Enabling unicast RPF on the switch interfaces filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. When a packet comes into an interface, if that interface is not the best return path to the source, the switch discards the packet. If the incoming interface is the best return path to the source, the switch forwards the packet.

---

NOTE: On EX3200, EX4200, and EX4300 switches, you can enable unicast RPF only globally—that is, on all switch interfaces. You cannot enable unicast RPF on a per-interface basis.

---

Before you begin:

- On an EX8200 and EX6200 switches, ensure that the selected switch interface is symmetrically routed before you enable unicast RPF. A symmetrically routed interface is an interface that uses the same route in both directions between the source and the destination. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.

- On an EX3200, EX4200, or EX4300 switch, ensure that all switch interfaces are symmetrically routed before you enable unicast RPF on an interface. When you enable unicast RPF on any interface, it is enabled globally on all switch interfaces. Do not enable unicast RPF on asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination.
To enable unicast RPF, configure it explicitly on a selected customer-edge interface:

```
[edit interfaces]
user@switch# set ge-1/0/10 unit 0 family inet rpf-check
```

**BEST PRACTICE:** On EX3200, EX4200, and EX4300 switches, unicast RPF is enabled globally on all switch interfaces, regardless of whether you configure it explicitly on only one interface or only on some interfaces.

On EX3200, EX4200, and EX4300 switches, we recommend that you enable unicast RPF explicitly on either all interfaces or only one interface. To avoid possible confusion, do not enable it on only some interfaces:

- Enabling unicast RPF explicitly on only one interface makes it easier if you choose to disable it in the future because you must explicitly disable unicast RPF on every interface on which you explicitly enabled it. If you explicitly enable unicast RPF on two interfaces and you disable it on only one interface, unicast RPF is still implicitly enabled globally on the switch. The drawback of this approach is that the switch displays the flag that indicates that unicast RPF is enabled only on interfaces on which unicast RPF is explicitly enabled, so even though unicast RPF is enabled on all interfaces, this status is not displayed.

- Enabling unicast RPF explicitly on all interfaces makes it easier to know whether unicast RPF is enabled on the switch because every interface shows the correct status. (Only interfaces on which you explicitly enable unicast RPF display the flag that indicates that unicast RPF is enabled.) The drawback of this approach is that if you want to disable unicast RPF, you must explicitly disable it on every interface. If unicast RPF is enabled on any interface, it is implicitly enabled on all interfaces.

**Related Documentation**

- *Example: Configuring Unicast RPF on an EX Series Switch*
- *Verifying Unicast RPF Status on page 2467*
- *Disabling Unicast RPF (CLI Procedure) on page 2348*
- *Troubleshooting Unicast RPF on page 2547*
- *Understanding Unicast RPF for EX Series Switches on page 2276*

**Disabling Unicast RPF (CLI Procedure)**

Unicast reverse-path forwarding (RPF) can help protect your LAN from denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on untrusted interfaces. Unicast RPF filters traffic with source addresses that do not use the incoming interface as the best return path back to the source. If the network configuration changes so that an interface that has unicast RPF enabled becomes a trusted interface or becomes asymmetrically routed (the interface that receives a packet is not the best return path to the packet's source), disable unicast RPF.
To disable unicast RPF on an EX3200, EX4200, or EX4300 switch, you must delete it from every interface on which you explicitly configured it. If you do not disable unicast RPF on every interface on which you explicitly enabled it, it remains implicitly enabled on all interfaces. If you attempt to delete unicast RPF from an interface on which it was not explicitly enabled, the warning: statement not found message appears. If you do not disable unicast RPF on every interface on which you explicitly enabled it, unicast RPF remains implicitly enabled on all interfaces of the EX3200, EX4200, or EX4300 switch.

On EX8200 and EX6200 switches, the switch does not apply unicast RPF to an interface unless you explicitly enable that interface for unicast RPF.

To disable unicast RPF, delete its configuration from the interface:

```
[edit interfaces]
user@switch# delete ge-1/0/10 unit 0 family inet rpf-check
```

---

**NOTE:** On EX3200, EX4200, and EX4300 switches, if you do not disable unicast RPF on every interface on which you explicitly enabled it, unicast RPF remains implicitly enabled on all interfaces.

---

**Related Documentation**

- Example: Configuring Unicast RPF on an EX Series Switch
- Verifying Unicast RPF Status on page 2467
- Configuring Unicast RPF (CLI Procedure) on page 2347
- Understanding Unicast RPF for EX Series Switches on page 2276

---

**Configuring IP Directed Broadcast (CLI Procedure)**

---

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring IP Directed Broadcast (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

You can use IP directed broadcast on an EX Series switch to facilitate remote network management by sending broadcast packets to hosts on a specified subnet without broadcasting to the entire network. IP directed broadcast packets are broadcast on only the target subnet. The rest of the network treats IP directed broadcast packets as unicast packets and forwards them accordingly.

Before you begin to configure IP directed broadcast:

- Ensure that the subnet on which you want broadcast packets using IP direct broadcast is not directly connected to the Internet.
- Configure an integrated routing and bridging (IRB) interface or routed VLAN interface (RVI) for the subnet that will be enabled for IP direct broadcast. See “Configuring
Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122, Configuring Routed VLAN Interfaces (CLI Procedure), or Configuring VLANs for EX Series Switches (J-Web Procedure) on page 2117.

NOTE: We recommend that you do not enable IP directed broadcast on subnets that have a direct connection to the Internet because of increased exposure to denial-of-service (DoS) attacks.

To enable IP directed broadcast for a specified subnet:

1. Add the target subnet’s logical interfaces to the VLAN:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/0.0 family ethernet-switching vlan members v1
   user@switch# set ge-0/0/1.0 family ethernet-switching vlan members v1
   ```

2. Configure the Layer 3 interface on the VLAN that is the target of the IP directed broadcast packets:

   ```
   [edit interfaces]
   user@switch# set irb.1 family inet address 10.1.2.1/24
   ```

3. Associate a Layer 3 interface with the VLAN:

   ```
   [edit vlans]
   user@switch# set v1 l3-interface (VLANs) irb.1
   ```

4. Enable the Layer 3 interface for the VLAN to receive IP directed broadcasts:

   ```
   [edit interfaces]
   user@switch# set irb.1 family inet targeted-broadcast
   ```

Related Documentation

• Example: Configuring IP Directed Broadcast on an EX Series Switch

• Understanding IP Directed Broadcast for EX Series Switches on page 2280

Tracing Operations of an Individual Router or Switch Interface

To trace the operations of individual router or switch interfaces, include the `traceoptions` statement at the `[edit interfaces interface-name]` hierarchy level:

```
[edit interfaces interface-name]
traceoptions { flag flag; }
```

You can specify the following interface tracing flags:

- `all`—Trace all interface operations.
- `event`—Trace all interface events.
- `ipc`—Trace all interface interprocess communication (IPC) messages.
- `media`—Trace all interface media changes.

The interfaces `traceoptions` statement does not support a trace file. The logging is done by the kernel, so the tracing information is placed in the system `syslog` files.
Tracing Operations of the Interface Process

To trace the operations of the router or switch interface process, dcd, include the `traceoptions` statement at the `[edit interfaces]` hierarchy level:

```
[edit interfaces]
traceoptions {
    file <filename> <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
    flag flag <disable>;
    no-remote-trace;
}
```

By default, interface process operations are placed in the file named dcd and three 1-MB files of tracing information are maintained.

You can specify the following flags in the `interfaces traceoptions` statement:

- `change-events`—Log changes that produce configuration events.
- `config-states`—Log the configuration state machine changes.
- `kernel`—Log configuration IPC messages to kernel.
- `kernel-detail`—Log details of configuration messages to kernel.

For general information about tracing, see the tracing and logging information in the `Junos OS Administration Library for Routing Devices`.

Configuration Statements

- [edit chassis] Configuration Statement Hierarchy on EX Series Switches on page 2352
- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2354
- [edit interfaces ae] Configuration Statement Hierarchy on EX Series Switches on page 2354
- [edit interfaces et] Configuration Statement Hierarchy on EX Series Switches on page 2360
- [edit interfaces ge] Configuration Statement Hierarchy on EX Series Switches on page 2365
- [edit interfaces interface-range] Configuration Statement Hierarchy on EX Series Switches on page 2371
- [edit interfaces irb] Configuration Statement Hierarchy on EX Series Switches on page 2379
This topic lists supported and unsupported configuration statements in the [edit chassis] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit chassis] Hierarchy Level on page 2352

**Supported Statements in the [edit chassis] Hierarchy Level**

The following hierarchy shows the [edit chassis] configuration statements supported on EX Series switches:

```
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
      lACP {
        link-protection non-revertive;
        system-priority system-priority-number
      }
    }
  }
  alarm {
    ethernet {
      link-down (ignore | red | yellow);
    }
    management-ethernet {
      link-down (ignore | red | yellow);
    }
    container-devices {
      device-count device-count-number;
    }
  }
}
```
disk-partition {
  /config {
    level (full | high) {
      free-space (free-space-threshold-value | mb | percent);
    }
  }
  /var {
    level (full | high) {
      free-space (free-space-threshold-value | mb | percent);
    }
  }
}

fpc slot-number{
  pic pic-number {
    no-multi-rate;
    q-pic-large-buffer (large-scale | small-scale);
  }
}

maximum-ecmp maximum-ecmp-routes;

lcd-menu {
  fpc slot-number {
    menu-item menu-name);
    disable;
    pseudowire-service {
      device-count device-count-number;
    }
    psu {
      redundancy {
        n-plus-n;
      }
      redundancy {
        graceful-switchover;
      }
      slow-pfe-alarm;
    }
}

Related Documentation
  - Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
  - Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
  - Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504
  - Configuring Power Supply Redundancy (CLI Procedure) on page 2223
  - Configuring the Power Priority of Line Cards (CLI Procedure)
  - Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)
[edit interfaces] Configuration Statement Hierarchy on EX Series Switches

Each of the following topics lists the statements at a subhierarchy of the [edit interfaces] hierarchy:

- [edit interfaces ae] Configuration Statement Hierarchy on EX Series Switches on page 2354
- [edit interfaces et] Configuration Statement Hierarchy on EX Series Switches on page 2360
- [edit interfaces ge] Configuration Statement Hierarchy on EX Series Switches on page 2365
- [edit interfaces interface-range] Configuration Statement Hierarchy on EX Series Switches on page 2371
- [edit interfaces irb] Configuration Statement Hierarchy on EX Series Switches on page 2379
- [edit interfaces lo] Configuration Statement Hierarchy on EX Series Switches on page 2383
- [edit interfaces me] Configuration Statement Hierarchy on EX Series Switches on page 2386
- [edit interfaces vme] Configuration Statement Hierarchy on EX Series Switches on page 2389
- [edit interfaces xe] Configuration Statement Hierarchy on EX Series Switches on page 2393

Related Documentation

- EX Series Switches Interfaces Overview on page 2267
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
  - Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring a Layer 3 Subinterface (CLI Procedure) on page 2346
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
  - Configuring the Virtual Management Ethernet Interface for Global Management of an EX Series Virtual Chassis (CLI Procedure)
- Junos OS Interfaces Fundamentals Configuration Guide
- Junos OS Ethernet Interfaces Configuration Guide

[edit interfaces ae] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces ae] hierarchy level on EX Series switches.

- Supported statements are those that you can use to configure some aspect of a software feature on the switch.
• **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

• [Supported Statements in the [edit interfaces ae] Hierarchy Level on page 2355](#)
• [Unsupported Statements in the [edit interfaces ae] Hierarchy Level on page 2358](#)

**Supported Statements in the [edit interfaces ae] Hierarchy Level**

The following hierarchy shows the [edit interfaces ae] configuration statements supported on EX Series switches.

```
interfaces {
  aeX {
    accounting-profile name;
    aggregated-ether-options {
      ethernet-switch-profile {
        tag-protocol-id identifiers;
      }
      (flow-control | no-flow-control);
      lacp {
        (active | passive);
        link-protection {
          disable;
          (revertive | non-revertive);
        }
        periodic interval;
        system-priority number;
      }
      (link-protection | no-link-protection);
      link-speed speed;
      (loopback | no-loopback);
      minimum-links number;
      rebalance-periodic;
    }
    description text;
    disable;
    encapsulation type;
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    mtu bytes;
    native-vlan-id
    no-gratuitous-arp-request;
    traceoptions {
      flag flag;
    }
    (traps | no-traps);
    unit logical-unit-number {
      accounting-profile name;
      arp-resp { restricted | unrestricted; }
      bandwidth rate;
    }
  }
  }
```

2355

Copyright © 2013, Juniper Networks, Inc.
description text;
disable;
encapsulation type;
family ccc {
  filter {
    group group-number;
    input filter-name;
    input-list [filter-names];
    output filter-name;
    output-list [filter-names];
  }
  policer {
    input policer-name;
    output policer-name;
  }
}
family ethernet-switching {
  filter {
    input filter-name;
    output filter-name;
  }
  interface-mode (access | trunk);
  recovery-timeout seconds;
  storm-control profile-name;
  vlan {
    members [members];
  }
}
family inet {
  accounting {
    destination-class-usage;
    source-class-usage {
      input;
      output;
    }
  }
  address ipv4-address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    preferred;
    primary;
    vrrp-group group-number {
      (accept-data | no-accept-data);
      advertise-interval seconds;
      advertisements-threshold number;
      authentication-key key;
      authentication-type authentication;
      fast-interval milliseconds;
      (preempt | no-preempt) {
        hold-time seconds;
      }
      priority number;
      track {
        interface interface-name {
          priority-cost number;
        }
        priority-hold-time seconds;
      }
route ip-address/mask routing-instance instance-name priority-cost cost;
}
virtual-address [addresses];
vrp-inherit-from {
    active-group group-number;
    active-interface interface-name;
}
}
}
filter {
    input filter-name;
    output filter-name;
}
mtu bytes;
no-neighbor-learn;
no-redirects;
primary;
rpf-check {
    fail-filter filter-name;
    mode {
        loose;
    }
}
}
family inet6 {
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
    address address [eui-64];
    ndp ip-address (mac | multicast-mac) mac-address <publish>;
    preferred;
    primary;
    vrrp-inet6-group group-id {
        accept-data | no-accept-data;
        advertisements-threshold number;
        authentication-key key;
        authentication-type authentication;
        fast-interval milliseconds;
        inet6-advertise-interval milliseconds;
        preempt | no-preempt {
            hold-time seconds;
        }
        priority number;
        track {
            interface interface-name {
                priority-cost number;
            }
            priority-hold-time seconds;
            route ip-address/mask routing-instance instance-name priority-cost cost;
        }
    virtual-inet6-address [addresses];
virtual-link-local-address ipv6-address;
vrrp-inherit-from {
  active-group group-name;
  active-interface interface-name;
}
(dad-disable | no-dad-disable);
filter {
  input filter-name;
  output filter-name;
}
mtu bytes;
nd6-stale-time time;
no-neighbor-learn;
no-redirects;
policer {
  input policer-name;
  output policer-name;
}
rpf-check {
  fail-filter filter-name;
  mode {
    loose;
  }
}
family iso {
  address interface-address;
  mtu bytes;
}
proxy-arp (restricted | unrestricted);
(traps | no-traps);
vlan-id (Layer 3 Subinterfaces) vlan-id-number;
vlan-tagging;
}

Unsupported Statements in the [edit interfaces ae] Hierarchy Level

All statements in the [edit interfaces ae] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 305: Unsupported [edit interfaces ae] Configuration Statements for EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>stacked-vlan-tagging</td>
<td>[edit interfaces ae]</td>
</tr>
<tr>
<td>admin-key</td>
<td>[edit interfaces ae aggregated-ether-options lacp]</td>
</tr>
<tr>
<td>system-id</td>
<td>[edit interfaces ae aggregated-ether-options lacp]</td>
</tr>
<tr>
<td>input-vlan-map</td>
<td>[edit interfaces ae unit]</td>
</tr>
</tbody>
</table>
Table 305: Unsupported [edit interfaces ae] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces ae unit]</td>
</tr>
<tr>
<td>native-inner-vlan-id</td>
<td>[edit interfaces ae unit]</td>
</tr>
<tr>
<td>output-vlan-map</td>
<td>[edit interfaces ae unit]</td>
</tr>
<tr>
<td>swap-by-poppush</td>
<td>[edit interfaces ae unit]</td>
</tr>
<tr>
<td>vlan-id-list</td>
<td>[edit interfaces ae unit]</td>
</tr>
<tr>
<td>vlan-id-range</td>
<td>[edit interfaces ae unit]</td>
</tr>
<tr>
<td>vlan-tags</td>
<td>[edit interfaces ae unit]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces ae unit family]</td>
</tr>
<tr>
<td>vpls</td>
<td>[edit interfaces ae unit family]</td>
</tr>
<tr>
<td>bridge-domain-type</td>
<td>[edit interfaces ae unit family ethernet-switching]</td>
</tr>
<tr>
<td>inner-vlan-id-list</td>
<td>[edit interfaces ae unit family ethernet-switching]</td>
</tr>
<tr>
<td>vlan-rewrite</td>
<td>[edit interfaces ae unit family ethernet-switching]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces ae unit family inet]</td>
</tr>
<tr>
<td>sampling</td>
<td>[edit interfaces ae unit family inet]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces ae unit family inet]</td>
</tr>
<tr>
<td>simple-filter</td>
<td>[edit interfaces ae unit family inet]</td>
</tr>
<tr>
<td>targeted-broadcast</td>
<td>[edit interfaces ae unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces ae unit family inet]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces ae unit family inet address vrrp-group track interface]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces ae unit family inet6]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces ae unit family inet6 address vrrp-group track interface]</td>
</tr>
<tr>
<td>group</td>
<td>[edit interfaces ae unit family inet6 filter]</td>
</tr>
</tbody>
</table>
[edit interfaces et] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces et] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit interfaces et] Hierarchy Level on page 2360
- Unsupported Statements in the [edit interfaces et] Hierarchy Level on page 2363

**Supported Statements in the [edit interfaces et] Hierarchy Level**

The following hierarchy shows the [edit interfaces et] configuration statements supported on EX Series switches.

```
interfaces {
  et-fpc/pic/port {
    accounting-profile name;
    description text;
    disable;
    encapsulation type;
    ether-options {
      802.3ad {
        aex;
        (backup | primary);
        lacp {
          force-up;
          port-priority number;
        }
      }
      (flow-control | no-flow-control);
      (loopback | no-loopback);
      no-auto-mdix;
    }
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    mtu bytes;
    native-vlan-id
    no-gratuitous-arp-request;
    traceoptions {
      flag flag;
    }
  }
```
(traps | no-traps);
unit logical-unit-number {
  accounting-profile name;
  bandwidth rate;
  description text;
  disable;
  encapsulation type;
  family ccc;
  filter {
    group group-number;
    input filter-name;
    input-list [filter-names];
    output filter-name;
    output-list [filter-names];
  }
  policer {
    input policer-name;
    output policer-name;
  }
} family ethernet-switching {
  filter {
    input filter-name;
    output filter-name;
  }
  interface-mode (access | trunk);
  recovery-timeout seconds;
  storm-control profile-name;
  vlan {
    members (vlan-name | [-vlan-names] | all);}
} family inet {
  accounting {
    destination-class-usage;
    source-class-usage {
      input;
      output;
    }
  }
  address ipv4-address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    preferred;
    primary;
    vrrp-group group-number {
      advertise-interval seconds;
      advertisements-threshold number;
      authentication-key key;
      authentication-type authentication;
      fast-interval milliseconds;
      (preempt | no-preempt) {
      hold-time seconds;
    }
    priority number;
track {
    interface interface-name {
        priority-cost number;
    }
    priority-hold-time seconds;
    route ip-address/mask routing-instance instance-name priority-cost cost;
}
virtual-address [addresses];
vrrp-inherit-from {
    active-group group-number;
    active-interface interface-name;
}
}
}
filter {
    input filter-name;
    output filter-name;
}
mtu bytes;
no-neighbor-learn;
no-redirects;
primary;
rpf-check {
    fail-filter filter-name;
    mode {
        loose;
    }
}
}
}
family inet6 {
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
    address address {
        eui-64;
        ndp ip-address (mac | multicast-mac) mac-address <publish>;
        preferred;
        primary;
        vrrp-inet6-group group-id {
            accept-data | no-accept-data;
            advertisements-threshold number;
            authentication-key key;
            authentication-type authentication;
            fast-interval milliseconds;
            inet6-advertise-interval milliseconds;
            preempt | no-preempt {
                hold-time seconds;
            }
            priority number;
            track {
                interface interface-name {
                    priority-cost number;
                }
            }
        }
    }
}
} priority-hold-time seconds;
route ip-address/mask routing-instance instance-name priority-cost cost;
}
virtual-inet6-address [addresses];
virtual-link-local-address ipv6-address;
vrp-inherit-from {
active-group group-name;
active-interface interface-name;
}
}
(dad-disable | no-dad-disable);
filter {
input filter-name;
output filter-name;
}
mtu bytes;
nd6-stale-time time;
no-neighbor-learn;
no-redirects;
policer {
input policer-name;
output policer-name;
}
rpf-check {
fail-filter filter-name;
mode {
loose;
}
}
}
family iso {
address interface-address;
mtu bytes;
}
proxy-arp (restricted | unrestricted);
swap-by-poppush;
(traps | no-traps);
vlan-id vlan-id-number;
}
vlan-tagging;
}
}

Unsupported Statements in the [edit interfaces et] Hierarchy Level

All statements in the [edit interfaces et] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:
<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive-monitor-mode</td>
<td>[edit interfaces et]</td>
</tr>
<tr>
<td>stacked-vlan-tagging</td>
<td>[edit interfaces et]</td>
</tr>
<tr>
<td>asynchronous-notification</td>
<td>[edit interfaces et ether-options]</td>
</tr>
<tr>
<td>ethernet-switch-profile</td>
<td>[edit interfaces et ether-options]</td>
</tr>
<tr>
<td>ignore-l3-incompletes</td>
<td>[edit interfaces et ether-options]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces et ether-options]</td>
</tr>
<tr>
<td>source-address-filter</td>
<td>[edit interfaces et ether-options]</td>
</tr>
<tr>
<td>source-filtering</td>
<td>[edit interfaces et ether-options]</td>
</tr>
<tr>
<td>no-source-filtering</td>
<td>[edit interfaces et ether-options]</td>
</tr>
<tr>
<td>accept-source-mac</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>input-vlan-map</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>native-inner-vlan-id</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>output-vlan-map</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>vlan-id-list</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>vlan-id-range</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>vlan-tags</td>
<td>[edit interfaces et unit]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces et unit family]</td>
</tr>
<tr>
<td>tcc</td>
<td>[edit interfaces et unit family]</td>
</tr>
<tr>
<td>vpls</td>
<td>[edit interfaces et unit family]</td>
</tr>
<tr>
<td>bridge-domain-type</td>
<td>[edit interfaces et unit family ethernet-switching]</td>
</tr>
<tr>
<td>inner-vlan-id-list</td>
<td>[edit interfaces et unit family ethernet-switching]</td>
</tr>
<tr>
<td>vlan-rewrite</td>
<td>[edit interfaces et unit family ethernet-switching]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces et unit family inet]</td>
</tr>
</tbody>
</table>
Table 306: Unsupported [edit interfaces et] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>sampling</td>
<td>[edit interfaces et unit family inet]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces et unit family inet]</td>
</tr>
<tr>
<td>targeted-broadcast</td>
<td>[edit interfaces et unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces et unit family inet]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces et unit family inet address vrrp-group track interface]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces et unit family inet6]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces et unit family inet6 address vrrp-group track interface]</td>
</tr>
<tr>
<td>group</td>
<td>[edit interfaces et unit family inet6 filter]</td>
</tr>
</tbody>
</table>

Related Documentation

• [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2133

[edit interfaces ge] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces ge] hierarchy level on EX Series switches.

• Supported statements are those that you can use to configure some aspect of a software feature on the switch.

• Unsupported statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

• Supported Statements in the [edit interfaces ge] Hierarchy Level on page 2365

• Unsupported Statements in the [edit interfaces ge] Hierarchy Level on page 2369

Supported Statements in the [edit interfaces ge] Hierarchy Level

The following hierarchy shows the [edit interfaces ge] configuration statements supported on EX Series switches.

```plaintext
interfaces {
    ge-fpc/pic/port {
        accounting-profile name;
        description text;
```
disable;
encapsulation type;
ether-options {
  802.3ad {
    aex;
    (backup | primary);
    lACP {
      force-up;
      port-priority number;
    }
  }
  (auto-negotiation | no-auto-negotiation);
  (flow-control | no-flow-control);
  ieee-802-3az-eee;
  (loopback | no-loopback);
  no-auto-mdix;
}
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds;
link-mode {
  full-duplex;
}
mtu bytes;
native-vlan-id
no-gratuitous-arp-request;
speed speed;
traceoptions {
  flag flag;
}
(traps | no-traps);
unit logical-unit-number {
  accounting-profile name;
  arp-resp (restricted | unrestricted);
  bandwidth rate;
  description text;
  disable;
  encapsulation type;
  family ccc;
  filter {
    group group-number;
    input filter-name;
    input-list [filter-names];
    output filter-name;
    output-list [filter-names];
  }
policer {
  input policer-name;
  output policer-name;
}
}
family ethernet-switching {
 filter {
  input filter-name;
  output filter-name;
}
interface-mode (access | trunk);
recovery-timeout seconds;
storm-control profile-name;
vlan {
    members (vlan-name [-vlan-names] | all);
}
}
family inet {
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
    address ipv4-address {
        arp ip-address (mac | multicast-mac) mac-address <publish>;
        broadcast address;
        preferred;
        primary;
        vrrp-group group-number {
            (accept-data | no-accept-data);
            advertise-interval seconds;
            advertisements-threshold number;
            authentication-key key;
            authentication-type authentication;
            fast-interval milliseconds;
            (preempt | no-preempt) {
                hold-time seconds;
            }
            priority number;
            track {
                interface interface-name {
                    priority-cost number;
                }
                priority-hold-time seconds;
                route ip-address/mask routing-instance instance-name priority-cost cost;
            }
            virtual-address [addresses];
        vrrp-inherit-from {
            active-group group-number;
            active-interface interface-name;
        }
    }
}
filter {
    input filter-name;
    output filter-name;
}
mtu bytes;
no-neighbor-learn;
no-redirects;
primary;
rpf-check {
    fail-filter filter-name;
    mode {
        loose;
family inet6
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
address address {
    eui-64;
    ndp ip-address (mac | multicast-mac) mac-address <publish>;
    preferred;
    primary;
    vrrp-inet6-group group-id {
        accept-data | no-accept-data;
        advertisements-threshold number;
        authentication-key key;
        advertisement-type authentication;
        fast-interval milliseconds;
        inet6-advertise-interval milliseconds;
        preempt | no-preempt {
            hold-time seconds;
        }
        priority number;
        track {
            interface interface-name {
                priority-cost number;
            }
            priority-hold-time seconds;
            route ip-address/mask routing-instance instance-name priority-cost cost;
        }
        virtual-inet6-address [addresses];
        virtual-link-local-address ipv6-address;
        vrrp-inherit-from {
            active-group group-name;
            active-interface interface-name;
        }
    }
    (dad-disable | no-dad-disable);
filter {
    input filter-name;
    output filter-name;
}
mtu bytes;
nd6-stale-time time;
no-neighbor-learn;
no-redirects;
policer {
    input policer-name;
    output policer-name;
}
rpf-check {
fail-filter filter-name;
mode {
    loose;
}
}
}
family iso {
    address interface-address;
    mtu bytes;
}
interface-shared-with {
    psd-name;
}
proxy-arp (restricted | unrestricted);
swap-by-poppush;
(traps | no-traps);
vlan-id vlan-id-number;
}
vlan-tagging;
}
}

Unsupported Statements in the [edit interfaces ge] Hierarchy Level

All statements in the [edit interfaces ge] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 307: Unsupported [edit interfaces ge] Configuration Statements for EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive-monitor-mode</td>
<td>[edit interfaces ge]</td>
</tr>
<tr>
<td>stacked-vlan-tagging</td>
<td>[edit interfaces ge]</td>
</tr>
<tr>
<td>asynchronous-notification</td>
<td>[edit interfaces ge ether-options]</td>
</tr>
<tr>
<td>ethernet-switch-profile</td>
<td>[edit interfaces ge ether-options]</td>
</tr>
<tr>
<td>ignore-l3-incompletes</td>
<td>[edit interfaces ge ether-options]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces ge ether-options]</td>
</tr>
<tr>
<td>source-address-filter</td>
<td>[edit interfaces ge ether-options]</td>
</tr>
<tr>
<td>source-filtering</td>
<td>[edit interfaces ge ether-options]</td>
</tr>
<tr>
<td>no-source-filtering</td>
<td>[edit interfaces ge ether-options]</td>
</tr>
<tr>
<td>accept-source-mac</td>
<td>[edit interfaces ge unit]</td>
</tr>
<tr>
<td>input-vlan-map</td>
<td>[edit interfaces ge unit]</td>
</tr>
</tbody>
</table>
### Table 307: Unsupported [edit interfaces ge] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces ge unit]</td>
</tr>
<tr>
<td>native-inner-vlan-id</td>
<td>[edit interfaces ge unit]</td>
</tr>
<tr>
<td>output-vlan-map</td>
<td>[edit interfaces ge unit]</td>
</tr>
<tr>
<td>vlan-id-list</td>
<td>[edit interfaces ge unit]</td>
</tr>
<tr>
<td>vlan-id-range</td>
<td>[edit interfaces ge unit]</td>
</tr>
<tr>
<td>vlan-tags</td>
<td>[edit interfaces ge unit]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces ge unit family]</td>
</tr>
<tr>
<td>tcc</td>
<td>[edit interfaces ge unit family]</td>
</tr>
<tr>
<td>vpls</td>
<td>[edit interfaces ge unit family]</td>
</tr>
<tr>
<td>bridge-domain-type</td>
<td>[edit interfaces ge unit family ethernet-switching]</td>
</tr>
<tr>
<td>inner-vlan-id-list</td>
<td>[edit interfaces ge unit family ethernet-switching]</td>
</tr>
<tr>
<td>vlan-rewrite</td>
<td>[edit interfaces ge unit family ethernet-switching]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces ge unit family inet]</td>
</tr>
<tr>
<td>sampling</td>
<td>[edit interfaces ge unit family inet]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces ge unit family inet]</td>
</tr>
<tr>
<td>simple-filter</td>
<td>[edit interfaces ge unit family inet]</td>
</tr>
<tr>
<td>targeted-broadcast</td>
<td>[edit interfaces ge unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces ge unit family inet]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces ge unit family inet address vrrp-group track interface]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces ge unit family inet6]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces ge unit family inet6 address vrrp-group track interface]</td>
</tr>
<tr>
<td>group</td>
<td>[edit interfaces ge unit family inet6 filter]</td>
</tr>
</tbody>
</table>
[edit interfaces interface-range] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces interface-range] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27

This topic lists:

- Supported Statements in the [edit interfaces interface-range] Hierarchy Level on page 2371
- Unsupported Statements in the [edit interfaces interface-range] Hierarchy Level on page 2374

**Supported Statements in the [edit interfaces interface-range] Hierarchy Level**

The following hierarchy shows the [edit interfaces interface-range] configuration statements supported on EX Series switches.

```
interfaces {
  interface-range name {
    accounting-profile name;
    aggregated-ether-options {
      ethernet-switch-profile {
        tag-protocol-id identifier ;
      }
      (flow-control | no-flow-control);
      lacp {
        (active | passive);
        admin-key key;
        periodic interval;
        system-id mac-address;
      }
      (link-protection | no-link-protection);
      link-speed speed;
      (loopback | no-loopback);
      minimum-links number;
      rebalance-periodic;
      source-address-filter filter;
      source-filtering | no-source-filtering;
    }
    description text;
    disable;
    ether-options {
      ```
802.3ad {
  aex;
  (backup | primary);
  lacp {
    force-up;
  }
}
(auto-negotiation | no-auto-negotiation);
(flow-control | no-flow-control);
(loopback | no-loopback);
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds;
link-mode mode;
member interface-name;
member-range starting-interface name to ending-interface name;
mtu bytes;
native-vlan-id
no-gratuitous-arp-request;
speed speed;
traceoptions {
  flag flag;
}
(traps | no-traps);
unit logical-unit-number [
  accept-source-mac {
    mac-address mac-address {
      policer {
        input policer-name;
        output policer-name;
      }
    }
  }
  accounting-profile name;
  arp-resp;
  bandwidth rate;
  description text;
  disable;
  family ccc;
  family ethernet-switching {
    filter {
      input filter-name;
      output filter-name;
    }
  }
  interface-mode (access | trunk);
  recovery-timeout seconds;
  storm-control profile-name;
  vlan {
    members [ members ];
  }
}
family inet {
  accounting {
    destination-class-usage;
    source-class-usage;
  }
address ipv4-address {
  arp ip-address (mac | multicast-mac) mac-address <publish>;
  broadcast address;
  destination-class-usage;
  destination-profile;
  master-only;
  preferred;
  primary;
  vrrp-group group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-key key;
    authentication-type authentication;
    fast-interval milliseconds;
    (preempt | no-preempt) {
      hold-time seconds;
    }
    priority number;
    track {
      interface interface-name {
        priority-cost number;
      }
      priority-hold-time seconds;
      route ip-address/mask routing-instance instance-name priority-cost cost;
    }
    virtual-address [ addresses ];
    virtual-link-local-address address;
    vrrp-inherit-from {
      active-group group-number;
      active-interface interface-name;
    }
  }
}
filter {
  input filter-name;
  output filter-name;
}
mtu bytes;
no-neighbor-learn;
no-redirects;
primary;
rpf-check;
}
family inet6 {
  accounting {
    destination-class-usage;
    source-class-usage;
  }
  address address {
    eui-64;
    ndp ip-address (mac | multicast-mac) mac-address <publish>;
    preferred;
    primary;
    vrrp-inet6-group group-id {
      accept-data | no-accept-data;
      authentication-key key;
authentication-type authentication;
fast-interval milliseconds;
inet6-advertise-interval milliseconds;
preempt | no-preempt {
  hold-time seconds;
}
priority number;
track {
  interface interface-name {
    priority-cost number;
  }
  priority-hold-time seconds;
  route ( address | routing-instance routing-instance-name );
}
virtual-inet6-address [addresses];
virtual-link-local-address ipv6–address;
}
vrp-inherit-from {
  active-group group-name;
  active-interface interface-name;
}
(dad-disable | no-dad-disable);
filter {
  input filter-name;
  output filter-name;
}
mtu bytes;
no-neighbor-learn;
policer {
  input policer-name;
  output policer-name;
}
rpf-check;
}
family iso {
  address interface-address;
  mtu bytes;
}
minimum-links;
mtu;
proxy-arp (restricted | unrestricted);
swap-by-poppush;
(traps | no-traps);
vlan-id vlan-id-number;
}
vlan-tagging;
}

Unsupported Statements in the [edit interfaces interface-range] Hierarchy Level

All statements in the [edit interfaces interface-range] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:
### Table 308: Unsupported [edit interfaces interface-range] Configuration Statements for EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>cesopsn-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>container-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>framing</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>lmi</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>logical-tunnel-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>lsoq-failure-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>multiservice-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>passive-monitor-mode</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>ppp-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>receive-bucket</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>satop-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>serial-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>stacked-vlan-tagging</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>transmit-bucket</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>vdsl-options</td>
<td>[edit interfaces interface-range]</td>
</tr>
<tr>
<td>asynchronous-notification</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
<tr>
<td>ethernet-switch-profile</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
<tr>
<td>ieee-802-3az-eee</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
<tr>
<td>ignore-l3-incompletes</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
<tr>
<td>no-source-filtering</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
<tr>
<td>source-address-filter</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
</tbody>
</table>

**NOTE:** Variables, such as `interface-range`, are not shown in the statements or hierarchies.
Table 308: Unsupported [edit interfaces interface-range] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-filtering</td>
<td>[edit interfaces interface-range ether-options]</td>
</tr>
<tr>
<td>accept-source-mac</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>allow-any-vci</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>atm-l2circuit-mode</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>atm-scheduler-map</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>cell-bundle-size</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>clear-don-fragment-bit</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>compression-device</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>copy-tos-to-outer-ip-hearder</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>diable-mlppp-inner-ppp-pfc</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>dici</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>drop-timeout</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>epd-threshold</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>fragment-threshold</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>input-vlan-map</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>interface-shared-with</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>interleave-fragments</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>inverse-arp</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>link-layer-overhead</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>load-balancing-options</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>mrru</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>multicast-dici</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
</tbody>
</table>
### Table 308: Unsupported [edit interfaces interface-range] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast-vci</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>multilink-max-classes</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>multipoint</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>native-inner-vlan-id</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>oam-liveness</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>oam-period</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>output-vlan-map</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>peer-unit</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>ptp-to-clp</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>point-to-point</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>ppp-options</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>receive-lap</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>service-domain</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>shaping</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>short-sequence</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>transmit-lsp</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>transmit-weight</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>trunk-bandwidth</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>trunk-id</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>tunnel</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>vci</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>vci-range</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>vlan-id-list</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>Statement</td>
<td>Hierarchy</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vpl</td>
<td>[edit interfaces interface-range unit]</td>
</tr>
<tr>
<td>mflr-end-to-end</td>
<td>[edit interfaces interface-range unit family]</td>
</tr>
<tr>
<td>mflr-uni-nni</td>
<td>[edit interfaces interface-range unit family]</td>
</tr>
<tr>
<td>mllppp</td>
<td>[edit interfaces interface-range unit family]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces interface-range unit family]</td>
</tr>
<tr>
<td>tcc</td>
<td>[edit interfaces interface-range unit family]</td>
</tr>
<tr>
<td>vpls</td>
<td>[edit interfaces interface-range unit family]</td>
</tr>
<tr>
<td>bridge-domain-type</td>
<td>[edit interfaces interface-range unit family ethernet-switching]</td>
</tr>
<tr>
<td>inner-vlan-id-list</td>
<td>[edit interfaces interface-range unit family ethernet-switching]</td>
</tr>
<tr>
<td>vlan-rewrite</td>
<td>[edit interfaces interface-range unit family ethernet-switching]</td>
</tr>
<tr>
<td>ipsec-sa</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>multicast-only</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>negotiate-address</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>next-hop-tunnel</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>receive-options-packets</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>receive-ttl-exceeded</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>sampling</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>simple-filter</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>targeted-broadcast</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces interface-range unit family inet]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces interface-range unit family inet address vrrp-group track interface]</td>
</tr>
</tbody>
</table>
Table 308: Unsupported [edit interfaces interface-range] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>[edit interfaces interface-range unit family inet6]</td>
</tr>
<tr>
<td>group</td>
<td>[edit interfaces interface-range unit family inet6 filter]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces interface-range unit family inet6 address vrrp-group track interface]</td>
</tr>
</tbody>
</table>

Related Documentation

• [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2133

[edit interfaces irb] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces irb] hierarchy level on EX Series switches.

• **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.

• **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

• Supported Statements in the [edit interfaces irb] Hierarchy Level on page 2379

• Unsupported Statements in the [edit interfaces irb] Hierarchy Level on page 2382

Supported Statements in the [edit interfaces irb] Hierarchy Level

The following hierarchy shows the [edit interfaces irb] configuration statements supported on EX Series switches.

interfaces {
  irb {
    accounting-profile name;
    description text;
    disable;

    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    mtu bytes;
    no-gratuitous-arp-request;
    traceoptions {
      flag flag;
    }
    (traps | no-traps);
  }
}
unit logical-unit-number {
    accounting-profile name;
    bandwidth rate;
    description text;
    disable;
    family inet {
        accounting {
            destination-class-usage;
            source-class-usage {
                input;
                output;
            }
        }
        address ipv4-address {
            arp ip-address (mac | multicast-mac) mac-address <publish>;
            broadcast address;
            preferred;
            primary;
            vrrp-group group-number {
                (accept-data | no-accept-data);
                advertise-interval seconds;
                advertisements-threshold number;
                authentication-key key;
                authentication-type authentication;
                fast-interval milliseconds;
                (preempt | no-preempt) {
                    hold-time seconds;
                }
                priority number;
                track {
                    interface interface-name {
                        priority-cost number;
                    }
                    priority-hold-time seconds;
                    route ip-address/mask routing-instance instance-name priority-cost cost;
                }
                virtual-address [addresses];
                vrrp-inherit-from {
                    active-group group-number;
                    active-interface interface-name;
                }
            }
        }
    }
    filter {
        input filter-name;
        output filter-name;
    }
    mtu bytes;
    no-neighbor-learn;
    no-redirects;
    primary;
    rpf-check {
        fail-filter filter-name;
        mode {
            loose;
        }
    }
}

Copyright © 2013, Juniper Networks, Inc.
family inet6 {
  accounting {
    destination-class-usage;
    source-class-usage {
      input;
      output;
    }
  }
  address address {
    eui-64;
    ndp ip-address (mac | multicast-mac) mac-address <publish>;
    preferred;
    primary;
    vrrp-inet6-group group-id {
      accept-data | no-accept-data;
      advertisements-threshold number;
      authentication-key key;
      authentication-type authentication;
      fast-interval milliseconds;
      inet6-advertise-interval milliseconds;
      preempt | no-preempt {
        hold-time seconds;
      }
      priority number;
      track {
        interface interface-name {
          priority-cost number;
        }
        priority-hold-time seconds;
        route ip-address/mask routing-instance instance-name priority-cost cost;
      }
    virtual-inet6-address [addresses];
    virtual-link-local-address ipv6-address;
    vrrp-inherit-from {
      active-group group-number;
      active-interface interface-name;
    }
  }
  (dad-disable | no-dad-disable);
  filter {
    input filter-name;
    output filter-name;
  }
  mtu bytes;
  nd6-stale-time seconds;
  no-neighbor-learn;
  no-redirects;
  policer {
    input policer-name;
    output policer-name;
  }
  rpf-check {
    fail-filter filter-name;
mode {
    loose;
}
}
}
}
}
family iso {
    address interface-address;
    mtu bytes;
}
native-inner-vlan-id vlan-id;
proxy-arp (restricted | unrestricted);
(traps | no-traps);
vlan-id-list [vlan-id's];
vlan-id-range [vlan-id-range];
} }
}
}

Unsupported Statements in the [edit interfaces irb] Hierarchy Level

All statements in the [edit interfaces irb] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 309: Unsupported [edit interfaces irb] Configuration Statements for EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation</td>
<td>[edit interfaces irb]</td>
</tr>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces irb unit]</td>
</tr>
<tr>
<td>ccc</td>
<td>[edit interfaces irb unit family]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces irb unit family]</td>
</tr>
<tr>
<td>tcc</td>
<td>[edit interfaces irb unit family]</td>
</tr>
<tr>
<td>vpis</td>
<td>[edit interfaces irb unit family]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces irb unit family inet]</td>
</tr>
<tr>
<td>sampling</td>
<td>[edit interfaces irb unit family inet]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces irb unit family inet]</td>
</tr>
<tr>
<td>targeted-broadcast</td>
<td>[edit interfaces irb unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces irb unit family inet]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces irb unit family inet address vrrp-group track interface]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces irb unit family inet6]</td>
</tr>
</tbody>
</table>
Table 309: Unsupported [edit interfaces irb] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces irb unit family inet6 address vrrp-inet6-group track interface]</td>
</tr>
<tr>
<td>group</td>
<td>[edit interfaces irb unit family inet6 filter]</td>
</tr>
</tbody>
</table>

Related Documentation

[edit interfaces lo] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces lo] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit interfaces lo] Hierarchy Level on page 2383
- Unsupported Statements in the [edit interfaces lo] Hierarchy Level on page 2385

Supported Statements in the [edit interfaces lo] Hierarchy Level

The following hierarchy shows the [edit interfaces lo] configuration statements supported on EX Series switches.

```
interfaces {
    lo0 {
        accounting-profile name;
        description text;
        disable;
        hold-time down milliseconds up milliseconds ;
        traceoptions {
            flag flag;
        } (traps | no-traps);
        unit logical-unit-number {
            accounting-profile name;
            arp-resp;
            bandwidth rate;
            description text;
            disable;
            family ccc;
        }
    }
```
family inet {
    address ipv4-address {
        preferred;
        primary;
        vrrp-group group-number {
            (accept-data | no-accept-data);
            advertise-interval seconds;
            authentication-key key;
            authentication-type authentication;
            fast-interval milliseconds;
            (preempt | no-preempt) {
                hold-time seconds;
            }
            priority number;
        }
        track {
            interface interface-name {
                bandwidth-threshold bandwidth;
                priority-cost number;
            }
            priority-hold-time seconds;
        }
        virtual-address [ addresses ];
        virtual-link-local-address;
        vrrp-inherit-from {
            active-group group-number;
            active-interface interface-name;
        }
    }
}

dhcp {
    client-identifier (ascii client-id | hexadecimal client-id);
    lease-time (seconds | infinite);
    retransmission-attempt number;
    retransmission-interval sections;
    server-address ip-address;
    update-server
    vendor-id
}

filter {
    input filter-name;
    output filter-name;
}

no-neighbor-learn;
no-redirects;
primary;
}

family inet6 {
    address address {
        preferred;
        primary;
        vrrp-inet6-group group-id {
            accept-data | no-accept-data;
            authentication-key key;
            authentication-type authentication;
            fast-interval milliseconds;
        }
    }
}
inet6-advertise-interval milliseconds;
preempt | no-preempt {
  hold-time seconds;
}
priority number;
track {
  interface interface-name {
    bandwidth-threshold bandwidth priority-cost number;
  }
  priority-hold-time seconds;
  route ( address | routing-instance routing-instance-name );
}
virtual-inet6-address [addresses];
virtual-link-local-address ipv6-address;
vrp-inherit-from {
  active-group group-name;
  active-interface interface-name;
}
(dad-disable | no-dad-disable);
filter {
  group group-name;
  input filter-name;
  output filter-name;
}
no-neighbor-learn;
policer {
  input policer-name;
  output policer-name;
}
family iso {
  address interface-address;
}
family mpls;
(traps | no-traps);
}
}

Unsupported Statements in the [edit interfaces lo] Hierarchy Level

All statements in the [edit interfaces lo] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces lo unit]</td>
</tr>
<tr>
<td>any</td>
<td>[edit interfaces lo unit family]</td>
</tr>
</tbody>
</table>
Table 310: Unsupported [edit interfaces lo] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcc</td>
<td>[edit interfaces lo unit family]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces lo unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces lo unit family inet]</td>
</tr>
</tbody>
</table>

Related Documentation

- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches
- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2133

[edit interfaces me] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces me] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit interfaces me] Hierarchy Level on page 2386
- Unsupported Statements in the [edit interfaces me] Hierarchy Level on page 2388

**Supported Statements in the [edit interfaces me] Hierarchy Level**

The following hierarchy shows the [edit interfaces me] configuration statements supported on EX Series switches.

```plaintext
interfaces {
  me0 {
    accounting-profile name;
    description text;
    disable;
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    no-gratuitous-arp-request;
    traceoptions {
      flag flag;
    }
    (traps | no-traps);
    unit logical-unit-number {
```
accounting-profile name;
ar-presp;
bandwidth rate;
description text;
disable;
family ethernet-switching {
  filter {
    input filter-name;
    output filter-name;
  }
native-vlan-id vlan-id-number;
port-mode (access | trunk);
  vlan {
    members [ members ];
  }
}
family inet {
  accounting {
    destination-class-usage;
    source-class-usage {
      input;
      output;
    }
  }
  address ipv4-address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    master-only;
    preferred;
    primary;
  }
  dhcp {
    client-identifier (ascii client-id | hexadecimal client-id);
    lease-time (seconds | infinite);
    retransmission-attempt number;
    retransmission-interval sections;
    server-address ip-address;
    update-server
    vendor-id
  }
  filter {
    input filter-name;
    output filter-name;
  }
  mtu bytes;
  no-neighbor-learn;
  primary;
  rpf-check;
}
family inet6 {
  accounting {
    destination-class-usage;
    source-class-usage {
      input;
      output;
    }
  }
Unsupported Statements in the [edit interfaces me] Hierarchy Level

All statements in the [edit interfaces me] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 311: Unsupported [edit interfaces me] Configuration Statements for EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>encapsulation</td>
<td>[edit interfaces me]</td>
</tr>
<tr>
<td>link-mode</td>
<td>[edit interfaces me]</td>
</tr>
<tr>
<td>encapsulation</td>
<td>[edit interfaces me unit]</td>
</tr>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces me unit]</td>
</tr>
<tr>
<td>native-inner-vlan-id</td>
<td>[edit interfaces me unit]</td>
</tr>
</tbody>
</table>
Table 311: Unsupported [edit interfaces me] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id-list</td>
<td>[edit interfaces me unit]</td>
</tr>
<tr>
<td>vlan-id-range</td>
<td>[edit interfaces me unit]</td>
</tr>
<tr>
<td>ccc</td>
<td>[edit interfaces me unit family]</td>
</tr>
<tr>
<td>tcc</td>
<td>[edit interfaces me unit family]</td>
</tr>
<tr>
<td>vpls</td>
<td>[edit interfaces me unit family]</td>
</tr>
<tr>
<td>no-redirects</td>
<td>[edit interfaces me unit family inet]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces me unit family inet]</td>
</tr>
<tr>
<td>sampling</td>
<td>[edit interfaces me unit family inet]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces me unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces me unit family inet]</td>
</tr>
<tr>
<td>vrrp-group</td>
<td>[edit interfaces me unit family inet address]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces me unit family inet6]</td>
</tr>
<tr>
<td>vrrp-inet6-group</td>
<td>[edit interfaces me unit family inet6 address]</td>
</tr>
</tbody>
</table>

Related Documentation

- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2133

[edit interfaces vme] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces vme] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see "EX Series Switch Software Features Overview" on page 27.
This topic lists:

- Supported Statements in the [edit interfaces vme] Hierarchy Level on page 2390
- Unsupported Statements in the [edit interfaces vme] Hierarchy Level on page 2392

**Supported Statements in the [edit interfaces vme] Hierarchy Level**

The following hierarchy shows the [edit interfaces vme] configuration statements supported on EX Series switches.

```
interfaces {
  vme {
    accounting-profile name;
    description text;
    disable;
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    mtu bytes;
    no-gratuitous-arp-request;
    traceoptions {
      flag flag;
    }
    (traps | no-traps);
  } unit logical-unit-number {
    accounting-profile name;
    arp-resp;
    bandwidth rate;
    description text;
    disable;
    family inet {
      accounting {
        destination-class-usage;
        source-class-usage {
          input;
          output;
        }
      }
      address ipv4-address {
        arp ip-address (mac | multicast-mac) mac-address <publish>;
        broadcast address;
        master-only;
        preferred;
        primary;
        vrrp-group group-number {
          (accept-data | no-accept-data);
          advertise-interval seconds;
          authentication-key key;
          authentication-type authentication;
          fast-interval milliseconds;
          (preempt | no-preempt) {
            hold-time seconds;
          }
        }
        priority number;
        track {
          interface interface-name {
```
bandwidth-threshold bandwidth;
  priority-cost number;
}
  priority-hold-time seconds;
  route ip-address/mask routing-instance instance-name priority-cost cost;
}
virtual-address [ addresses ];
virtual-link-local-address address;
vrp-inherit-from {
  active-group group-number;
  active-interface interface-name;
}
}
}
}
dhcp {
  client-identifier (ascii client-id | hexadecimal client-id);
  lease-time (seconds | infinite);
  retransmission-attempt number;
  retransmission-interval sections;
  server-address ip-address;
  update-server vendor-id
}
filter {
  input filter-name;
  output filter-name;
}
mtu bytes;
no-neighbor-learn;
primary;
rpf-check;
}
family inet6 {
  accounting {
    destination-class-usage;
    source-class-usage {
      input;
      output;
    }
  }
  address address {
    eui-64;
    ndp ip-address (mac | multicast-mac) mac-address <publish>;
    preferred;
    primary;
    vrrp-inet6-group group-id {
      accept-data | no-accept-data;
      authentication-key key;
      authentication-type authentication;
      fast-interval milliseconds;
      inet6-advertise-interval milliseconds;
      preempt | no-preempt {
        hold-time seconds;
      }
      priority number;
    track {

interface interface-name {
    bandwidth-threshold bandwidth priority-cost number;
    priority-cost number;
}
priority-hold-time seconds;
route (address | routing-instance routing-instance-name);
}
virtual-inet6-address [addresses];
virtual-link-local-address ipv6-address;
vrp-inherit-from {
    active-group group-name;
    active-interface interface-name;
};
}
(dad-disable | no-dad-disable);
filter {
    group group-name;
    input filter-name;
    output filter-name;
}
mtu bytes;
no-neighbor-learn;
policer {
    input policer-name;
    output policer-name;
}
rpf-check;
}
family iso {
    address interface-address;
    mtu bytes;
}
family mpls {
    mtu bytes;
}
(traps|no-traps);
vlan-id vlan-id-number;
}
vlan-tagging;
}

Unsupported Statements in the [edit interfaces vme] Hierarchy Level

All statements in the [edit interfaces vme] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches
- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2133
[edit interfaces xe] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit interfaces xe] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit interfaces xe] Hierarchy Level on page 2393
- Unsupported Statements in the [edit interfaces xe] Hierarchy Level on page 2396

Supported Statements in the [edit interfaces xe] Hierarchy Level

The following hierarchy shows the [edit interfaces xe] configuration statements supported on EX Series switches.

```plaintext
interfaces {
  xe-fpc/pic/port {
    accounting-profile name;
    description text;
    disable;
    encapsulation type;
    ether-options {
      802.3ad {
        (backup | primary);
        lacp {
          force-up;
          port-priority number;
        }
      }
    (auto-negotiation | no-auto-negotiation);
    (flow-control | no-flow-control);
    (loopback | no-loopback);
  }
  ( gratuitous-arp-reply | no-gratuitous-arp-reply);
  hold-time up milliseconds down milliseconds;
  link mode {
    full-duplex;
  }
  mtu bytes;
  native-vlan-id
  no-gratuitous-arp-request;
  traceoptions {
    flag flag;
  }
  (traps | no-traps);
```
unit logical-unit-number {
  accounting-profile name;
  bandwidth rate;
  description text;
  disable;
  encapsulation type;
  family ccc {
    filter {
      input filter-name;
      output filter-name;
    }
    policer{
      input policer-name;
      output policer-name;
    }
  }
  family ethernet-switching {
    filter {
      input filter-name;
      output filter-name;
    }
    interface-mode (access | trunk);
    recovery-timeout seconds;
    storm-control profile-name;
    vlan {
      members (vlan-name | [vlan-names] | all);
    }
  }
  family inet {
    accounting {
      destination-class-usage;
      source-class-usage {
        input;
        output;
      }
    }
    address ipv4-address {
      arp ip-address (mac | multicast-mac) mac-address <publish>;
      broadcast address;
      preferred;
      primary;
      vrrp-group group-number {
        (accept-data | no-accept-data);
        advertise-interval seconds;
        advertisements-thresholds number;
        authentication-key key;
        authentication-type authentication;
        fast-interval milliseconds;
        (preempt | no-preempt) {
          hold-time seconds;
        }
        priority number;
        track {
          interface interface-name {
            priority-cost number;
          }
        }
      }
    }
  }
}
priority-hold-time seconds;
route ip-address/mask routing-instance instance-name priority-cost cost;
}
virtual-address [addresses];
vrp-inherit-from {
    active-group group-number;
    active-interface interface-name;
}
}
}
filter {
    input filter-name;
    output filter-name;
}
mtu bytes;
no-neighbor-learn;
no-redirects;
primary;
rpf-check {
    fail-filter filter-name;
    mode {
        loose;
    }
}
}
family inet6 {
    accounting {
        destination-class-usage;
        source-class-usage {
            input;
            output;
        }
    }
}
address address {
    eui-64;
    ndp ip-address (mac | multicast-mac) mac-address <publish>;
    preferred;
    primary;
    vrrp-inet6-group group-id {
        accept-data | no-accept-data;
        authentication-key key;
        authentication-type authentication;
        fast-interval milliseconds;
        inet6-advertise-interval milliseconds;
        preempt | no-preempt {
            hold-time seconds;
        }
    }
    priority number;
    track {
        interface interface-name {
            priority-cost number;
        }
    }
    priority-hold-time seconds;
    route (address | routing-instance routing-instance-name);
}
virtual-inet6-address [addresses];
virtual-link-local-address ipv6-address;  
vrp-inherit-from {  
    active-group group-name;  
    active-interface interface-name;  
  }  
}  
dad-disable | no-dad-disable;  
filter {  
    input filter-name;  
    output filter-name;  
}  
mtu bytes;  
no-neighbor-learn;  
no-redirects;  
policer {  
    input policer-name;  
    output policer-name;  
}  
rpf-check {  
    fail-filter filter-name;  
    mode {  
        loose;  
    }  
}  
family iso {  
    address interface-address;  
    mtu bytes;  
}  
interface-shared-with psdn numerical-index;  
proxy-arp (restricted | unrestricted);  
swap-by-poppush;  
(traps | no-traps);  
vlan-id (Layer 3 Subinterfaces) vlan-id-number;  
}  
vlan-tagging;  
}

Unsupported Statements in the [edit interfaces xe] Hierarchy Level

All statements in the [edit interfaces xe] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 312: Unsupported [edit interfaces xe] Configuration Statements for EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>clocking</td>
<td>[edit interfaces xe]</td>
</tr>
<tr>
<td>framing</td>
<td>[edit interfaces xe]</td>
</tr>
<tr>
<td>passive-monitor-mode</td>
<td>[edit interfaces xe]</td>
</tr>
</tbody>
</table>
Table 312: Unsupported [edit interfaces xe] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>stacked-vlan-tagging</td>
<td>[edit interfaces xe]</td>
</tr>
<tr>
<td>ynchronous-notification</td>
<td>[edit interfaces xe ether-options]</td>
</tr>
<tr>
<td>ethernet-switch-profile</td>
<td>[edit interfaces xe ether-options]</td>
</tr>
<tr>
<td>ignore-l3-incompletes</td>
<td>[edit interfaces xe ether-options]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces xe ether-options]</td>
</tr>
<tr>
<td>source-address-filter</td>
<td>[edit interfaces xe ether-options]</td>
</tr>
<tr>
<td>source-filtering</td>
<td>[edit interfaces xe ether-options]</td>
</tr>
<tr>
<td>no-source-filtering</td>
<td>[edit interfaces xe ether-options]</td>
</tr>
<tr>
<td>accept-source-mac</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>input-vlan-map</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>layer2-policer</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>native-inner-vlan-id</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>output-vlan-map</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>vlan-id-list</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>vlan-id-range</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>vlan-tags</td>
<td>[edit interfaces xe unit]</td>
</tr>
<tr>
<td>mpls</td>
<td>[edit interfaces xe unit family]</td>
</tr>
<tr>
<td>tcc</td>
<td>[edit interfaces xe unit family]</td>
</tr>
<tr>
<td>vpls</td>
<td>[edit interfaces xe unit family]</td>
</tr>
<tr>
<td>bridge-domain-type</td>
<td>[edit interfaces xe unit family ethernet-switching]</td>
</tr>
<tr>
<td>inner-vlan-id-list</td>
<td>[edit interfaces xe unit family ethernet-switching]</td>
</tr>
<tr>
<td>vlan-rewrite</td>
<td>[edit interfaces xe unit family ethernet-switching]</td>
</tr>
<tr>
<td>policer</td>
<td>[edit interfaces xe unit family inet]</td>
</tr>
</tbody>
</table>
### Table 312: Unsupported [edit interfaces xe] Configuration Statements for EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>sampling</td>
<td>[edit interfaces xe unit family inet]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces xe unit family inet]</td>
</tr>
<tr>
<td>simple-filter</td>
<td>[edit interfaces xe unit family inet]</td>
</tr>
<tr>
<td>targeted-broadcast</td>
<td>[edit interfaces xe unit family inet]</td>
</tr>
<tr>
<td>unnumbered-address</td>
<td>[edit interfaces xe unit family inet]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces xe unit family inet address vrrp-group track interface]</td>
</tr>
<tr>
<td>service</td>
<td>[edit interfaces xe unit family inet6]</td>
</tr>
<tr>
<td>bandwidth-threshold</td>
<td>[edit interfaces xe unit family inet6 address vrrp-group track interface]</td>
</tr>
<tr>
<td>group</td>
<td>[edit interfaces xe unit family inet6 filter]</td>
</tr>
</tbody>
</table>

**Related Documentation**
- [edit interfaces] Configuration Statement Hierarchy on EX Series Switches on page 2133

### [edit protocols lacp] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit protocols lacp] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:
- Supported Statements in the [edit protocols lacp] Hierarchy Level on page 2398
- Unsupported Statements in the [edit protocols lacp] Hierarchy Level on page 2399

### Supported Statements in the [edit protocols lacp] Hierarchy Level

The following hierarchy shows the [edit protocols lacp] configuration statements supported on EX Series switches:

```plaintext
protocols {
  lacp {
```
Unsupported Statements in the [edit protocols lACP] Hierarchy Level

All statements in the [edit protocols lACP] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation
- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
802.3ad

Syntax

802.3ad {
  aex;
  (backup | primary);
  lacp {
    force-up;
    port-priority
  }
}

Hierarchy Level  [edit interfaces interface-name ether-options]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure membership in a link aggregation group (LAG).

Options

- **aex**—Name of the LAG.
- **backup**—Designate the interface as the backup interface for link-protection mode.
- **primary**—Designate the interface as the primary interface for link-protection mode.

The remaining statements are described separately.

Required Privilege Level  interface—To view this statement in the configuration.

interfaced-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Multicast Load Balancing for Use with Aggregated 10-Gigabit Ethernet Interfaces on EX8200 Switches
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
accounting-profile

Syntax  accounting-profile name;

Hierarchy Level  [edit interfaces interface-name],
                 [edit interfaces interface-name unit logical-unit-number],
                 [edit interfaces interface-range name]

Release Information  Statement introduced before Junos OS Release 7.4.
                    Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Enable collection of accounting data for the specified physical or logical interface or interface range.

Options  name—Name of the accounting profile.

Required Privilege  Level

       interface—To view this statement in the configuration.
       interface-control—To add this statement to the configuration.

Related Documentation  • Applying an Accounting Profile to the Physical Interface on page 2328
                       • Applying an Accounting Profile to the Logical Interface on page 2329
address

Syntax

```
address address {
  arp ip-address (mac | multicast-mac) mac-address <publish>;
  broadcast address;
  destination address;
  destination-profile name;
  eui-64;
  master-only;
  multipoint-destination address dlci dlci-identifier;
  multipoint-destination address {
    epd-threshold cells;
    inverse-arp;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst length);
      queue-length number;
    }
    vci vpi-identifier vci-identifier;
  }
  primary;
  preferred;
  (vrrp-group | vrrp-inet6-group) group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-type authentication;
    authentication-key key;
    fast-interval milliseconds;
    (preempt | no-preempt) {
      hold-time seconds;
    }
    priority-number number;
    track {
      priority-cost seconds;
      priority-hold-time interface-name {
        interface priority;
        bandwidth-threshold bits-per-second {
          priority;
        }
      }
      route ip-address/mask routing-instance instance-name priority-cost cost;
    }
    virtual-address [ addresses ];
  }
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]
```
### Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

### Description
Configure the interface address.

### Options
- **address**—Address of the interface.

The remaining statements are explained separately.

---

**NOTE:** The `edit logical-systems hierarchy` is not available on QFabric systems.

---

### Required Privilege Level
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

### Related Documentation
- [Configuring the Protocol Family](#)
- `negotiate-address`
- `unnumbered-address (Ethernet)`
- [Junos OS Administration Library for Routing Devices](#)
- `family on page 1482`
aggregated-devices

Syntax

```aggregated-devices { ethernet (Aggregated Devices) { device-count number; lacp } }```

Hierarchy Level

[edit chassis]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure properties for aggregated devices on the switch.

The remaining statements are explained separately.

Default

Aggregated devices are disabled.

Required Privilege

Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272
- Junos OS Ethernet Interfaces Configuration Guide
**aggregated-ether-options**

**Syntax**

```plaintext
aggregated-ether-options {
  flow-control | no-flow-control;
  lACP {
    (active | passive);
    admin-key key;
    periodic interval;
    system-id mac-address;
  }
  (link-protection | no-link-protection);
  link-speed speed;
  (loopback | no-loopback);
  minimum-links number;
  system-priority
}
```

**Hierarchy Level**

[edit interfaces aex]

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the aggregated Ethernet properties of a specific aggregated Ethernet interface.

The remaining statements are explained separately.

**Required Privilege Level**
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272
- Junos OS Ethernet Interfaces Configuration Guide
arp (Interfaces)

Syntax  
```
arp ip-address (mac | multicast-mac) mac-address publish;
```

Hierarchy Level  
```
[edit interfaces interface-name unit logical-unit-number family inetaddress address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inetaddress address]
```

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
For Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, configure Address Resolution Protocol (ARP) table entries, mapping IP addresses to MAC addresses.

Options  
- `ip-address`—IP address to map to the MAC address. The IP address specified must be part of the subnet defined in the enclosing `address` statement.

- `mac mac-address`—MAC address to map to the IP address. Specify the MAC address as six hexadecimal bytes in one of the following formats: `nnnn.nnnn.nnnn` or `nn:nn:nn:nn:nn:nn`. For example, `0011.2233.4455` or `00:11:22:33:44:55`.

- `multicast-mac mac-address`—Multicast MAC address to map to the IP address. Specify the multicast MAC address as six hexadecimal bytes in one of the following formats: `nnnn.nnnn.nnnn` or `nn:nn:nn:nn:nn:nn`. For example, `0011.2233.4455` or `00:11:22:33:44:55`.

- `publish`—(Optional) Have the router or switch reply to ARP requests for the specified IP address. If you omit this option, the router or switch uses the entry to reach the destination but does not reply to ARP requests.

---

**NOTE:** The `edit logical-systems` hierarchy is not available on QFabric systems.

Required Privilege Level  
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation  
- Configuring Static ARP Table Entries on page 2332
- Configuring Static ARP Entries
**auto-negotiation**

**Syntax**

(auto-negotiation | no-auto-negotiation) <remote-fault (local-interface-online | local-interface-offline)>;

**Hierarchy Level**

[edit interfaces interface-name ether-options],
[edit interfaces interface-name gigether-options],
[edit interfaces ge-pim/0/0 switch-options switch-port port-number]

**Release Information**

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 8.4 for J Series Services Routers.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

**Description**

For Gigabit Ethernet interfaces on M Series, MX Series, T Series, TX Matrix routers, and ACX Series routers explicitly enable autonegotiation and remote fault. For EX Series switches and J Series Services Routers, explicitly enable autonegotiation only.

- **auto-negotiation**—Enables autonegotiation. This is the default.
- **no-auto-negotiation**—Disable autonegotiation. When autonegotiation is disabled, you must explicitly configure the link mode and speed.

When you configure Tri-Rate Ethernet copper interfaces to operate at 1 Gbps, autonegotiation must be enabled.

---

**NOTE:** On EX Series switches, an interface configuration that disables autonegotiation and manually sets the link speed to 1 Gbps is accepted when you commit the configuration; however, if the interface you are configuring is a Tri-Rate Ethernet copper interface, the configuration is ignored as invalid and autonegotiation is enabled by default.

To correct the invalid configuration and disable autonegotiation:

1. Delete the no-auto-negotiation statement and commit the configuration.
2. Set the link speed to 10 or 100 Mbps, set no-auto-negotiation, and commit the configuration.

On J Series Services Routers with universal Physical Interface Modules (uPIMs) and on EX Series switches, if the link speed and duplex mode are also configured, the interfaces use the values configured as the desired values in the negotiation. If autonegotiation is disabled, the link speed and link mode must be configured.

---

**NOTE:** On T4000 routers, the auto-negotiation command is ignored for interfaces other than Gigabit Ethernet.
<table>
<thead>
<tr>
<th>Default</th>
<th>Autonegotiation is automatically enabled. No explicit action is taken after the autonegotiation is complete or if the negotiation fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>remote-fault (local-interface-online</td>
</tr>
<tr>
<td>Default:</td>
<td>local-interface-online</td>
</tr>
</tbody>
</table>

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Gigabit Ethernet Autonegotiation Overview
- Configuring J Series Services Router Switching Interfaces
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
## bandwidth (Interfaces)

**Syntax**

```
bandwidth rate;
```

**Hierarchy Level**

- [edit interfaces interface-name unit logical-unit-number],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure an informational-only bandwidth value for an interface. This statement is valid for all logical interface types except multilink and aggregated interfaces.

**NOTE:** We recommend that you be careful when setting this value. Any interface bandwidth value that you configure using the `bandwidth` statement affects how the interface cost is calculated for a dynamic routing protocol, such as OSPF. By default, the interface cost for a dynamic routing protocol is calculated using the following formula:

\[
\text{cost} = \frac{\text{reference-bandwidth}}{\text{bandwidth}},
\]

where bandwidth is the physical interface speed. However, if you specify a value for bandwidth using the `bandwidth` statement, that value is used to calculate the interface cost, rather than the actual physical interface bandwidth.

**Options**

- `rate`—Peak rate, in bits per second (bps) or cells per second (cps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation `k` (1000), `m` (1,000,000), or `g` (1,000,000,000). You can also specify a value in cells per second by entering a decimal number followed by the abbreviation `c`; values expressed in cells per second are converted to bits per second by means of the formula 1 cps = 384 bps.

**Range:** Not limited.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring the Interface Bandwidth on page 2306
### broadcast

**Syntax**

```
broadcast address;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family family address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Set the broadcast address on the network or subnet. On a subnet you cannot specify a host address of 0, nor can you specify a broadcast address.

**Default**

The default broadcast address has a host portion of all ones.

**Options**

`address`—Broadcast address. The address must have a host portion of either all ones or all zeros. You cannot specify the addresses `0.0.0.0` or `255.255.255.255`.

**NOTE:** The `edit logical-systems` hierarchy is not available on QFabric systems.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring the Interface Address on page 2302
chassis

Syntax

chassis {
  aggregated-devices {
    ethernet (Aggregated Devices) {
      device-count number;
    }
  }
  auto-image-upgrade;
  fpc slot {
    pic pic-number {
      sfpplus {
        pic-mode mode;
      }
    }
    power-budget-priority priority;
  }
  lcd-menu {
    fpc slot-number {
      menu-item (menu-name | menu-option) {
        disable;
      }
    }
  }
  nssu {
    upgrade-group group-name {
      fpcs (NSSU Upgrade Groups) (slot-number | [list-of-slot-numbers]);
      member (NSSU Upgrade Groups) member-id {
        fpcs (NSSU Upgrade Groups) (slot-number | [list-of-slot-numbers]);
      }
    }
  }
  PSU {
    redundancy {
      n-plus-n (Power Management);
    }
    redundancy {
      graceful-switchover;
    }
  }
}

Hierarchy Level  [edit]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure chassis-specific properties for the switch.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.
Related Documentation

- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Upgrading Software Using Automatic Software Download
- Configuring the LCD Panel on EX Series Switches (CLI Procedure) on page 115
- Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504
- Configuring Power Supply Redundancy (CLI Procedure) on page 2223
- Configuring the Power Priority of Line Cards (CLI Procedure)
- Configuring Line-Card Upgrade Groups for Nonstop Software Upgrade (CLI Procedure)
description (Interfaces)

Syntax
description text;

Hierarchy Level
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

Description
Provide a textual description of the interface or the logical unit. Any descriptive text you include is displayed in the output of the show interfaces commands, and is also exposed in the ifAlias Management Information Base (MIB) object. It has no effect on the operation of the interface on the router or switch.

The textual description can also be included in the extended DHCP relay option 82 Agent Circuit ID suboption.

Options
text—Text to describe the interface. If the text includes spaces, enclose the entire text in quotation marks.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring Interface Description
• Adding a Logical Unit Description to the Configuration on page 2299
• Configuring Gigabit Ethernet Interfaces (CLI Procedure)
• Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
• Configuring Gigabit and 10-Gigabit Ethernet Interfaces
• Enabling and Disabling Insertion of Option 82 Information on page 1303
• Junos OS Network Interfaces Library for Routing Devices
• Example: Connecting Access Switches to a Distribution Switch on page 2083
**device-count**

**Syntax**
```
device-count number;
```

**Hierarchy Level**
```
[edit chassis aggregated-devices ethernet (Aggregated Devices)]
```

**Release Information**

**Description**
Configure the number of aggregated Ethernet logical devices available to the switch.

**Options**
- `number`—Maximum number of aggregated Ethernet logical interfaces on the switch.
  - **Range**: 1 through 32 for EX2200, EX3200, and standalone EX3300 switches and for EX3300 Virtual Chassis
  - **Range**: 1 through 64 for standalone EX4200, standalone EX4500, and EX6200 switches and for EX4200 and EX4500 Virtual Chassis
  - **Range**: 1 through 239 for EX8200 Virtual Chassis
  - **Range**: 1 through 255 for standalone EX8200 switches

**Required Privilege Level**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch*
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- *Junos OS Network Interfaces Configuration Guide*
disable (Interface)

**Syntax**
```plaintext
disable;
```

**Hierarchy Level**
- `[edit interfaces interface-name]`
- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]`

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

**Description**
Disable a physical or a logical interface, effectively unconfiguring it.

---

**CAUTION:**
- Dynamic subscribers and logical interfaces use physical interfaces for connection to the network. The Junos OS allows you to set the interface to disable and commit the change while dynamic subscribers and logical interfaces are still active. This action results in the loss of all subscriber connections on the interface. Use care when disabling interfaces.
- If aggregated SONET links are configured between a T1600 router and a T4000 router, interface traffic is disrupted when you disable the physical interface configured on the T1600 router. If you want to remove the interface, we recommend that you deactivate the interface instead of disabling it.

---

**NOTE:**
- When you use the disable statement at the `[edit interfaces]` hierarchy level, depending on the PIC type, the interface might or might not turn off the laser. Older PIC transceivers do not support turning off the laser, but newer Gigabit Ethernet (GE) PICs with SFP and XFP transceivers do support it and the laser will be turned off when the interface is disabled.
- When you disable or deactivate an interface, then all the references made to the deactivated interface must be removed from the routing instance.

---

**WARNING:** Do not stare into the laser beam or view it directly with optical instruments even if the interface has been disabled.
**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Disabling a Physical Interface on page 2299
- Disabling a Logical Interface on page 2301

### eui-64

**Syntax**
eui-64;

**Hierarchy Level**
[edit interfaces interface-name unit number family inet6 address address]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

**Description**
For interfaces that carry IP version 6 (IPv6) traffic, automatically generate the host number portion of interface addresses. Not supported on QFX Series switches.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring the Interface Address on page 2302
ether-options

Syntax  Gigabit Ethernet interfaces:

```
ether-options {
  802.3ad {
    aex;
    (backup | primary);
    lACP {
      force-up;
      port-priority
    }
  }
  (auto-negotiation | no-auto-negotiation);
  (flow-control | no-flow-control);
  iEEE-802-3az-EEE;
  link-mode mode;
  (loopback | no-loopback);
  speed (speed | auto-negotiation);
}
```

10-Gigabit Ethernet interfaces:

```
ether-options {
  802.3ad {
    aex;
    (backup | primary);
    lACP {
      force-up;
      port-priority
    }
  }
  (flow-control | no-flow-control);
  (loopback | no-loopback);
}
```

Hierarchy Level

[edit interfaces interface-name],
[edit interfaces interface-range range]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure Ethernet properties for a Gigabit Ethernet interface or a 10-Gigabit Ethernet interface on an EX Series switch.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
ethernet (Aggregated Devices)

Syntax

ethernet {
  device-count number;
  lacp {
    link-protection {
      non-revertive;
    }
    system-priority;
  }
}

Hierarchy Level
[edit chassis aggregated-devices]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure properties for Ethernet aggregated devices on the switch.

The remaining statement is explained separately.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
- Junos OS Ethernet Interfaces Configuration Guide
family

Syntax
family ccc on page 1482
family ethernet-switching on page 1482
family inet on page 1482
family inet6 on page 1483
family ison on page 1483

family ccc

family ccc;
filter {
group group-number;
input filter-name;
input-list [filter-names];
output filter-name;
output-list [filter-names];
}
policer {
input policer-name;
output policer-name;
}
}

family ethernet-switching

family ethernet-switching{
filter {
input filter-name;
output filter-name;
}
interface-mode (access|trunk);
recovery-timeout seconds;
storm-control profile-name;
vlan {
members (vlan-name [-vlan-names] all);
}
}

family inet

family inet{
accounting {
destination-class-usage;
source-class-usage {
input;
output;
}
}
address ipv4-address {
arp ip-address (mac | multicast-mac) mac-address <publish>;
broadcast address;
preferred;
primary;
vrp-group group-number {
(accept-data | no-accept-data);
advertise-interval seconds;
advertisements-threshold number;
authentication-key key key;
authentication-type authentication;
}
fast-interval milliseconds;
(preempt | no-preempt) {
  hold-time seconds;
}
priority number;
track {
  interface interface-name {
    priority-cost number;
  }
priority-hold-time seconds;
  route ip-address/mask routing-instance instance-name priority-cost cost;
}
virtual-address [addresses];
vrrp-inherit-from {
  active-group group-number;
  active-interface interface-name;
}
}
}
filter {
  input filter-name;
  output filter-name;
}
mtu bytes;
no-neighbor-learn;
no-redirects;
primary;
rpf-check {
  fail-filter filter-name;
  mode {
    loose;
  }
}
}
family inet6

family inet6 [  
    accounting {  
        destination-class-usage;  
        source-class-usage {  
            input;  
            output;  
        }  
    }  
]

address address [  
    eui-64;  
    ndp ip-address (mac | multicast-mac) mac-address <publish>;  
    preferred;  
    primary;  
    vrrp-inet6-group group-id {  
        accept-data | no-accept-data;  
        advertisements-threshold number;  
        authentication-key key;  
        authentication-type authentication;  
        fast-interval milliseconds;  
        inet6-advertise-interval milliseconds;  
        preempt | no-preempt {  
            hold-time seconds;  
        }  
        priority number;  
        track {  
            interface interface-name {  
                priority-cost number;  
            }  
            priority-hold-time seconds;  
            route ip-address/mask routing-instance instance-name priority-cost cost;  
        }  
        virtual-inet6-address [addresses];  
        virtual-link-local-address ipv6-address;  
        vrrp-inherit-from {  
            active-group group-name;  
            active-interface interface-name;  
        }  
    }  
]  
(dad-disable | no-dad-disable);  
filter {  
    input filter-name;  
    output filter-name;  
}  
mtu bytes;  
nd6-stale-time time;  
oo-neighbor-learn;  
no-redirects;  
policer {  
    input policer-name;  
    output policer-name;  
}  
rfp-check {  
    fail-filter filter-name;  
    mode {  
        loose;  
    }  
}
family iso

family iso {
  address interface-address;
  mtu bytes;
}

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-range name unit logical-unit-number]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches, including options ethernet-switching, inet, and iso.
Option inet6 introduced in Junos OS Release 9.3 for EX Series switches.
Options ccc introduced in Junos OS Release 9.5 for EX Series switches.

Description

Configure protocol family information for the logical interface on the switch.

You must configure a logical interface to be able to use the physical device.

Default

Interfaces on EX4300 switches are set to family ethernet-switching by the default factory configuration. Before you can change the family setting for an interface to another family type, you must delete this default setting or any user-configured family setting.
Options  See Table 177 on page 1484 for protocol families available on the switch interfaces. Different protocol families support different subsets of the interface types on the switch.

Interface types on the switch are:

- Aggregated Ethernet (ae0)
- 40-Gigabit Ethernet (et)
- Gigabit Ethernet (ge)
- Interface-range configuration (interface-range)
- Loopback (lo0)
- Management Ethernet (me0)
- Integrated Routing and Bridging (IRB) interfaces (IRB) (irb)
- Virtual management Ethernet (vme)
- 10-Gigabit Ethernet (xe)

If you are using an interface range, the supported protocol families are the ones supported by the interface types that compose the range.

Not all interface types support all family substatements. Check your switch CLI for supported substatements for a particular protocol family configuration.

Table 313: Protocol Families and Supported Interface Types

<table>
<thead>
<tr>
<th>Family</th>
<th>Description</th>
<th>Supported Interface Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccc</td>
<td>Circuit cross-connect protocol family</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>ethernet-switching</td>
<td>Ethernet switching protocol family</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>inet</td>
<td>IPv4 protocol family</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>inet6</td>
<td>IPv6 protocol family</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>iso</td>
<td>Junos OS protocol family for IS-IS traffic</td>
<td>✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

The remaining statements are explained separately.

Required Privilege Level
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.
Related Documentation

- Configuring a DHCP Server on Switches (CLI Procedure) on page 1250
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
filter

Syntax

```plaintext
filter {
  group filter-group-number;
  input filter-name;
  input-list [ filter-names ];
  output filter-name:
  output-list [ filter-names ];
}
```

Hierarchy Level

- [edit interfaces interface-name unit logical-unit-number family family]
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Apply a filter to an interface. You can also use filters for encrypted traffic. When you configure filters, you can configure them under the `family ethernet-switching`, `inet`, `inet6`, `mpls`, or `vpls` only.

Options

- **group filter-group-number**—Define an interface to be part of a filter group.
  - Range: 1 through 255

- **input filter-name**—Name of one filter to evaluate when packets are received on the interface.

- **output filter-name**—Name of one filter to evaluate when packets are transmitted on the interface.

The remaining statements are explained separately.

Required Privilege Level

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

Related Documentation

- Applying a Filter to an Interface
- Junos OS Services Interfaces Library for Routing Devices
- Routing Policy Feature Guide for Routing Devices
- Junos OS Administration Library for Routing Devices
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters and Policers for VPLS
- family on page 1482
- family on page 2419
flow-control

**Syntax**
(flow-control | no-flow-control);

**Hierarchy Level**
[edit interfaces interface-name aggregated-ether-options],
[edit interfaces interface-name ether-options],
[edit interfaces interface-name fastether-options],
[edit interfaces interface-name gigether-options],
[edit interfaces interface-name multiservice-options],
[edit interfaces interface-range name aggregated-ether-options],
[edit interfaces interface-range name ether-options]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 in EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

**Description**
For aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces only, explicitly enable flow control, which regulates the flow of packets from the router or switch to the remote side of the connection. Enabling flow control is useful when the remote device is a Gigabit Ethernet switch. Flow control is not supported on the 4-port Fast Ethernet PIC.

---

**NOTE:** On the Type 5 FPC, to prioritize control packets in case of ingress oversubscription, you must ensure that the neighboring peers support MAC flow control. If the peers do not support MAC flow control, then you must disable flow control.

**Default**
Flow control is enabled.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Flow Control on page 2301
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
### force-up

<table>
<thead>
<tr>
<th>Syntax</th>
<th>force-up;</th>
</tr>
</thead>
</table>

**Hierarchy Level**
- [edit interfaces interface-name ether-options 802.3ad lacp]

**Release Information**
Statement introduced in Junos OS Release 10.0 for EX Series switches.

**Description**
Set the state of the interface as UP when the peer has limited LACP capability.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272
- Junos OS Ethernet Interfaces Configuration Guide

### gratuitous-arp-reply

| Syntax      | (gratuitous-arp-reply | no-gratuitous-arp-reply); |
|-------------|------------------------|

**Hierarchy Level**
- [edit interfaces interface-name]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 in EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

**Description**
For Ethernet interfaces, enable updating of the Address Resolution Protocol (ARP) cache for gratuitous ARPs.

**Default**
Updating of the ARP cache is disabled on all Ethernet interfaces.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Gratuitous ARP on page 2331
- no-gratuitous-arp-request on page 2447
hold-time (Physical Interface)

Syntax

hold-time up milliseconds down milliseconds;

Hierarchy Level

[edit interfaces interface-name],
[edit interfaces interface-range interface-range-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 10.4R5 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

Description

Specify the hold-time value to use to damp interface transitions. When an interface goes from up to down, it is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly, an interface is not advertised as being up until it has remained up for the hold-time period.

NOTE:

• We recommend that you configure the hold-time value after determining an appropriate value by performing repeated tests in the actual hardware environment. This is because the appropriate value for hold-time depends on the hardware (XFP, SFP, SR, ER, or LR) used in the networking environment.

• The hold-time option is not available for controller interfaces.

Default

Interface transitions are not damped.

Options

down milliseconds—Hold time to use when an interface transitions from up to down. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

Range: 0 through 4,294,967,295 milliseconds
Default: 0 milliseconds (interface transitions are not damped)

up milliseconds—Hold time to use when an interface transitions from down to up. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

Range: 0 through 4,294,967,295 milliseconds
Default: 0 milliseconds (interface transitions are not damped)

Required Privilege Level

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation

• advertise-interval
• interfaces (for EX Series switches)
### interface-mode

**Syntax**

```plaintext
interface-mode (access | trunk);
```

**Hierarchy Level**

- `[edit interfaces interface-name unit logical-unit-number family bridge]`
- `[edit interfaces interface-name unit logical-unit-number family ethernet-switching]`
- `[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family bridge]`

**Release Information**

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.

**Description**

(QFX Series 3500 and 3600 standalone switches)—Determine whether the logical interface accepts or discards packets based on VLAN tags. Specify the `trunk` option to accept packets with a VLAN ID that matches the list of VLAN IDs specified in the `vlan-id` or `vlan-id-list` statement, then forward the packet within the bridge domain or VLAN configured with the matching VLAN ID. Specify the `access` option to accept packets with no VLAN ID, then forward the packet within the bridge domain or VLAN configured with the VLAN ID that matches the VLAN ID specified in the `vlan-id` statement.

**NOTE:** On MX Series routers, if you want IGMP snooping to be functional for a bridge domain, then you should not configure `interface-mode` and `irb` for that bridge. Such a configuration commit succeeds, but IGMP snooping is not functional, and a message informing the same is displayed. For more information, see `Configuring a Trunk Interface on a Bridge Network`.

**Options**

- **access**—Configure a logical interface to accept untagged packets. Specify the VLAN to which this interface belongs using the `vlan-id` statement.

- **trunk**—Configure a single logical interface to accept packets tagged with any VLAN ID specified with the `vlan-id` or `vlan-id-list` statement.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring a Logical Interface for Access Mode
- Configuring a Logical Interface for Trunk Mode
- Example: Connecting Access Switches to a Distribution Switch on page 2083
interface-range

Syntax

```
interface-range name {
    accounting-profile name;
    description text;
    disable;
    ether-options {
        802.3ad {
            ae;
            (backup | primary);
            lacp {
                force-up;
            }
        }
        (auto-negotiation | no-auto-negotiation);
        (flow-control | no-flow-control);
        ieee-802-3az-eee;
        link-mode mode;
        (loopback | no-loopback);
        speed (auto-negotiation | speed);
    }
    (gratuitous-arp-reply | no-gratuitous-arp-reply);
    hold-time up milliseconds down milliseconds;
    member interface-name;
    member-range starting-interface name to ending-interface name;
    mtu bytes;
    no-gratuitous-arp-request;
    traceoptions {
        flag flag;
    }
    (traps | no-traps);
    unit logical-unit-number {
        accounting-profile name;
        bandwidth rate;
        description text;
        disable;
        family family-name {...}
        proxy-arp (restricted | unrestricted);
        (traps | no-traps);
        vlan-id (Layer 3 Subinterfaces) vlan-id-number;
    }
    vlan-tagging;
}
```

Hierarchy Level

[edit interfaces]

Release Information

Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description

Group interfaces that share a common configuration profile.

NOTE: You can specify interface ranges only for Gigabit and 10-Gigabit Ethernet interfaces.
## Options

**name**—Name of the interface range.

**NOTE:** You can use regular expressions and wildcards to specify the interfaces in the member configuration. Do not use wildcards for interface types.

The remaining statements are explained separately.

<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>interface-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

### Related Documentation
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Understanding Interface Ranges on EX Series Switches
- Understanding Interface Ranges on EX Series Switches on page 2281
- EX Series Switches Interfaces Overview on page 2267
- Junos OS Interfaces Fundamentals Configuration Guide
**lcap (Aggregated Ethernet)**

**Syntax**
```
lcap {
  (active | passive);
  admin-key key;
  accept-data;
  fast-failover;
  link-protection {
    disable;
    (revertive | non-revertive);
  }
  periodic interval;
  system-id mac-address;
  system-priority priority;
}
```

**Hierarchy Level**
```
[edit interfaces ae
X
aggregated-ether-options]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- `fast-failover` option introduced in Junos OS Release 12.2.

**Description**
For aggregated Ethernet interfaces only, configure the Link Aggregation Control Protocol (LACP).

When you configure the `accept-data` statement at the `[edit interfaces ae
X
aggregated-ether-options lcap]` hierarchy level, the router processes packets received on a member link irrespective of the LACP state if the aggregated Ethernet bundle is up.

**NOTE:** When you use the `accept-data` statement at the `[edit interfaces ae
X
aggregated-ether-options lcap]` hierarchy level, this behavior occurs:

- By default, the `accept-data` statement is not configured when LACP is enabled.
- You can configure the `accept-data` statement to improve convergence and reduce the number of dropped packets when member links in the bundle are enabled or disabled.
- When LACP is down and a member link receives packets, the router does not process packets as defined in the IEEE 802.1ax standard. According to this standard, the packets should be dropped, but they are processed instead because the `accept-data` statement is configured.

**Default**
If you do not specify LACP as either `active` or `passive`, LACP remains passive.

**Options**
- `active`—Initiate transmission of LACP packets.
- `admin-key number`—Specify an administrative key for the router or switch.
NOTE: You must also configure Multichassis Link Aggregation (MC-LAG) when you configure the admin-key.

**fast-failover**—Specify to override the IEEE 802.3ad standard and allow the standby link to receive traffic. Overriding the default behavior facilitates subsecond failover.

**passive**—Respond to LACP packets.

The remaining statements are explained separately.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Aggregated Ethernet LACP
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
**lACP (802.3ad)**

**Syntax**
```
lACP {
  force-up;
  port-priority
}
```

**Hierarchy Level**
```
[edit interfaces interface-name ether-options 802.3ad]
[edit interfaces aeX aggregated-ether-options]
[edit chassis aggregated-devices ethernet]
```

**Release Information**
Statement introduced in Junos OS Release 10.0 for EX Series switches.
Support for LACP link protection introduced in Junos OS Release 11.4 for EX Series switches.

**Description**
Configure the Link Aggregation Control Protocol (LACP) parameters for aggregated Ethernet interfaces on the global level (for all the aggregated Ethernet interfaces on the switch) or for a specific aggregated Ethernet interface.

**Required Privilege Level**
- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

**Related Documentation**
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
- Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272
- Junos OS Ethernet Interfaces Configuration Guide
# link-mode

## Syntax

```
Syntax   link-mode mode;
```

## Hierarchy Level

```
Hierarchy Level  [edit interfaces interface-name],
                 [edit interfaces interface-name ether-options],
                 [edit interfaces ge-pim/0/0 switch-options switch-port port-number]
```

## Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

## Description

Set the device's link connection characteristic.

## Options

- `mode`—Link characteristics:
  - `automatic`—Link mode is negotiated. This is the default for EX Series switches.
  - `full-duplex`—Connection is full duplex.
  - `half-duplex`—Connection is half duplex.

**Default:** Fast Ethernet interfaces, except the J Series ePIM Fast Ethernet interfaces, can operate in either full-duplex or half-duplex mode. The router’s management Ethernet interface, `fxp0` or `em0`, the built-in Fast Ethernet interfaces on the FIC (M7i router), and the Gigabit Ethernet ports on J Series Services Routers with uPIMs installed and configured for access switching mode autonegotiate whether to operate in full-duplex or half-duplex mode. Unless otherwise noted here, all other interfaces operate only in full-duplex mode.

**NOTE:** On J Series ePIM Fast Ethernet interfaces, if you specify half-duplex (or if full-duplex mode is not autonegotiated), the following message is written to the system log: "Half-duplex mode not supported on this PIC, forcing full-duplex mode."

## NOTE:

On EX Series switches, if no-auto-negotiation is specified in `[edit interfaces interface-name ether-options]`, you can select only full-duplex or half-duplex. If auto-negotiation is specified, you can select any mode.

**NOTE:** Member links of an aggregated Ethernet bundle must not be explicitly configured with a link mode. You must remove any such link-mode configuration before committing the aggregated Ethernet configuration.
Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Configuring the Link Characteristics on Ethernet Interfaces
- Understanding Management Ethernet Interfaces
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
**link-protection**

**Syntax**

```
link-protection {
  disable;
  (revertive | non-revertive);
}
```

**Hierarchy Level**

- `[edit interfaces aex aggregated-ether-options]`
- `[edit interfaces aex aggregated-ether-options lACP]`

**Release Information**

- Statement introduced in Junos OS Release 8.3.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for `disable`, `revertive`, and `non-revertive` statements added in Junos OS Release 9.3.

**Description**

On the router, for aggregated Ethernet interfaces only, configure link protection. In addition to enabling link protection, a primary and a secondary (backup) link must be configured to specify what links egress traffic should traverse. To configure primary and secondary links on the router, include the `primary` and `backup` statements at the `[edit interfaces ge-fpc/pic/port gigether-options 802.3ad aex]` hierarchy level or the `[edit interfaces fe-fpc/pic/port fastether-options 802.3ad aex]` hierarchy level.

On the switch, you can configure either Junos OS link protection for aggregated Ethernet interfaces or the LACP standards link protection for aggregated Ethernet interfaces.

For Junos OS link protection, specify `link-protection` at the following hierarchy levels:

- `[edit interfaces ge-fpc/pic/port ether-options 802.3ad aex]`
- `[edit interfaces xe-fpc/pic/port ether-options 802.3ad aex]`

For LACP standards link protection, specify `link-protection` at the following hierarchy levels:

- For global LACP link protection, specify at `[edit chassis aggregated-devices ethernet lACP]`
- For a specific aggregated Ethernet interface, specify at `[edit interfaces aeX aggregated-ether-options lACP]`

**Options**

The statements are explained separately.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- **Configuring Aggregated Ethernet Link Protection on page 2342**
- **Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340**
link-speed (Aggregated Ethernet)

Syntax

```
link-speed speed;
```

Hierarchy Level

```
[edit interfaces aex aggregated-ether-options],
[edit interfaces interface-range name aggregated-ether-options],
[edit interfaces interface-range name aggregated-sonet-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

For aggregated Ethernet interfaces only, set the required link speed.

Options

`speed`—For aggregated Ethernet links, you can specify `speed` in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation `k` (1000), `m` (1,000,000), or `g` (1,000,000,000).

Aggregated Ethernet links on the M120 router can have one of the following speeds:

- `100m`—Links are 100 Mbps.
- `10g`—Links are 10 Gbps.
- `1g`—Links are 1 Gbps.
- `oc192`—Links are OC192 or STM64c.

Aggregated Ethernet links on EX Series switches can be configured to operate at one of the following speeds:

- `10m`—Links are 10 Mbps.
- `100m`—Links are 100 Mbps.
- `1g`—Links are 1 Gbps.
- `10g`—Links are 10 Gbps.

Aggregated Ethernet links on T Series routers can be configured to operate at one of the following speeds:

- `100g`—Links are 100 Gbps.
- `100m`—Links are 100 Mbps.
- `10g`—Links are 10 Gbps.
- `1g`—Links are 1 Gbps.
- `40g`—Links are 40 Gbps.
- `50g`—Links are 50 Gbps.
- `80g`—Links are 80 Gbps.
- `8g`—Links are 8 Gbps.
• **mixed**—Links are of various speeds.
• **oc192**—Links are OC192.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>interface-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- *Aggregated Ethernet Interfaces Overview*
- Configuring Aggregated Ethernet Link Speed on page 2343
- *Configuring Mixed Aggregated Ethernet Links*
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch

---

**loopback (Aggregated Ethernet, Fast Ethernet, and Gigabit Ethernet)**

**Syntax**

(loopback | no-loopback);

**Hierarchy Level**

- [edit interfaces interface-name aggregated-ether-options],
- [edit interfaces interface-name ether-options],
- [edit interfaces interface-name fastether-options],
- [edit interfaces interface-name gigether-options],
- [edit interfaces interface-range name ether-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

**Description**

For aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, enable or disable loopback mode.

---

**NOTE:** By default, local aggregated Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces connect to a remote system.

---

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>interface-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Configuring Ethernet Loopback Capability on page 2330
### member (Interface Ranges)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>member interface-name;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit interfaces interface-range interface-range-name]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 10.0 for EX Series switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify the name of the member interface belonging to an interface range on the EX Series switch.</td>
</tr>
<tr>
<td>Options</td>
<td>interface-name—Name of the interface.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
| Related Documentation | - Configuring Gigabit Ethernet Interfaces (CLI Procedure)  
                          - Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286  
                          - Understanding Interface Ranges on EX Series Switches  
                          - Understanding Interface Ranges on EX Series Switches on page 2281  
                          - EX Series Switches Interfaces Overview on page 2267  
                          - Junos OS Interfaces Fundamentals Configuration Guide |
**member-range**

**Syntax**  
`member-range starting-interface-name to ending-interface-name;`

**Hierarchy Level**  
[edit interfaces interface-range interface-range-name]

**Release Information**  
Statement introduced in Junos OS Release 10.0 for EX Series switches.

**Description**  
Specify the names of the first and last members of a sequence of interfaces belonging to an interface range.

**Options**  
**Range:** `Starting interface-name to ending interface-name`—The name of the first member and the name of the last member in the interface sequence.

**Required Privilege**  
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**  
- [Configuring Gigabit Ethernet Interfaces (CLI Procedure)](#)
- [Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286](#)
- [Understanding Interface Ranges on EX Series Switches](#)
- [Understanding Interface Ranges on EX Series Switches on page 2281](#)
- [EX Series Switches Interfaces Overview on page 2267](#)
- [Junos OS Interfaces Fundamentals Configuration Guide](#)
members

Syntax:  
members [{all | names | vlan-ids}];

Hierarchy Level:  
[edit interfaces interface-name unit logical-unit-number family ethernet-switching vlan (802.1Q Tagging)]

Release Information:  
Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement updated with enhanced \( ? \) (CLI completion feature) functionality in Junos OS Release 9.5 for EX Series switches.

Description:  
For trunk interfaces, configure the VLANs that can carry traffic.

TIP:  
To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type \( ? \) after vlan or vlans in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

NOTE:  
The number of VLANs supported per switch varies for each model. Use the configuration-mode command set vlans id vlan-id ? to determine the maximum number of VLANs allowed on a switch. You cannot exceed this VLAN limit because each VLAN is assigned an ID number when it is created. You can, however, exceed the recommended VLAN member maximum.

On an EX Series switch that runs Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style, the maximum number of VLAN members allowed on the switch is 8 times the maximum number of VLANs the switch supports \((v_{member\ limit} = vlan\ max \times 8)\). If the switch configuration exceeds the recommended VLAN member maximum, you see a warning message when you commit the configuration. If you ignore the warning and commit such a configuration, the configuration succeeds but you run the risk of crashing the Ethernet switching process \((eswd)\) due to memory allocation failure.

On an EX Series switch that runs Junos OS that supports ELS, the maximum number of VLAN members allowed on the switch is 24 times the maximum number of VLANs the switch supports \((v_{member\ limit} = vlan\ max \times 24)\). If the configuration of one of these switches exceeds the recommended VLAN member maximum, a warning message appears in the system log \((syslog)\).

Options:  
all—Specifies that this trunk interface is a member of all the VLANs that are configured on this switch. When a new VLAN is configured on the switch, this trunk interface automatically becomes a member of the VLAN.
NOTE: Since VLAN members are limited, specifying all could cause the number of VLAN members to exceed the limit at some point.

*names*—Name of one or more VLANs. VLAN IDs are applied automatically in this case.

NOTE: *all* cannot be a VLAN name.

*vlan-ids*—Numeric identifier of one or more VLANs. For a series of tagged VLANs, specify a range; for example, 10–20 or 10–20 23–30.

NOTE: Each configured VLAN must have a specified VLAN ID to successfully commit the configuration; otherwise, the configuration commit fails.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- show ethernet-switching interfaces
- show ethernet-switching interface on page 2183
- show vlans
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch
- Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch on page 2073
- Example: Connecting an Access Switch to a Distribution Switch
- Example: Connecting Access Switches to a Distribution Switch on page 2083
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
- Configuring VLANs for EX Series Switches (CLI Procedure)
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
- Creating a Series of Tagged VLANs (CLI Procedure)
- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Junos OS Ethernet Interfaces Configuration Guide
### mtu

**Syntax**

```
mtu bytes;
```

**Hierarchy Level**

- [edit interfaces interface-name],
- [edit interfaces interface-name unit logical-unit-number family family],
- [edit interfaces interface-range name],
- [edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family],
- [edit logical-systems logical-system-name protocols l2circuit local-switching interface interface-name backup-neighbor address],
- [edit logical-systems logical-system-name protocols l2circuit neighbor address interface interface-name],
- [edit logical-systems logical-system-name protocols l2circuit neighbor address interface interface-name backup-neighbor address],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols l2vpn interface interface-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols vpls],
- [edit protocols l2circuit local-switching interface interface-name backup-neighbor address],
- [edit protocols l2circuit neighbor address interface interface-name]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for Layer 2 VPNs and VPLS introduced in Junos OS Release 10.4.
- Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
- Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
- Support at the [set interfaces interface-name unit logical-unit-number family ccc] hierarchy level introduced in Junos OS Release 12.3R3 for MX Series routers.

**Description**

Specify the maximum transmission unit (MTU) size for the media or protocol. The default MTU size depends on the device type. Changing the media MTU or protocol MTU causes an interface to be deleted and added again.

To route jumbo data packets on an integrated routing and bridging (irb) interface or routed VLAN interface (RVI) on EX Series switches, you must configure the jumbo MTU size on the member physical interfaces and also on the IRB interface or RVI itself (the irb or vlan interface, respectively).

---

**CAUTION:** For EX Series switches, setting or deleting the jumbo MTU size on an IRB interface or RVI while the switch is transmitting packets might cause packets to be dropped.
NOTE: If a packet whose size is larger than the configured MTU size is received on the receiving interface, the packet is eventually dropped. The value considered for MRU (maximum receive unit) size is also the same as the MTU size configured on that interface.

NOTE: Not all devices allow you to set an MTU value, and some devices have restrictions on the range of allowable MTU values. You cannot configure an MTU for management Ethernet interfaces (fxf0, em0, or me0) or for loopback, multilink, and multicast tunnel devices.

For more information about configuring MTU for specific interfaces and router or switch combinations, see “Configuring the Media MTU” on page 2307.

Options

<table>
<thead>
<tr>
<th>bytes</th>
<th>MTU size.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range:</td>
<td>256 through 9192 bytes, 256 through 9500 bytes (Junos OS 12.1X48R2 for PTX Series routers)</td>
</tr>
<tr>
<td>Default:</td>
<td>1500 bytes (INET, INET6, and ISO families), 1448 bytes (MPLS), 1514 bytes (EX Series switch interfaces)</td>
</tr>
</tbody>
</table>

Required Privilege Level

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Routed VLAN Interfaces (CLI Procedure)
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
- Configuring the Media MTU on page 2307
- Configuring the MTU for Layer 2 Interfaces
- Setting the Protocol MTU on page 2318
native-vlan-id

**Syntax**

native-vlan-id number;

**Hierarchy Level**

[edit interfaces ge-fpc/pic/port],
[edit interfaces interface-name]

**Release Information**

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

**Description**

For 1-, 4-, and 8-port Gigabit Ethernet IQ2 and IQ2-E PICs, for 1-port 10-Gigabit Ethernet
IQ2 and IQ2-E PICs configured for 802.1Q flexible VLAN tagging, for all Ethernet interfaces
on MX Series routers, and for aggregated Ethernet interfaces on IQ2 and IQ2-E PICs or
MX Series DPCs, and for 100-Gigabit Ethernet Type 5 PIC with CFP, configure mixed
tagging support for untagged packets on a port. When the `native-vlan-id` statement is
included with the `flexible-vlan-tagging` statement, untagged packets are accepted on
the same mixed VLAN-tagged port.

---

**NOTE:** Mixed VLAN tagging is not supported on EX Series switches.

---

The logical interface on which untagged packets are received must be configured with
the same VLAN ID as the native VLAN ID configured on the physical interface. To configure
the logical interface, include the `vlan-id` statement (matching the `native-vlan-id` statement
on the physical interface) at the `[edit interfaces interface-name unit logical-unit-number]`
hierarchy level.

When the `native-vlan-id` statement is included with the `interface-mode` statement,
untagged packets are accepted and forwarded within the bridge domain or VLAN that
is configured with the matching VLAN ID.

**Options**

- `number`—VLAN ID number.
  
  **Range:** (ACX Series routers and EX Series switches) 0 through 4094.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring Mixed Tagging Support for Untagged Packets
- Configuring a Logical Interface for Access Mode
- Configuring the Native VLAN Identifier (CLI Procedure) on page 2124
- Understanding Bridging and VLANs on EX Series Switches on page 2049
- `flexible-vlan-tagging`
no-gratuitous-arp-request

Syntax  
no-gratuitous-arp-request;

Hierarchy Level  
[edit interfaces interface-name]

Release Information  
Statement introduced in Junos OS Release 9.6 for EX Series switches.  
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

Description  
For Ethernet interfaces and pseudowire logical interfaces, do not respond to gratuitous ARP requests.

Default  
Gratuitous ARP responses are enabled on all Ethernet interfaces.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  
• Configuring Gratuitous ARP on page 2331  
• gratuitous-arp-reply on page 2427

no-redirects

Syntax  
no-redirects;

Hierarchy Level  
[edit interfaces interface-name unit logical-unit-number family family]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Do not send protocol redirect messages on the interface.

To disable the sending of protocol redirect messages for the entire router or switch, include the no-redirects statement at the [edit system] hierarchy level.

Default  
Interfaces send protocol redirect messages.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  
• Disabling the Transmission of Redirect Messages on an Interface on page 2333  
• Junos OS Administration Library for Routing Devices
**periodic**

**Syntax**

```plaintext
periodic interval;
```

**Hierarchy Level**

```
[edit interfaces aex aggregated-ether-options lACP],
[edit interfaces interface-range name aggregated-ether-options lACP]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

For aggregated Ethernet interfaces only, configure the interval for periodic transmission of LACP packets.

**Options**

`interval`—Interval for periodic transmission of LACP packets.

- `fast`—Transmit packets every second.
- `slow`—Transmit packets every 30 seconds.

Default: fast

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring Aggregated Ethernet LACP
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
preferred

Syntax

preferred;

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number family family address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure this address to be the preferred address on the interface. If you configure more than one address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet.

NOTE: The edit logical-systems hierarchy is not available on QFabric systems.

Default

The lowest-numbered address on the subnet is the preferred address.

Required Privilege

interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation

• Configuring the Interface Address on page 2302
primary (Address on Interface)

Syntax primary;

Hierarchy Level [edit interfaces interface-name unit logical-unit-number family family address address],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family family address address]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure this address to be the primary address of the protocol on the interface. If the logical unit has more than one address, the primary address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.

NOTE: The edit logical-systems hierarchy is not available on QFabric systems.

Default For unicast traffic, the primary address is the lowest non-127 (in other words, non-loopback) preferred address on the unit.

Required Privilege Level interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation • Configuring the Interface Address on page 2302
proxy-arp

Syntax

proxy-arp (restricted | unrestricted);

Hierarchy Level

[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.6 for EX Series switches.
restricted added in Junos OS Release 10.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for the QFX Series.

Description

For Ethernet interfaces only, configure the router or switch to respond to any ARP request, as long as the router or switch has an active route to the ARP request’s target address.

NOTE: You must configure the IP address and the inet family for the interface when you enable proxy ARP.

Default

Proxy ARP is not enabled. The router or switch responds to an ARP request only if the destination IP address is its own.

Options

- none—The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address.
- restricted—(Optional) The router or switch responds to ARP requests in which the physical networks of the source and target are different and does not respond if the source and target IP addresses are in the same subnet. The router or switch must also have a route to the target IP address.
- unrestricted—(Optional) The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address.

Default: unrestricted

Required Privilege

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Restricted and Unrestricted Proxy ARP on page 2333
- Configuring Proxy ARP (CLI Procedure)
- Configuring Proxy ARP (CLI Procedure) on page 2130
- Example: Configuring Proxy ARP on an EX Series Switch on page 2113
- Configuring Gratuitous ARP on page 2331
**rpf-check**

**Syntax**
```plaintext
rpf-check;
```

**Hierarchy Level**
```plaintext
[edit interfaces interface-name unit logical-unit-number family inet],
[edit interfaces interface-name unit logical-unit-number family inet6]
```

**Release Information**
Statement introduced in Junos OS Release 9.3 for EX Series switches.

**Description**
On EX3200 and EX4200 switches, enable a reverse-path forwarding (RPF) check on unicast traffic (except ECMP packets) on all ingress interfaces.

On EX8200 switches, enable an RPF check on unicast traffic, including ECMP packets, on the selected ingress interface.

**Default**
Unicast RPF is disabled on all interfaces.

**Required Privilege Level**
- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring Unicast RPF on an EX Series Switch*
  - Configuring Unicast RPF (CLI Procedure) on page 2347
  - Disabling Unicast RPF (CLI Procedure) on page 2348
  - Understanding Unicast RPF for EX Series Switches on page 2276
speed (Ethernet)

**Syntax**

```
speed (10m | 100m | 1g | auto | auto-10m-100m);
```

**Hierarchy Level**

```
[edit interfaces interface-name],
[edit interfaces ge-pim/0/0 switch-options switch-port port-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Configure the interface speed. This statement applies to the management Ethernet interface (`fxp0` or `em0`), Fast Ethernet 12-port and 48-port PICs, the built-in Fast Ethernet port on the FIC (M7i router), the built-in Ethernet interfaces on J Series Services Routers, Combo Line Rate DPCs and Tri-Rate Ethernet Copper interfaces on MX Series routers, Gigabit Ethernet ports on J Series Services Routers with uPIMs installed and configured for access switching mode, and Gigabit Ethernet interfaces on EX Series switches.

When you configure the Tri-Rate Ethernet copper interface to operate at 1 Gbps, autonegotiation must be enabled. When you configure 100BASE-FX SFP, you must set the port speed at 100 Mbps.

**Options**

You can specify the speed as either `10m` (10 Mbps), `100m` (100 Mbps), or on J Series routers with uPIMs installed and on MX Series routers, `1g` (1 Gbps). You can also specify the `auto` option on MX Series routers.

For Gigabit Ethernet interfaces on EX Series switches, you can specify one of the following options:

- `10m`—10 Mbps
- `100m`—100 Mbps
- `1g`—1 Gbps
- `auto`—Automatically negotiate the speed (10 Mbps, 100 Mbps, or 1 Gbps) based on the speed of the other end of the link.
- `auto-10m-100m`—Automatically negotiate the speed (10 Mbps or 100 Mbps) based on the speed of the other end of the link.

**Required Privilege Level**

- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring the Interface Speed
- Configuring the Interface Speed on Ethernet Interfaces
- Configuring Gigabit Ethernet Autonegotiation
- Configuring J Series Services Router Switching Interfaces
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
traceoptions (Individual Interfaces)

Syntax

traceoptions {
  file name <files name> <size size> <world-readable | no-world-readable>;
  flag flag;
  match;
}

Hierarchy Level

[edit interfaces interface-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

Description

Define tracing operations for individual interfaces.

To specify more than one tracing operation, include multiple flag statements.

The interfaces traceoptions statement does not support a trace file. The logging is done by the kernel, so the tracing information is placed in the system syslog file in the directory /var/log.

Default

If you do not include this statement, no interface-specific tracing operations are performed.

Options

- **file name**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. By default, interface process tracing output is placed in the file filesnumber.

- **files name**—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

- **match**—(Optional) Regular expression for lines to be traced.

- **no-world-readable**—(Optional) Prevent any user from reading the log file.

- **world-readable**—(Optional) Allow any user to read the log file.

- **flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. The following are the interface-specific tracing options.

  - **all**—All interface tracing operations
  - **event**—Interface events
- **ipc**—Interface interprocess communication (IPC) messages
- **media**—Interface media changes
- **q921**—Trace ISDN Q.921 frames
- **q931**—Trace ISDN Q.931 frames

**Required Privilege**
- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**
- *Tracing Operations of an Individual Router Interface*
traceoptions (Interface Process)

Syntax

```plaintext
traceoptions {
  file <filename> <files number> <match regular-expression> <size size> <world-readable |
  no-world-readable>;
  flag flag <disable>;
  no-remote-trace;
}
```

Hierarchy Level
[edit interfaces]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Define tracing operations for the interface process (dcd).

Default
If you do not include this statement, no interface-specific tracing operations are performed.

Options

- **disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

- **filename**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. By default, interface process tracing output is placed in the file `dcd`.

- **files number**—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

  **Range:** 2 through 1000

  **Default:** 3 files

- **flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

  - **all**
  - **change-events**—Log changes that produce configuration events
  - **config-states**—Log the configuration state machine changes
  - **kernel**—Log configuration IPC messages to kernel
  - **kernel-detail**—Log details of configuration messages to kernel
  - **no-world-readable**—(Optional) Disallow any user to read the log file.
size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When the `trace-file` again reaches its maximum size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option.

Syntax: `xk` to specify kilobytes, `xm` to specify megabytes, or `xg` to specify gigabytes

Range: 10 KB through the maximum file size supported on your router

Default: 1 MB

world-readable—(Optional) Allow any user to read the log file.

match regex—(Optional) Refine the output to include only those lines that match the given regular expression.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation
• Tracing Operations of the Interface Process

traps

Syntax (traps | no-traps);

Hierarchy Level
[edit interfaces interface-name],
[edit interfaces interface-name unit logical-unit-number],
[edit interfaces interface-range name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.

Description
Enable or disable the sending of Simple Network Management Protocol (SNMP) notifications when the state of the connection changes.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation
• Enabling or Disabling SNMP Notifications on Physical Interfaces
• Enabling or Disabling SNMP Notifications on Logical Interfaces on page 2334
unit

Syntax

unit logical-unit-number {
  accounting-profile name;
  bandwidth rate;
  description text;
  disable;
  family family-name {...}
  proxy-arp (restricted | unrestricted);
  (traps | no-traps);
  vlan-id (Layer 3 Subinterfaces) vlan-id-number;
}

Hierarchy Level

[edit interfaces interface-name],
[edit interfaces interface-range name]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure a logical interface on the physical device. You must configure a logical interface
to be able to use the physical device.

Options

logical-unit-number—Number of the logical unit.

Range: 0 through 16,384

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- EX Series Switches Interfaces Overview on page 2267
- Junos OS Ethernet Interfaces Configuration Guide
**vlan (802.1Q Tagging)**

**Syntax**

```
vlan {
  members [(all | names | vlan-ids)];
}
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number family ethernet-switching]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Bind an 802.1Q VLAN tag ID to a logical interface.

The remaining statement is explained separately.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- `show ethernet-switching interfaces`
- `show ethernet-switching interface` on page 2183
- *Example: Setting Up Bridging with Multiple VLANs for EX Series Switches*
- *Configuring Routed VLAN Interfaces (CLI Procedure)*
- Configuring Integrated Routing and Bridging Interfaces (CLI Procedure) on page 2122
- Understanding Bridging and VLANS on EX Series Switches on page 2049
- *Junos OS Ethernet Interfaces Configuration Guide*
**vlan-id (Layer 3 Subinterfaces)**

**Syntax**

```
vlan-id vlan-id-number;
```

**Hierarchy Level**

```
[edit interfaces interface-name unit logical-unit-number]
```

**Release Information**

Statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Bind an 802.1Q VLAN tag ID to a logical interface.

**NOTE:** The VLAN tag ID cannot be configured on logical interface unit 0. The logical unit number must be 1 or higher.

**Options**

- **vlan-id-number**—A valid VLAN identifier.
  
  **Range:** 1 through 4094

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- `vlan-tagging on page 2461`
- `Example: Configuring Layer 3 Subinterfaces for a Distribution Switch and an Access Switch`
  
  - `Configuring Gigabit Ethernet Interfaces (CLI Procedure)`
  - `Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286`
  - `Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289`
  - `Configuring a Layer 3 Subinterface (CLI Procedure) on page 2346`
  - `Junos OS Ethernet Interfaces Configuration Guide`
vlan-tagging

Syntax  

```sh
vlan-tagging;
```

Hierarchy Level  

- [edit interfaces interface-name],
- [edit logical-systems logical-system-name interfaces interface-name]

Release Information  

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
- Statement introduced in Junos OS Release 13.2 for PTX Series Routers.

Description  

For Fast Ethernet and Gigabit Ethernet interfaces, aggregated Ethernet interfaces configured for VPLS, and pseudowire subscriber interfaces, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface.

Required Privilege Level  

- interface—to view this statement in the configuration.
- interface-control—to add this statement to the configuration.

Related Documentation  

- Example: Configuring Layer 3 Subinterfaces for a Distribution Switch and an Access Switch
- Example: Configuring BGP Autodiscovery for LDP VPLS
- Configuring a Layer 3 Subinterface (CLI Procedure) on page 2346
- Configuring Tagged Aggregated Ethernet Interfaces on page 2346
- Configuring Interfaces for VPLS Routing
- Enabling VLAN Tagging
- 802.1Q VLANs Overview on page 2283
- vlan-id on page 2460
CHAPTER 46

Administration

- Routine Monitoring on page 2463
- Operational Commands on page 2470

Routine Monitoring

- Monitoring Interface Status and Traffic on page 2463
- Verifying the Status of a LAG Interface on page 2465
- Verifying That LACP Is Configured Correctly and Bundle Members Are Exchanging LACP Protocol Packets on page 2465
- Verifying That Layer 3 Subinterfaces Are Working on page 2466
- Verifying Unicast RPF Status on page 2467
- Verifying IP Directed Broadcast Status on page 2469

Monitoring Interface Status and Traffic

**Purpose**

Use the monitoring functionality to view interface status or to monitor interface bandwidth utilization and traffic statistics on the EX Series switches.

The J-Web interface monitors interface bandwidth utilization and plots real-time charts to display input and output rates in bytes per second. In addition, the Interface monitoring page displays input and output packet counters and error counters in the form of charts.

Alternatively, you can enter the `show` commands in the CLI to view interface status and traffic statistics.

---

**NOTE:** For logical interfaces on EX Series switches, the traffic statistics fields in `show interfaces` commands show only control traffic; the traffic statistics do not include data traffic.

---

**NOTE:** EX Series switches do not support the collection and reporting of IPv6 transit statistics. Therefore, the IPv6 transit statistics field in the `show interfaces` commands displays all values as 0.
**Action**  
To view general interface information in the J-Web interface such as available interfaces, select **Monitor > Interfaces**. Click any interface to view details about its status.

To set up interface monitoring for Virtual Chassis and EX8200 switches, select a member from the **Port for Member** list. Details such as the admin status and link status are displayed in the table. For an EX8200 Virtual Chassis setup, select the member, **FPC**, and the required interface.

---

**NOTE:** By default, the details of the first member in the **FPC** list is displayed. In an EX8200 Virtual Chassis setup, details of the first member and the first **FPC** is displayed.

You have the following options:

- **Start/Stop**—Starts or stops monitoring the selected interface.
- **Show Graph**—Displays input and output packet counters and error counters in the form of charts. Click the pop-up icon to view the graph in a separate window.
- **Details**—Displays interface information such as general details, traffic statistics, I/O errors, CoS counters, and Ethernet statistics.
- **Refresh Interval (sec)**—Displays the time interval you have set for page refresh.
- **Clear Statistics**—Clears the statistics for the interface selected from the table.

**Using the CLI:**

- To view interface status for all the interfaces, enter `show interfaces xe-`.
- To view status and statistics for a specific interface, enter `show interfaces xe-interface-name`.
- To view status and traffic statistics for all interfaces, enter either `show interfaces xe-detail` or `show interfaces xe-extensive`.

**Meaning**  
In the J-Web interface the charts displayed are:

- **Bar charts**—Display the input and output error counters.
- **Pie charts**—Display the number of broadcast, unicast, and multicast packet counters.

For details about output from the CLI commands, see `show interfaces ge-` (Gigabit Ethernet) or `show interfaces xe-` (10-Gigabit Ethernet).

**Related Documentation**

- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure) on page 2286
Verifying the Status of a LAG Interface

**Purpose**
Verify that a LAG (ae0) has been created on the switch.

**Action**
Enter the following command:

```
user@switch> show interfaces ae0 terse
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
<th>Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ae0.0</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td>10.10.10.2/24</td>
<td></td>
</tr>
</tbody>
</table>

**Meaning**
The output confirms that the ae0 link is up and shows the family and IP address assigned to this link.

**Related Documentation**
- Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
- Configuring Aggregated Ethernet Interfaces (J-Web Procedure) on page 2336
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch

Verifying That LACP Is Configured Correctly and Bundle Members Are Exchanging LACP Protocol Packets

Verify that LACP has been set up correctly and that the bundle members are transmitting LACP protocol packets.

1. Verifying the LACP Setup on page 2465
2. Verifying That LACP Packets Are Being Exchanged on page 2466

**Verifying the LACP Setup**

**Purpose**
Verify that the LACP has been set up correctly.

**Action**
To verify that LACP has been enabled as active on one end:

```
user@switch> show lacp interfaces xe-0/1/0
```

<table>
<thead>
<tr>
<th>Aggregated interface: ae0</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACP state:</td>
</tr>
<tr>
<td>Role</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>xe-0/1/0</td>
</tr>
<tr>
<td>xe-0/1/0</td>
</tr>
<tr>
<td>LACP protocol:</td>
</tr>
<tr>
<td>Receive State</td>
</tr>
<tr>
<td>xe-0/1/0</td>
</tr>
</tbody>
</table>
Meaning This output shows that LACP has been configured with one side as active and the other as passive. When LACP is enabled, at least one side must be set as active for the bundled link to be up.

**Verifying That LACP Packets Are Being Exchanged**

**Purpose** Verify that LACP packets are being exchanged between interfaces.

**Action** Use the `show interfaces ae0 statistics` command to display LACP BPDU exchange information.

```
show interfaces ae0 statistics
Physical interface: ae0, Enabled, Physical link is Down
Interface index: 153, SNMP ifIndex: 30
Link-level type: Ethernet, MTU: 1514, Speed: Unspecified, Loopback: Disabled,
Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1,
Minimum bandwidth needed: 0
Device flags : Present Running
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Current address: 02:19:e2:50:45:e0, Hardware address: 02:19:e2:50:45:e0
Last flapped : Never
Statistics last cleared: Never
  Input packets : 0
  Output packets: 0
  Input errors: 0, Output errors: 0

Logical interface ae0.0 (Index 71) (SNMP ifIndex 34)
  Flags: Hardware-Down Device-Down SNMP-Traps Encapsulation: ENET2
  Statistics Packets pps Bytes bps
  Bundle: 
    Input : 0 0 0 0
    Output: 0 0 0 0
  Protocol inet,
  Flags: None
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 10.10.10/24, Local: 10.10.10.1, Broadcast: 10.10.10.255
```

**Meaning** The output here shows that the link is down and that no PDUs are being exchanged (when there is no other traffic flowing on the link).

**Related Documentation**
- Configuring Aggregated Ethernet LACP
- Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
- Verifying the Status of a LAG Interface
- Verifying the Status of a LAG Interface on page 2465

**Verifying That Layer 3 Subinterfaces Are Working**

**Purpose** After configuring Layer 3 subinterfaces, verify they are set up properly and transmitting data.
1. Use the `show interfaces` command to determine whether you successfully created the subinterfaces and the links are up:

```
user@switch> show interfaces interface-name terse
Interface Admin Link Proto Local    Remote
ge-0/0/0    up    up
ge-0/0/0.0  up    up    inet     1.1.1.1/24
ge-0/0/0.1  up    up    inet     2.1.1.1/24
ge-0/0/0.2  up    up    inet     3.1.1.1/24
ge-0/0/0.3  up    up    inet     4.1.1.1/24
ge-0/0/0.4  up    up    inet     5.1.1.1/24
ge-0/0/0.32767 up    up
```

2. Use the `ping` command from a device on one subnet to an address on another subnet to determine whether packets were transmitted correctly on the subinterface VLANs:

```
user@switch> ping ip-address
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: icmp_seq=0 ttl=64 time=0.157 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=0.238 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=0.255 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.128 ms
--- 1.1.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
```

**Meaning**
The output confirms that the subinterfaces are created and the links are up.

**Related Documentation**
- Configuring a Layer 3 Subinterface (CLI Procedure) on page 2346
- Example: Configuring Layer 3 Subinterfaces for a Distribution Switch and an Access Switch

### Verifying Unicast RPF Status

**Purpose**
Verify that unicast reverse-path forwarding (RPF) is enabled and is working on the interface.

**Action**
Use one of the `show interfaces interface-name` commands with either the `extensive` or `detail` options to verify that unicast RPF is enabled and working on the switch. The following example displays output from the `show interfaces ge-1/0/10 extensive` command.

```
user@switch> show interfaces ge-1/0/10 extensive
Physical interface: ge-1/0/10, Enabled, Physical link is Down
Interface index: 139, SNMP ifIndex: 58, Generation: 140
Link-level type: Ethernet, MTU: 1514, Speed: Auto, MAC-REWRITE Error: None,
Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,
Auto-negotiation: Enabled, Remote fault: Online
Device flags   : Present Running
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags     : None
CoS queues     : 8 supported, 8 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:19:e2:50:95:ab, Hardware address: 00:19:e2:50:95:ab
Last flapped   : Never
Statistics last cleared: Never
Traffic statistics:
   Input bytes : 0  0 bps
```
Output bytes : 0
Input packets: 0
Output packets: 0
IPv6 transit statistics:
Input bytes :
0
Output bytes :
0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:
0 best-effort 0
1 assured-forw 0
5 expedited-fo 0
7 network-cont 0
Active alarms : LINK
Active defects : LINK
MAC statistics:
Receive Transmit
Total octets 0 0
Total packets 0 0
Unicast packets 0 0
Broadcast packets 0 0
Multicast packets 0 0
CRC/Align errors 0 0
FIFO errors 0 0
MAC control frames 0 0
MAC pause frames 0 0
Oversized frames 0
Jabber frames 0
Fragment frames 0
VLAN tagged frames 0
Code violations 0
Filter statistics:
Input packet count 0
Input packet rejects 0
Input DA rejects 0
Input SA rejects 0
Output packet count 0
Output packet pad count 0
Output packet error count 0
CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
  Negotiation status: Incomplete
Packet Forwarding Engine configuration:
  Destination slot: 1

Logical interface ge-1/0/10.0 (Index 69) (SNMP ifIndex 59) (Generation 135)
Flags: Device-Down SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
Meaning  The `show interfaces ge-1/0/10 extensive` command (and the `show interfaces ge-1/0/10 detail` command) displays in-depth information about the interface. The Flags: output field near the bottom of the display reports the unicast RPF status. If unicast RPF has not been enabled, the `uRPF` flag is not displayed.

On EX3200, EX4200, and EX4300 switches, unicast RPF is implicitly enabled on all switch interfaces, including aggregated Ethernet interfaces (also referred to as link aggregation groups or LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVis) when you enable unicast RPF on a single interface. However, the unicast RPF status is shown as enabled only on interfaces for which you have explicitly configured unicast RPF. Thus, the `uRPF` flag is not displayed on interfaces for which you have not explicitly configured unicast RPF even though unicast RPF is implicitly enabled on all interfaces on EX3200 and EX4200 switches.

Related Documentation
- show interfaces xe- on page 2524
- Example: Configuring Unicast RPF on an EX Series Switch
- Configuring Unicast RPF (CLI Procedure) on page 2347
- Disabling Unicast RPF (CLI Procedure) on page 2348
- Troubleshooting Unicast RPF on page 2547

Verifying IP Directed Broadcast Status

Purpose  Verify that IP directed broadcast is enabled and is working on the subnet.
Action  Use the `show vlans extensive` command to verify that IP directed broadcast is enabled and working on the subnet as shown in Example: Configuring IP Directed Broadcast on an EX Series Switch.

Related 
Documentation  
- Configuring IP Directed Broadcast (CLI Procedure)  
- Configuring IP Directed Broadcast (CLI Procedure) on page 2349  
- Example: Configuring IP Directed Broadcast on an EX Series Switch

Operational Commands
monitor interface

Syntax

monitor interface

<interface-name | traffic <detail>>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display real-time statistics about interfaces, updating the statistics every second. Check for and display common interface failures, such as SONET/SDH and T3 alarms, loopbacks detected, and increases in framing errors.

NOTE: This command is not supported on the QFX3000 QFabric system.

Options
none—Display real-time statistics for all interfaces.

detail—(Optional) With traffic option only, display detailed output.

interface-name—(Optional) Display real-time statistics for the specified interface. In a TX Matrix or TX Matrix Plus router, display real-time statistics for the physical interfaces on the specified line-card chassis (LCC) only.

traffic—(Optional) Display traffic data for all active interfaces. In a TX Matrix or TX Matrix Plus router, display real-time statistics for the physical interfaces on the specified LCC only.

Additional Information
The output of this command shows how much each field has changed since you started the command or since you cleared the counters by pressing the c key. For a description of the statistical information provided in the output of this command, see the show interfaces extensive command for a particular interface type in the Junos OS Operational Mode Commands. To control the output of the monitor interface command while it is running, use the keys listed in Table 314 on page 2471. The keys are not case-sensitive.

Table 314: Output Control Keys for the monitor interface Command

<table>
<thead>
<tr>
<th>Key</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Clears (returns to zero) the delta counters since monitor interface was started. This does not clear the accumulative counter. To clear the accumulative counter, use the clear interfaces interval command.</td>
</tr>
<tr>
<td>f</td>
<td>Freezes the display, halting the display of updated statistics and delta counters.</td>
</tr>
<tr>
<td>i</td>
<td>Displays information about a different interface. The command prompts you for the name of a specific interface.</td>
</tr>
</tbody>
</table>
Table 314: Output Control Keys for the monitor interface Command (continued)

<table>
<thead>
<tr>
<th>Key</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>Displays information about the next interface. The <code>monitor interface</code> command displays the physical or logical interfaces in the same order as the <code>show interfaces terse</code> command.</td>
</tr>
<tr>
<td>q or Esc</td>
<td>Quits the command and returns to the command prompt.</td>
</tr>
<tr>
<td>t</td>
<td>Thaws the display, resuming the update of the statistics and delta counters.</td>
</tr>
</tbody>
</table>

To control the output of the `monitor interface traffic` command while it is running, use the keys listed in Table 315 on page 2472. The keys are not case-sensitive.

Table 315: Output Control Keys for the monitor interface traffic Command

<table>
<thead>
<tr>
<th>Key</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>b</td>
<td>Displays the statistics in units of bytes and bytes per second (Bps).</td>
</tr>
<tr>
<td>c</td>
<td>Clears (return to 0) the delta counters in the <code>Current Delta</code> column. The statistics counters are not cleared.</td>
</tr>
<tr>
<td>d</td>
<td>Displays the <code>Current Delta</code> column (instead of the rate column) in Bps or packets per second (pps).</td>
</tr>
<tr>
<td>p</td>
<td>Displays the statistics in units of packets and packets per second (pps).</td>
</tr>
<tr>
<td>q or Esc</td>
<td>Quits the command and returns to the command prompt.</td>
</tr>
<tr>
<td>r</td>
<td>Displays the rate column (instead of the <code>Current Delta</code> column) in Bps and pps.</td>
</tr>
</tbody>
</table>

**Required Privilege Level**

| trace |

**List of Sample Output**

- `monitor interface (Physical) on page 2474`
- `monitor interface (OTN Interface) on page 2475`
- `monitor interface (Logical) on page 2476`
- `monitor interface (QFX3500 Switch) on page 2476`
- `monitor interface traffic on page 2477`
- `monitor interface traffic (QFX3500 Switch) on page 2477`
- `monitor interface traffic detail (QFX3500 Switch) on page 2478`

**Output Fields**

Table 316 on page 2473 describes the output fields for the `monitor interface` command. Output fields are listed in the approximate order in which they appear.
Table 316: monitor interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>router1</td>
<td>Hostname of the router.</td>
<td>All levels</td>
</tr>
<tr>
<td>Seconds</td>
<td>How long the monitor interface command has been running or how long since you last cleared the counters.</td>
<td>All levels</td>
</tr>
<tr>
<td>Time</td>
<td>Current time (UTC).</td>
<td>All levels</td>
</tr>
<tr>
<td>Delay x/y/z</td>
<td>Time difference between when the statistics were displayed and the actual clock time.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• x—Time taken for the last polling (in milliseconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• y—Minimum time taken across all pollings (in milliseconds).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• z—Maximum time taken across all pollings (in milliseconds).</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Short description of the interface, including its name, status, and encapsulation.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link</td>
<td>State of the link: <strong>Up</strong>, <strong>Down</strong>, or <strong>Test</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Current delta</td>
<td>Cumulative number for the counter in question since the time shown in the Seconds field, which is the time since you started the command or last cleared the counters.</td>
<td>All levels</td>
</tr>
<tr>
<td>Local Statistics</td>
<td>(Logical interfaces only) Number and rate of bytes and packets destined to the router or switch through the specified interface. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It usually takes less than 1 second for this counter to stabilize.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Remote Statistics</td>
<td>(Logical interfaces only) Statistics for traffic transiting the router or switch. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It usually takes less than 1 second for this counter to stabilize.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>
Table 316: monitor interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic statistics</td>
<td>Total number of bytes and packets received and transmitted on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>These statistics are the sum of the local and remote statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It usually takes less than 1 second for this counter to stabilize.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

Description
With the traffic option, displays the interface description configured at the [edit interfaces interface-name] hierarchy level.

Sample Output
monitor interface (Physical)

```
user@host> monitor interface so-0/0/0
router1                              Seconds:   19       Time: 15:46:29
Interface: so-0/0/0, Enabled, Link is Up
Encapsulation: PPP, Keepalives, Speed: OC48
Traffic statistics:                                           Current Delta
  Input packets:                      6045 (0 pps)                     [11]
  Input bytes:                     6290065 (0 bps)                  [13882]
  Output packets:                    10376 (0 pps)                     [10]
  Output bytes:                   10365540 (0 bps)                   [9418]
Encapsulation statistics:                                                                                       Current Delta
  Input keepalives:                   1901                              [2]
  Output keepalives:                  1901                              [2]
NCP state: Opened
LCP state: Opened
Error statistics:
  Input errors:                          0                              [0]
  Input drops:                           0                              [0]
  Input framing errors:                  0                              [0]
  Policed discards:                      0                              [0]
  L3 incompletes:                        0                              [0]
  L2 channel errors:                     0                              [0]
  L2 mismatch timeouts:                  0                              [0]
  Carrier transitions:                   1                              [0]
  Output errors:                         0                              [0]
  Output drops:                          0                              [0]
  Aged packets:                          0                              [0]
Active alarms : None
Active defects: None
SONET error counts/seconds:
  LOS count                              1                              [0]
  LOF count                              1                              [0]
  SEF count                              1                              [0]
  ES-S                                   0                              [0]
  SES-S                                   0                              [0]
SONET statistics:
  BIP-B1                                458871                         [0]
```
BIP-B2  460072  [0]
REI-L  465610  [0]
BIP-B3  458978  [0]
REI-P  458773  [0]

Received SONET overhead:
F1      : 0x00  J0        : 0x00  K1        : 0x00
K2      : 0x00  S1        : 0x00  C2        : 0x00
C2(cmp) : 0x00  F2        : 0x00  Z3        : 0x00
Z4      : 0x00  S1(cmp)   : 0x00

Transmitted SONET overhead:
F1      : 0x00  J0        : 0x01  K1        : 0x00
K2      : 0x00  S1        : 0x00  C2        : 0xcf
F2      : 0x00  Z3        : 0x00  Z4        : 0x00

Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'

monitor interface (OTN Interface)

user@host> monitor interface ge-7/0/0

Interface: ge-7/0/0, Enabled, Link is Up
Encapsulation: Ethernet, Speed: 10000mbps
Traffic statistics:
Input bytes:                          0 (0 bps)
Output bytes:                         0 (0 bps)
Input packets:                        0 (0 pps)
Output packets:                       0 (0 pps)
Error statistics:
Input errors:                         0
Input drops:                          0
Input framing errors:                 0
Policed discards:                     0
L3 incompletes:                       0
L2 channel errors:                    0
L2 mismatch timeouts:                 0
Carrier transitions:                  5
Output errors:                        0
Output drops:                         0
Aged packets:                         0
Active alarms : None
Active defects: None
Input MAC/Filter statistics:
  Unicast packets                      0
  Broadcast packets                    0
  Multicast packets                    0
  Oversized frames                     0
  Packet reject count                  0
  DA rejects                           0
  SA rejects                           0
Output MAC/Filter Statistics:
  Unicast packets                      0
  Broadcast packets                    0
  Multicast packets                    0
  Packet pad count                     0
  Packet error count                   0
OTN Link 0
  OTN Alarms: OTU_BDI, OTU_TTIM, ODU_BDI
  OTN Defects: OTU_BDI, OTU_TTIM, ODU_BDI, ODU_TTIM
  OTN OC - Seconds
    LOS                                2
monitor interface (Logical)

user@host> monitor interface so-1/0/0.0
host name          Seconds: 16                  Time: 15:33:39
                    Delay: 0/0/1

Interface: so-1/0/0.0, Enabled, Link is Down
Flags: Hardware-Down Point-To-Point SNMP-Traps
Encapsulation: PPP

Local statistics:                              Current delta
Input bytes:                          0       [0]
Output bytes:                         0       [0]
Input packets:                        0       [0]
Output packets:                       0       [0]

Remote statistics:
Input bytes:                          0 (0 bps)   [0]
Output bytes:                        0 (0 bps)   [0]
Input packets:                       0 (0 pps)   [0]
Output packets:                      0 (0 pps)   [0]

Traffic statistics:
Destination address: 192.168.8.193, Local: 192.168.8.21

Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'

monitor interface (QFX3500 Switch)

user@switch> monitor interface ge-0/0/0
Interface: ge-0/0/0, Enabled, Link is Down
Encapsulation: Ethernet, Speed: Unspecified

Traffic statistics:                                          Current delta
Input bytes:                          0 (0 bps)   [0]
Output bytes:                        0 (0 bps)   [0]
Input packets:                       0 (0 pps)   [0]
Output packets:                      0 (0 pps)   [0]

Error statistics:
Input errors:                        0       [0]
Input drops:                         0       [0]
Input framing errors:                0       [0]
Policed discards:                    0       [0]
L3 incompletes:                      0       [0]
L2 channel errors:                   0       [0]
L2 mismatch timeouts:                0       [0]
Carrier transitions:                 0       [0]
Output errors: 0
Output drops: 0
Aged packets: 0
Active alarms: LINK
Active defects: LINK
Input MAC/Filter statistics:
  Unicast packets: 0
  Broadcast packets: 0 Multicast packet: 0
Interface warnings:
  o Outstanding LINK alarm

```
monitor interface traffic
```

```
user@host> monitor interface traffic
host name Seconds: 15 Time: 12:31:09

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>Input packets</th>
<th>(pps)</th>
<th>Output packets</th>
<th>(pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-1/0/0</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>so-1/1/0</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>so-1/1/1</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>so-1/1/2</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>so-1/1/3</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>t3-1/2/0</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>t3-1/2/1</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>t3-1/2/2</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>t3-1/2/3</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/0/0</td>
<td>Up</td>
<td>211035</td>
<td>(1)</td>
<td>36778</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/0/1</td>
<td>Up</td>
<td>192753</td>
<td>(1)</td>
<td>36782</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/0/2</td>
<td>Up</td>
<td>211020</td>
<td>(1)</td>
<td>36779</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/0/3</td>
<td>Up</td>
<td>211029</td>
<td>(1)</td>
<td>36776</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/1/0</td>
<td>Up</td>
<td>189378</td>
<td>(1)</td>
<td>36349</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/1/1</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>18747</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/1/2</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>16078</td>
<td>(0)</td>
</tr>
<tr>
<td>so-2/1/3</td>
<td>Up</td>
<td>0</td>
<td>(0)</td>
<td>80338</td>
<td>(0)</td>
</tr>
<tr>
<td>at-2/3/0</td>
<td>Up</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>at-2/3/1</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
</tbody>
</table>

Bytes=b, Clear=c, Delta=d, Packets=p, Quit=q or ESC, Rate=r, Up=^U, Down=^D

```
monitor interface traffic (QFX3500 Switch)
```

```
user@switch> monitor interface traffic
switch Seconds: 7 Time: 16:04:37

<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>Input packets</th>
<th>(pps)</th>
<th>Output packets</th>
<th>(pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Up</td>
<td>0</td>
<td>(0)</td>
<td>392170</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>Up</td>
<td>0</td>
<td>(0)</td>
<td>392171</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/11</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/12</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/13</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
<tr>
<td>ge-0/0/14</td>
<td>Down</td>
<td>0</td>
<td>(0)</td>
<td>0</td>
<td>(0)</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Link</th>
<th>Input packets (pps)</th>
<th>Output packets (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Up</td>
<td>392183</td>
<td>392166</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>Up</td>
<td>392181</td>
<td>392168</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/11</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/12</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/13</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/14</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/15</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/16</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/17</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/18</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/19</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/20</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/21</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/22</td>
<td>Up</td>
<td>392169</td>
<td>392184</td>
</tr>
<tr>
<td>ge-0/0/23</td>
<td>Up</td>
<td>392182</td>
<td>392170</td>
</tr>
<tr>
<td>vcp-0</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ae0</td>
<td>Down</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bme0</td>
<td>Up</td>
<td>0</td>
<td>1568693</td>
</tr>
</tbody>
</table>
```

**monitor interface traffic detail (QFX3500 Switch)**

```
user@switch> monitor interface traffic detail
switch
Time: 16:03:02
Switch: Seconds: 74
```

Copyright © 2013, Juniper Networks, Inc.
request diagnostics tdr

Syntax
request diagnostics tdr (abort | start) interface interface-name

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Start a time domain reflectometry (TDR) diagnostic test on the specified interface. This test characterizes and locates faults on twisted-pair Ethernet cables. For example, it can detect a broken twisted pair and provide the approximate distance to the break. It can also detect polarity swaps, pair swaps, and excessive skew.

The TDR test is supported on the following switches and interfaces:

- EX2200, EX3200, EX3300, and EX4200 switches—RJ-45 network interfaces. The TDR test is not supported on management interfaces and SFP interfaces.
- EX6200 and EX8200 switches—RJ-45 interfaces on line cards.

NOTE: We recommend running the TDR test when there is no traffic on the interface under test.

You view the results of the TDR test with the show diagnostics tdr command.

Options
- abort—Stop the TDR test currently in progress on the specified interface. No results are reported, and previous results, if any, are cleared.
- interface-name—The name of the interface.
- start—Start a TDR test on the specified interface.

Required Privilege Level
maintenance

Related Documentation
- show diagnostics tdr on page 2481
- Diagnosing a Faulty Twisted-Pair Cable (CLI Procedure) on page 2547

List of Sample Output
request diagnostics tdr start interface ge-0/0/19 on page 2480

Output Fields
Table 317 on page 2480 lists the output fields for the request diagnostics tdr command. Output fields are listed in the approximate order in which they appear.
### Table 317: request diagnostics tdr Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Test Status</strong></td>
<td>Information about the status of the TDR test request:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Admin Down</strong> interface-name — The interface is administratively down.</td>
</tr>
<tr>
<td></td>
<td>The TDR test cannot run on interfaces that are administratively down.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interface not found</strong> — The interface does not exist.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Test successfully executed</strong> interface-name — The test has successfully</td>
</tr>
<tr>
<td></td>
<td>started on the interface. You can view the test results with the `show</td>
</tr>
<tr>
<td></td>
<td>diagnostics tdr` command.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VCT not supported on</strong> interface-name — The TDR test is not supported</td>
</tr>
<tr>
<td></td>
<td>on the interface.</td>
</tr>
</tbody>
</table>

### Sample Output

```plaintext
request diagnostics tdr start interface ge-0/0/19

user@switch> request diagnostics tdr start interface ge-0/0/19

Interface TDR detail:
Test status : Test successfully executed ge-0/0/19
```
### show diagnostics tdr

**Syntax**

```plaintext
show diagnostics tdr
  <interface interface-name>
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display the results of a time domain reflectometry (TDR) diagnostic test run on an interface. A TDR test characterizes and locates faults on twisted-pair Ethernet cables. For example, it can detect a broken twisted pair and provide the approximate distance to the break. It can also detect polarity swaps, pair swaps, and excessive skew.

The TDR test is supported on the following switches and interfaces:

- EX2200, EX3200, EX3300, and EX4200 switches—RJ-45 network interfaces. The TDR test is not supported on management interfaces and SFP interfaces.
- EX6200 and EX8200 switches—RJ-45 interfaces on line cards.

Use the `request diagnostics tdr` command to request a TDR test on a specified interface. Use the `show diagnostic tdr` command to display the last TDR test results for a specified interface or the last TDR test results for all network interfaces on the switch that support the TDR test.

**Options**

- `none`—Show summarized last results for all interfaces on the switch that support the TDR test.
- `interface interface-name`—(Optional) Show detailed last results for the specified interface or a range of interfaces. Specify a range of interfaces by entering the beginning and ending interface in the range, separated by a dash—for example, `ge-0/0/15-ge-0/0/20`.

**Required Privilege Level**

`view`

**Related Documentation**

- `request diagnostics tdr` on page 2479
- `Diagnosing a Faulty Twisted-Pair Cable (CLI Procedure)` on page 2547

**List of Sample Output**

- `show diagnostics tdr interface ge-0/0/19 (Normal Cable)` on page 2483
- `show diagnostics tdr interface ge-2/0/2 (Faulty Cable)` on page 2484
- `show diagnostics tdr (All Supported Interfaces)` on page 2484

**Output Fields**

Table 318 on page 2482 lists the output fields for the `show diagnostics tdr` command. Output fields are listed in the approximate order in which they appear.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name or Interface</td>
<td>Name of interface for which TDR test results are being reported.</td>
</tr>
<tr>
<td>Test status</td>
<td>Status of TDR test:</td>
</tr>
<tr>
<td></td>
<td>• Aborted—Test was terminated by operator before it was complete.</td>
</tr>
<tr>
<td></td>
<td>• Failed—Test was not completed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Interface interface-name not found—Specified interface does not exist.</td>
</tr>
<tr>
<td></td>
<td>• Not Started—No TDR test results are available for the interface.</td>
</tr>
<tr>
<td></td>
<td>• Passed—Test completed successfully. The cable, however, might still have a fault—see the Cable status field for information on the cable.</td>
</tr>
<tr>
<td></td>
<td>• Started—Test is currently running and not yet complete.</td>
</tr>
<tr>
<td></td>
<td>• VCT not supported on interface-name—TDR test is not supported on the interface.</td>
</tr>
<tr>
<td>Link status</td>
<td>Operating status of link: UP or Down.</td>
</tr>
<tr>
<td>MDI pair</td>
<td>Twisted pair for which test results are being reported, identified by pin numbers. (Displayed only when the interface option is used.)</td>
</tr>
<tr>
<td>Cable status</td>
<td>When detailed information is displayed, status for a twisted pair:</td>
</tr>
<tr>
<td></td>
<td>• Failed—TDR test failed on the cable pair.</td>
</tr>
<tr>
<td></td>
<td>• Impedance Mismatch—Impedance on the twisted pair is not correct. Possible reasons for an impedance mismatch include:</td>
</tr>
<tr>
<td></td>
<td>• The twisted pair is not connected properly.</td>
</tr>
<tr>
<td></td>
<td>• The twisted pair is damaged.</td>
</tr>
<tr>
<td></td>
<td>• The connector is faulty.</td>
</tr>
<tr>
<td></td>
<td>• Normal—No cable fault detected for the twisted pair.</td>
</tr>
<tr>
<td></td>
<td>• Open—Lack of continuity between the pins at each end of the twisted-pair.</td>
</tr>
<tr>
<td></td>
<td>• Short on Pair-n—A short-circuit was detected on the twisted pair.</td>
</tr>
<tr>
<td>Distance fault or Max distance fault</td>
<td>Distance to the fault in whole meters. If there is no fault, this value is 0. When summary information for all interfaces is displayed, this value is the distance to the most distant fault if there is more than one twisted pair with a fault.</td>
</tr>
</tbody>
</table>
Table 318: show diagnostics tdr Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polarity swap</td>
<td>Indicates the polarity status of the twisted pair:</td>
</tr>
<tr>
<td></td>
<td>• Normal—Polarity is normal. Each conductor in the twisted pair has been connected the same pins at the both ends of the connection. For example, a conductor connected to pin 1 at the near end of the connection is connected to pin 1 at the far end.</td>
</tr>
<tr>
<td></td>
<td>• Reversed—Polarity has been reversed. For the twisted pair, the conductors have switched which pins they are connected to at the near and far ends of the connection. For example, the conductor connected to pin 1 at the near end is connected to pin 2 at the far end.</td>
</tr>
<tr>
<td></td>
<td>(Not available on EX8200 switches.) (Displayed only when the interface option is used)</td>
</tr>
<tr>
<td>Skew time</td>
<td>Difference in nanoseconds between the propagation delay on this twisted pair and the twisted pair with the shortest propagation delay. (Not available on EX8200 switches.) (Displayed only when the interface option is used.)</td>
</tr>
<tr>
<td>Channel Pair</td>
<td>Number of the 10/100BASE-T transmit/receive pair being reported on.</td>
</tr>
<tr>
<td>Pair Swap</td>
<td>Indicates whether or not the twisted pairs are swapped:</td>
</tr>
<tr>
<td></td>
<td>• MDI—The pairs are not swapped (straight-through cable).</td>
</tr>
<tr>
<td></td>
<td>• MDIX—The pairs are swapped (cross-over cable).</td>
</tr>
<tr>
<td></td>
<td>(Displayed only when the interface option is used.)</td>
</tr>
<tr>
<td>Downshift</td>
<td>Indicates whether the connection speed is being downshifted:</td>
</tr>
<tr>
<td></td>
<td>• No Downshift—No downshifting of connection speed.</td>
</tr>
<tr>
<td></td>
<td>• Downshift occurs—Connection speed is downshifted to 10 or 100 Mbs. This occurs if the cable is a two-pair cable rather than the four-pair cable required by Gigabit Ethernet.</td>
</tr>
<tr>
<td></td>
<td>(Displayed only when the interface option is used.)</td>
</tr>
</tbody>
</table>

Sample Output

show diagnostics tdr interface ge-0/0/19 (Normal Cable)

```
user@switch> show diagnostics tdr interface ge-0/0/19
Interface TDR detail:
Interface name                  : ge-0/0/19
Test status                     : Passed
Link status                     : UP
MDI pair                        : 1-2
Cable status                   : Normal
Distance fault                  : 0 Meters
Polarity swap                   : Normal
Skew time                       : 0 ns
MDI pair                       : 3-6
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Test status</th>
<th>Link status</th>
<th>Cable status</th>
<th>Max distance fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

show diagnostics tdr (All Supported Interfaces)
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>State</th>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/4</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Passed</td>
<td>UP</td>
<td>Fault</td>
<td>173</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/11</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/12</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/13</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/14</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/15</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/16</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/17</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/18</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/19</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/20</td>
<td>Passed</td>
<td>Down</td>
<td>Fault</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/21</td>
<td>Passed</td>
<td>Down</td>
<td>Fault</td>
<td>5</td>
</tr>
<tr>
<td>ge-0/0/22</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/23</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
</tbody>
</table>
**show interfaces diagnostics optics**

**Syntax**  
show interfaces diagnostics optics *interface-name*

**Release Information**  
Command introduced in Junos OS Release 10.0 for EX Series switches.

**Description**  
Display diagnostics data and alarms for Gigabit Ethernet optical transceivers (SFP, SFP+, or XFP) installed in EX Series switches. The information provided by this command is known as digital optical monitoring (DOM) information.

Thresholds that trigger a high alarm, low alarm, high warning, or low warning are set by the transponder vendors. Generally, a high alarm or low alarm indicates that the optics module is not operating properly. This information can be used to diagnose why a transceiver is not working.

**Options**  
*interface-name*—Name of the interface associated with the port in which the transceiver is installed: *ge-fpc/pic/port* or *xe-fpc/pic/port*.

**Required Privilege Level**  
view

**Related Documentation**
- Monitoring Interface Status and Traffic on page 2463
- Installing a Transceiver in an EX Series Switch
- Removing a Transceiver from an EX Series Switch
- Junos OS Ethernet Interfaces Configuration Guide

**List of Sample Output**
- show interfaces diagnostics optics ge-0/1/0 (SFP Transceiver) on page 2490
- show interfaces diagnostics optics xe-0/1/0 (SFP+ Transceiver) on page 2491
- show interfaces diagnostics optics xe-0/1/0 (XFP Transceiver) on page 2491

**Output Fields**
Table 319 on page 2486 lists the output fields for the show interfaces diagnostics optics command. Output fields are listed in the approximate order in which they appear.

### Table 319: show interfaces diagnostics optics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical interface</td>
<td>Displays the name of the physical interface.</td>
</tr>
<tr>
<td>Laser bias current</td>
<td>Displays the magnitude of the laser bias power setting current, in milliamperes. The laser bias provides direct modulation of laser diodes and modulates currents.</td>
</tr>
<tr>
<td>Laser output power</td>
<td>Displays the laser output power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm).</td>
</tr>
<tr>
<td>Module temperature</td>
<td>Displays the temperature, in Celsius and Fahrenheit.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Module voltage</td>
<td>Displays the voltage, in Volts.</td>
</tr>
<tr>
<td></td>
<td>(Not available for XFP transceivers)</td>
</tr>
<tr>
<td>Laser rx power</td>
<td>Displays the laser received optical power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm).</td>
</tr>
<tr>
<td></td>
<td>(Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td>Receiver signal average optical power</td>
<td>Displays the receiver signal average optical power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm).</td>
</tr>
<tr>
<td></td>
<td>(Not available for XFP transceivers)</td>
</tr>
<tr>
<td>Laser bias current high alarm</td>
<td>Displays whether the laser bias power setting high alarm is On or Off.</td>
</tr>
<tr>
<td>Laser bias current low alarm</td>
<td>Displays whether the laser bias power setting low alarm is On or Off.</td>
</tr>
<tr>
<td>Laser bias current high warning</td>
<td>Displays whether the laser bias power setting high warning is On or Off.</td>
</tr>
<tr>
<td>Laser bias current low warning</td>
<td>Displays whether the laser bias power setting low warning is On or Off.</td>
</tr>
<tr>
<td>Laser output power high alarm</td>
<td>Displays whether the laser output power high alarm is On or Off.</td>
</tr>
<tr>
<td>Laser output power low alarm</td>
<td>Displays whether the laser output power low alarm is On or Off.</td>
</tr>
<tr>
<td>Laser output power high warning</td>
<td>Displays whether the laser output power high warning is On or Off.</td>
</tr>
<tr>
<td>Laser output power low warning</td>
<td>Displays whether the laser output power low warning is On or Off.</td>
</tr>
<tr>
<td>Module temperature high alarm</td>
<td>Displays whether the module temperature high alarm is On or Off.</td>
</tr>
<tr>
<td>Module temperature low alarm</td>
<td>Displays whether the module temperature low alarm is On or Off.</td>
</tr>
<tr>
<td>Module temperature high warning</td>
<td>Displays whether the module temperature high warning is On or Off.</td>
</tr>
<tr>
<td>Module temperature low warning</td>
<td>Displays whether the module temperature low warning is On or Off.</td>
</tr>
<tr>
<td>Module voltage high alarm</td>
<td>Displays whether the module voltage high alarm is On or Off.</td>
</tr>
<tr>
<td></td>
<td>(Not available for XFP transceivers)</td>
</tr>
<tr>
<td>Module voltage low alarm</td>
<td>Displays whether the module voltage low alarm is On or Off.</td>
</tr>
<tr>
<td></td>
<td>(Not available for XFP transceivers)</td>
</tr>
<tr>
<td>Module voltage high warning</td>
<td>Displays whether the module voltage high warning is On or Off.</td>
</tr>
<tr>
<td></td>
<td>(Not available for XFP transceivers)</td>
</tr>
</tbody>
</table>
### Table 319: show interfaces diagnostics optics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module voltage low warning</strong></td>
<td>Displays whether the module voltage low warning is On or Off. (Not available for XFP transceivers)</td>
</tr>
<tr>
<td><strong>Laser rx power high alarm</strong></td>
<td>Displays whether the receive laser power high alarm is On or Off.</td>
</tr>
<tr>
<td><strong>Laser rx power low alarm</strong></td>
<td>Displays whether the receive laser power low alarm is On or Off.</td>
</tr>
<tr>
<td><strong>Laser rx power high warning</strong></td>
<td>Displays whether the receive laser power high warning is On or Off.</td>
</tr>
<tr>
<td><strong>Laser rx power low warning</strong></td>
<td>Displays whether the receive laser power low warning is On or Off.</td>
</tr>
<tr>
<td><strong>Laser bias current high alarm threshold</strong></td>
<td>Displays the vendor-specified threshold for the laser bias current high alarm.</td>
</tr>
<tr>
<td><strong>Module not ready alarm</strong></td>
<td>Displays whether the module not ready alarm is On or Off. When the output is On, the module has an operational fault. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Module power down alarm</strong></td>
<td>Displays whether the module power down alarm is On or Off. When the output is On, module is in a limited power mode, low for normal operation. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Tx data not ready alarm</strong></td>
<td>Any condition leading to invalid data on the transmit path. Displays whether the Tx data not ready alarm is On or Off. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Tx not ready alarm</strong></td>
<td>Any condition leading to invalid data on the transmit path. Displays whether the Tx not ready alarm is On or Off. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Tx laser fault alarm</strong></td>
<td>Laser fault condition. Displays whether the Tx laser fault alarm is On or Off. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Tx CDR loss of lock alarm</strong></td>
<td>Transmit clock and data recovery (CDR) loss of lock. Loss of lock on the transmit side of the CDR. Displays whether the Tx CDR loss of lock alarm is On or Off. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Rx not ready alarm</strong></td>
<td>Any condition leading to invalid data on the receive path. Displays whether the Rx not ready alarm is On or Off. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Rx loss of signal alarm</strong></td>
<td>Receive loss of signal alarm. When on, indicates insufficient optical input power to the module. Displays whether the Rx loss of signal alarm is On or Off. (Not available for SFP and SFP+ transceivers)</td>
</tr>
<tr>
<td><strong>Rx CDR loss of lock alarm</strong></td>
<td>Receive CDR loss of lock. Loss of lock on the receive side of the CDR. Displays whether the Rx CDR loss of lock alarm is On or Off. (Not available for SFP and SFP+ transceivers)</td>
</tr>
</tbody>
</table>
### Table 319: show interfaces diagnostics optics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser bias current low alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser bias current low alarm.</td>
</tr>
<tr>
<td>Laser bias current high warning threshold</td>
<td>Displays the vendor-specified threshold for the laser bias current high warning.</td>
</tr>
<tr>
<td>Laser bias current low warning threshold</td>
<td>Displays the vendor-specified threshold for the laser bias current low warning.</td>
</tr>
<tr>
<td>Laser output power high alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser output power high alarm.</td>
</tr>
<tr>
<td>Laser output power low alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser output power low alarm.</td>
</tr>
<tr>
<td>Laser output power high warning threshold</td>
<td>Displays the vendor-specified threshold for the laser output power high warning.</td>
</tr>
<tr>
<td>Laser output power low warning threshold</td>
<td>Displays the vendor-specified threshold for the laser output power low warning.</td>
</tr>
<tr>
<td>Module temperature high alarm threshold</td>
<td>Displays the vendor-specified threshold for the module temperature high alarm.</td>
</tr>
<tr>
<td>Module temperature low alarm threshold</td>
<td>Displays the vendor-specified threshold for the module temperature low alarm.</td>
</tr>
<tr>
<td>Module temperature high warning threshold</td>
<td>Displays the vendor-specified threshold for the module temperature high warning.</td>
</tr>
<tr>
<td>Module temperature low warning threshold</td>
<td>Displays the vendor-specified threshold for the module temperature low warning.</td>
</tr>
<tr>
<td>Module voltage high alarm threshold</td>
<td>Displays the vendor-specified threshold for the module voltage high alarm.</td>
</tr>
<tr>
<td>(Not available for XFP transceivers)</td>
<td></td>
</tr>
<tr>
<td>Module voltage low alarm threshold</td>
<td>Displays the vendor-specified threshold for the module voltage low alarm.</td>
</tr>
<tr>
<td>(Not available for XFP transceivers)</td>
<td></td>
</tr>
<tr>
<td>Module voltage high warning threshold</td>
<td>Displays the vendor-specified threshold for the module voltage high warning.</td>
</tr>
<tr>
<td>(Not available for XFP transceivers)</td>
<td></td>
</tr>
<tr>
<td>Module voltage low warning threshold</td>
<td>Displays the vendor-specified threshold for the module voltage low warning.</td>
</tr>
<tr>
<td>(Not available for XFP transceivers)</td>
<td></td>
</tr>
<tr>
<td>Laser rx power high alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power high alarm.</td>
</tr>
<tr>
<td>(Not available for XFP transceivers)</td>
<td></td>
</tr>
</tbody>
</table>
Table 319: show interfaces diagnostics optics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser rx power low alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power low alarm.</td>
</tr>
<tr>
<td>Laser rx power high warning threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power high warning.</td>
</tr>
<tr>
<td>Laser rx power low warning threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power low warning.</td>
</tr>
</tbody>
</table>

Sample Output

show interfaces diagnostics optics ge-0/1/0 (SFP Transceiver)

```
user@host> show interfaces diagnostics optics ge-0/1/0
Physical interface: ge-0/1/0
  Laser bias current : 5.444 mA
  Laser output power : 0.3130 mW / -5.04 dBm
  Module temperature : 36 degrees C / 97 degrees F
  Module voltage : 3.2120 V
  Receiver signal average optical power : 0.3840 mW / -4.16 dBm
  Laser bias current high alarm : Off
  Laser bias current low alarm : Off
  Laser bias current high warning : Off
  Laser bias current low warning : Off
  Laser output power high alarm : Off
  Laser output power low alarm : Off
  Laser output power high warning : Off
  Laser output power low warning : Off
  Module temperature high alarm : Off
  Module temperature low alarm : Off
  Module temperature high warning : Off
  Module temperature low warning : Off
  Module voltage high alarm : Off
  Module voltage low alarm : Off
  Module voltage high warning : Off
  Module voltage low warning : Off
  Laser rx power high alarm : Off
  Laser rx power low alarm : Off
  Laser rx power high warning : Off
  Laser rx power low warning : Off
  Laser bias current high alarm threshold : 15.000 mA
  Laser bias current low alarm threshold : 1.000 mA
  Laser bias current high warning threshold : 12.000 mA
  Laser bias current low warning threshold : 2.000 mA
  Laser output power high alarm threshold : 0.6300 mW / -2.01 dBm
  Laser output power low alarm threshold : 0.0660 mW / -11.80 dBm
  Laser output power high warning threshold : 0.6300 mW / -2.01 dBm
  Laser output power low warning threshold : 0.0780 mW / -11.08 dBm
  Module temperature high alarm threshold : 109 degrees C / 228 degrees F
  Module temperature low alarm threshold : -29 degrees C / -20 degrees F
  Module temperature high warning threshold : 103 degrees C / 217 degrees F
  Module temperature low warning threshold : -13 degrees C / 9 degrees F
  Module voltage high alarm threshold : 3.900 V
  Module voltage low alarm threshold : 2.700 V
  Module voltage high warning threshold : 3.700 V
  Module voltage low warning threshold : 2.900 V
  Laser rx power high alarm threshold : 1.2589 mW / 1.00 dBm
```
Laser rx power low alarm threshold : 0.0100 mW / -20.00 dBm
Laser rx power high warning threshold : 0.7939 mW / -1.00 dBm
Laser rx power low warning threshold : 0.0157 mW / -18.04 dBm

Sample Output

show interfaces diagnostics optics xe-0/1/0 (SFP+ Transceiver)

user@host> show interfaces diagnostics optics xe-0/1/0
Physical interface: xe-0/1/0
  Laser bias current : 4.968 mA
  Laser output power : 0.4940 mW / -3.06 dBm
  Module temperature : 27 degrees C / 81 degrees F
  Module voltage : 3.2310 V
  Receiver signal average optical power : 0.0000
  Laser bias current high alarm : Off
  Laser bias current low alarm : Off
  Laser bias current high warning : Off
  Laser bias current low warning : Off
  Laser output power high alarm : Off
  Laser output power low alarm : Off
  Laser output power high warning : Off
  Laser output power low warning : Off
  Module temperature high alarm : Off
  Module temperature low alarm : Off
  Module temperature high warning : Off
  Module temperature low warning : Off
  Module voltage high alarm : Off
  Module voltage low alarm : Off
  Module voltage high warning : Off
  Module voltage low warning : Off
  Laser rx power high alarm : Off
  Laser rx power low alarm : On
  Laser rx power high warning : Off
  Laser rx power low warning : On
  Laser bias current high alarm threshold : 10.500 mA
  Laser bias current low alarm threshold : 2.000 mA
  Laser bias current high warning threshold : 9.000 mA
  Laser bias current low warning threshold : 2.500 mA
  Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
  Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
  Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
  Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
  Module temperature high alarm threshold : 75 degrees C / 167 degrees F
  Module temperature low alarm threshold : -5 degrees C / 23 degrees F
  Module temperature high warning threshold : 70 degrees C / 158 degrees F
  Module temperature low warning threshold : 0 degrees C / 32 degrees F
  Module voltage high alarm threshold : 3.630 V
  Module voltage low alarm threshold : 2.970 V
  Module voltage high warning threshold : 3.465 V
  Module voltage low warning threshold : 3.135 V
  Laser rx power high alarm threshold : 1.5849 mW / 2.00 dBm
  Laser rx power low alarm threshold : 0.0407 mW / -13.90 dBm
  Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
  Laser rx power low warning threshold : 0.1023 mW / -9.90 dBm

Sample Output

show interfaces diagnostics optics xe-0/1/0 (XFP Transceiver)

user@host> show interfaces diagnostics optics xe-0/1/0
Physical interface: xe-0/1/0

Laser bias current : 8.029 mA
Laser output power : 0.6430 mW / -1.92 dBm
Module temperature : 4 degrees C / 39 degrees F
Laser rx power : 0.0012 mW / -29.21 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : On
Laser rx power high warning : Off
Laser rx power low warning : On
Module not ready alarm : On
Module power down alarm : Off
Tx data not ready alarm : Off
Tx not ready alarm : Off
Tx laser fault alarm : Off
Tx CDR loss of lock alarm : Off
Rx not ready alarm : On
Rx loss of signal alarm : On
Rx CDR loss of lock alarm : On
Laser bias current high alarm threshold : 13.000 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 12.000 mA
Laser bias current low warning threshold : 3.000 mA
Laser output power high alarm threshold : 0.8310 mW / -0.80 dBm
Laser output power low alarm threshold : 0.1650 mW / -7.83 dBm
Laser output power high warning threshold : 0.7410 mW / -1.30 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Module temperature high alarm threshold : 90 degrees C / 194 degrees F
Module temperature low alarm threshold : 0 degrees C / 32 degrees F
Module temperature high warning threshold : 85 degrees C / 185 degrees F
Module temperature low warning threshold : 0 degrees C / 32 degrees F
Laser rx power high alarm threshold : 0.8912 mW / -0.50 dBm
Laser rx power low alarm threshold : 0.0912 mW / -10.40 dBm
Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
Laser rx power low warning threshold : 0.1023 mW / -9.90 dBm
**show interfaces ge-**

**Syntax**
```
show interfaces ge-fpc/pic/port
  <brief | detail | extensive | terse>
  <media>
  <statistics>
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display status information about the specified Gigabit Ethernet interface.

**NOTE:** You must have a transceiver plugged into an SFP or SFP+ port before information about the interface can be displayed.

**Options**
- `ge-fpc/pic/port`—Display standard information about the specified Gigabit Ethernet interface.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `media`—(Optional) Display media-specific information about network interfaces.

**Required Privilege Level**
view

**Related Documentation**
- Monitoring Interface Status and Traffic on page 2463
- Troubleshooting Network Interfaces on EX3200 Switches
- Troubleshooting Network Interfaces on EX4200 Switches
- Troubleshooting an Aggregated Ethernet Interface on page 2545
- Junos OS Ethernet Interfaces Configuration Guide

**List of Sample Output**
- show interfaces ge-0/0/0 on page 2500
- show interfaces ge-0/0/0 brief on page 2500
- show interfaces ge-0/0/0 brief (with EEE Enabled on the EEE-capable Base-T copper Ethernet interfaces) on page 2501
- show interfaces ge-0/0/0 detail on page 2501
- show interfaces ge-0/0/4 extensive on page 2502

**Output Fields**
Table 320 on page 2494 lists the output fields for the `show interfaces ge-` command. Output fields are listed in the approximate order in which they appear.
Table 320: show interfaces ge- Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical interface</strong></td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>State of the interface: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface index</strong></td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>SNMP ifIndex</strong></td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Generation</strong></td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Optional user-specified description.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Link-level type</strong></td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>Maximum transmission unit size on the physical interface. Default is 1514.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>Speed of the interface: Auto if autonegotiation of speed is enabled; speed in</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>megabits per second if the interface speed is explicitly configured.</td>
<td></td>
</tr>
<tr>
<td><strong>Duplex</strong></td>
<td>Link mode of the interface: Auto if autonegotiation of link mode is enabled;</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>Full-Duplex or Half-Duplex if the link mode is explicitly configured.</td>
<td></td>
</tr>
<tr>
<td><strong>Loopback</strong></td>
<td>Loopback status: <strong>Enabled</strong> or <strong>Disabled</strong>. If loopback is enabled, type of</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>loopback: <strong>Local</strong> or <strong>Remote</strong>.</td>
<td></td>
</tr>
<tr>
<td><strong>Source filtering</strong></td>
<td>Source filtering status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Flow control</strong></td>
<td>Flow control status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Auto-negotiation</strong></td>
<td>Autonegotiation status: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Remote-fault</strong></td>
<td>Remote fault status:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Online</strong>—Autonegotiation is manually configured as online.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Offline</strong>—Autonegotiation is manually configured as offline.</td>
<td></td>
</tr>
<tr>
<td><strong>IEEE 802.3az Energy Efficient Ethernet</strong></td>
<td>IEEE 802.3az Energy Efficient Ethernet status: <strong>Enabled</strong> or <strong>Disabled</strong> (appears only for EEE-capable Base-T copper Ethernet interfaces).</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Device flags</strong></td>
<td>Information about the physical device.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface flags</strong></td>
<td>Information about the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Link flags</strong></td>
<td>Information about the link.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>CoS queues</strong></td>
<td>Number of CoS queues configured.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 320: show interfaces ge- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hardware address</td>
<td>MAC address of the hardware.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago). For example, Last flapped: 2008–01–16 10:52:40 UTC (3d 22:58 ago).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface</td>
<td></td>
</tr>
<tr>
<td>NOTE:</td>
<td>The bandwidth bps counter is not enabled on the switch.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Errors—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Framing errors—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Runts—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L3 incompletes—Number of incoming packets discarded because they failed Layer 3 sanity checks of the headers. For example, a frame with less than 20 bytes of available IP header is discarded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L2 channel errors—Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L2 mismatch timeouts—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FIFO errors—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource errors—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>
Table 320: show interfaces ge- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Carrier transitions—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errors—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Collisions—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Aged packets—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FIFO errors—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HS link CRC errors—Number of errors on the high-speed links between the ASICs responsible for handling the switch interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MTU errors—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource errors—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Egress queues</td>
<td>Total number of egress queues supported on the specified interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Queue counters (Egress)</td>
<td>CoS queue number and its associated user-configured forwarding class name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Queued packets—Number of queued packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitted packets—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Dropped packets—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td>Active alarms and Active defects</td>
<td>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain time, it is promoted to an alarm. Based on the switch configuration, a defect can activate the red or yellow alarm bell on the switch or turn on the red or yellow alarm LED on the front of the switch. These fields can contain the value <strong>None</strong> or <strong>Link</strong>.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• None—There are no active defects or alarms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning.</td>
<td></td>
</tr>
</tbody>
</table>
Table 320: show interfaces ge- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC statistics</strong></td>
<td><strong>Receive and Transmit</strong> statistics reported by the PIC’s MAC subsystem.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Total octets</strong> and <strong>total packets</strong>—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Unicast packets, Broadcast packets, and Multicast packets</strong>—Number of unicast, broadcast, and multicast packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC/Align errors</strong>—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO error</strong>—Number of FIFO errors reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC control frames</strong>—Number of MAC control frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MAC pause frames</strong>—Number of MAC control frames with pause operational code.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Oversized frames</strong>—Number of frames that exceed 1518 octets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Jabber frames</strong>—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Fragment frames</strong>—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Code violations</strong>—Number of times an event caused the PHY to indicate “Data reception error” or “invalid data symbol error.”</td>
<td></td>
</tr>
<tr>
<td><strong>Filter Statistics</strong></td>
<td><strong>Receive and Transmit</strong> statistics reported by the PIC’s MAC address filter subsystem.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
### Table 320: show interfaces ge- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Autonegotiation information</strong></td>
<td>Information about link autonegotiation:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Negotiation status:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Complete</strong>—The autonegotiation process between the local and remote Ethernet interfaces was successful.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Incomplete</strong>—Remote Ethernet interface has the speed or link mode configured or does not perform autonegotiation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>No autonegotiation</strong>—Local Ethernet interface has autonegotiation disabled and the link mode and speed are manually configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link partner</strong>—Information from the link partner:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link mode</strong>—Depending on the capability of the attached Ethernet device, either Full-duplex or Half-duplex. If the link mode of the remote device cannot be determined, the value is Unknown.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flow control</strong>—Types of flow control supported by the remote Ethernet device. For Gigabit Ethernet interfaces, the types are: Symmetric (link partner supports PAUSE on receive and transmit); Asymmetric (link partner supports PAUSE on transmit); and Symmetric/Asymmetric (link partner supports PAUSE on both receive and transmit or PAUSE only on receive).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote fault</strong>—Remote fault information from the link partner—Failure indicates a receive link error. OK indicates that the link partner is receiving. Negotiation error indicates a negotiation error. Offline indicates that the link partner is going offline.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link partner speed</strong>—Speed of the link partner.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local resolution</strong>—Resolution of the autonegotiation process on the local interface:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flow control</strong>—Type of flow control that is used by the local interface. For Gigabit Ethernet interfaces, the types are: Symmetric (link partner supports PAUSE on receive and transmit); Asymmetric (link partner supports PAUSE on transmit); and Symmetric/Asymmetric (link partner supports PAUSE on both receive and transmit or PAUSE only on receive).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Link mode</strong>—Link mode of local interface: either Full-duplex or Half-duplex. Displayed when Negotiation status is Incomplete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Local link speed</strong>—Speed of the local interface. Displayed when Negotiation status is Incomplete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Remote fault</strong>—Remote fault information. Link OK (no error detected on receive), Offline (local interface is offline), and Link Failure (link error detected on receive).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Packet Forwarding Engine configuration</strong></th>
<th>Information about the configuration of the Packet Forwarding Engine:</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Destination slot</strong>—FPC slot number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On standalone switches with built-in interfaces, the slot number refers to the switch itself and is always 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On Virtual Chassis composed of switches with built-in interfaces, the slot number refers to the member ID of the switch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On switches with line cards or on Virtual Chassis composed of switches with line cards, the slot number refers to the line card slot number on the switch or Virtual Chassis.</td>
<td></td>
</tr>
</tbody>
</table>

**Logical Interface**
Table 320: show interfaces ge- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received (input) and transmitted (output) on the specified interface.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

**NOTE:** For logical interfaces on EX Series switches, the traffic statistics fields in `show interfaces` commands show only control traffic; the traffic statistics do not include data traffic.

<table>
<thead>
<tr>
<th>IPv6 transit statistics</th>
<th>EX Series switches do not support the collection and reporting of IPv6 transit statistics.</th>
<th>extensive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local statistics</td>
<td>Number and rate of bytes and packets destined to and from the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Route table in which the logical interface address is located. For example, <code>0</code> refers to the routing table <code>inet.0</code>.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Input Filters</td>
<td>Names of any input filters applied to this interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Output Filters</td>
<td>Names of any output filters applied to this interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

If unicast reverse-path forwarding (RPF) is explicitly configured on the specified interface, the uRPF flag is displayed. If unicast RPF was configured on a different interface (and therefore is enabled on all switch interfaces) but was not explicitly configured on the specified interface, the uRPF flag is not displayed even though unicast RPF is enabled.

| protocol-family       | Protocol family configured on the logical interface. If the protocol is `inet`, the IP address of the interface is also displayed.                                                                          | brief           |
| Flags                 | Information about the address flags.                                                                                                                                                                         | detail extensive none |
Table 320: show interfaces ge- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

```
show interfaces ge-0/0/0

Physical interface: ge-0/0/0, Enabled, Physical link is Down
Interface index: 129, SNMP ifIndex: 21
Remote fault: Online
Device flags     : Present Running Down
Interface flags  : Hardware-Down SNMP-Traps Internal: 0x0
CoS queues       : 8 supported, 8 maximum usable queues
Hold-times       : Up 0 ms, Down 0 ms
Current address  : 00:19:e2:50:3f:41, Hardware address: 00:19:e2:50:3f:41
Last flapped     : 2008-01-16 11:40:53 UTC (4d 02:30 ago)
Input rate       : 0 bps (0 pps)
Output rate      : 0 bps (0 pps)
Ingress rate at Packet Forwarding Engine : 0 bps (0 pps)
Ingress drop rate at Packet Forwarding Engine : 0 bps (0 pps)
Active alarms    : None
Active defects   : None
Logical interface ge-0/0/0.0 (Index 65) (SNMP ifIndex 22)
Flags: SNMP-Traps
Encapsulation: ENET2
Input packets : 0
Output packets: 0
Protocol eth-switch
Flags: None

show interfaces ge-0/0/0 brief

Physical interface: ge-0/0/0, Enabled, Physical link is Down
Description: voice priority and tcp and icmp traffic rate-limiting filter at ingress port
Device flags     : Present Running Down
Interface flags  : Hardware-Down SNMP-Traps Internal: 0x0
Link flags       : None

Logical interface ge-0/0/0.0
```
show interfaces ge-0/0/0 brief (with EEE Enabled on the EEE-capable Base-T copper Ethernet interfaces)

user@switch> show interfaces ge-0/0/0 brief
Physical interface: ge-0/0/0, Enabled, Physical link is Up
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto,
Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled,
Auto-negotiation: Enabled, Remote fault: Online,
IEEE 802.3az Energy Efficient Ethernet: Enabled, NO LPI
Device flags : Present Running
Interface flags: Hardware-Down SNMP-Traps Internal: 0x0
Link flags : None

show interfaces ge-0/0/0 detail

user@switch> show interfaces ge-0/0/0 detail
Physical interface: ge-0/0/0, Enabled, Physical link is Up
Interface index: 193, SNMP ifIndex: 206, Generation: 196
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source Filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:1f:12:30:ff:40, Hardware address: 00:1f:12:30:ff:40
Last flapped : 2009-05-05 06:03:05 UTC (00:22:13 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 0 0 0
1 assured-forw 0 0 0
5 expedited-fo 0 0 0
7 network-cont 0 0 0
Active alarms : None
Active defects : None

Logical interface ge-0/0/0.0 (Index 65) (SNMP ifIndex 235) (Generation 130)
Flags: SNMP-Traps Encapsulation: ENET2
Bandwidth: 0
Traffic statistics:
Input bytes : 0
show interfaces ge-0/0/4 extensive

user@switch> show interfaces ge-0/0/4 extensive
Physical interface: ge-0/0/4, Enabled, Physical link is Up
Interface index: 165, SNMP ifIndex: 152, Generation: 168
Link-level type: Ethernet, MTU: 1514, Speed: Auto, Duplex: Auto,
MAC-REWRITE Error: None, Loopback: Disabled, Source Filtering: Disabled,
Flow control: Enabled, Auto-negotiation: Enabled, Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x0
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:1f:12:33:65:44, Hardware address: 00:1f:12:33:65:44
Last flapped : 2008-09-17 11:02:25 UTC (16:32:54 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 2989761 984 bps
Input packets: 0 0 pps
Output packets: 24307 1 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
FIFO errors: 0, Resource errors: 0
Output errors:
Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,
FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters:

Queue types
0 best-effort 1 assured-forward 5 expedited-forward

<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 assured-forward</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5 expedited-forward</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Active alarms : None
Active defects : None

MAC statistics:

<table>
<thead>
<tr>
<th></th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>0</td>
<td>2989761</td>
</tr>
<tr>
<td>Total packets</td>
<td>0</td>
<td>24307</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>24307</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Autonegotiation information:
Negotiation status: Complete
Link partner:
  Link mode: Full-duplex, Flow control: None, Remote fault: OK,
  Link partner Speed: 1000 Mbps
Local resolution:
  Flow control: None, Remote fault: Link OK
Packet Forwarding Engine configuration:
  Destination slot: 0
  Direction : Output
CoS transmit queue

<table>
<thead>
<tr>
<th>Limit</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>%</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>950000000</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 network-control</td>
<td>5</td>
<td>500000000</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logical interface ge-0/0/4.0 (Index 82) (SNMP ifIndex 184) (Generation 147)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:

Input bytes : 0
Output bytes : 4107883
Input packets: 0
Output packets: 24307
IPv6 transit statistics:

Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:

Input bytes : 0
Output bytes : 4107883
Input packets: 0
Output packets: 24307
Transit statistics:

Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:

Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol eth-switch, Generation: 159, Route table: 0
Flags: None
Input Filters: f2,
Output Filters: f1,..,
show interfaces irb

Syntax

```
show interfaces irb
  <brief | detail | extensive | terse>
  <descriptions>
  <media>
  <routing-instance instance-name>
  <snmp-index snmp-index>
  <statistics>
```

Release Information

Command introduced in Junos OS Release 12.3R2.
Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Command introduced in Junos OS Release 13.2 for the QFX Series

Description

Display integrated routing and bridging interfaces information.

Options

- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `descriptions`—(Optional) Display interface description strings.
- `media`—(Optional) Display media-specific information about network interfaces.
- `routing-instance instance-name`—(Optional) Display information for the interface with the specified SNMP index.
- `snmp-index snmp-index`—(Optional) Display information for the interface with the specified SNMP index.

Additional Information

Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another VLAN that has a Layer 3 protocol configured.

Required Privilege

- `view`

List of Sample Output

- `show interfaces irb extensive on page 2509`
- `show interfaces irb snmp-index on page 2510`

Output Fields

Table 274 on page 2192 lists the output fields for the `show interfaces irb` command. Output fields are listed in the approximate order in which they appear.

Table 321: show interfaces irb Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Enabled</td>
<td>State of the physical interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Table 321: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proto</td>
<td>Protocol configured on the interface.</td>
<td>terse</td>
</tr>
<tr>
<td>Interface index</td>
<td>Physical interface index number, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Type</td>
<td>Physical interface type.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>MTU</td>
<td>MTU size on the physical interface.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>Clocking</td>
<td>Reference clock source: Internal or External. Always unspecified on IRB interfaces.</td>
<td>detail extensive brief</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running. Always unspecified on IRB interfaces.</td>
<td>detail extensive brief</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device. Possible values are described in the “Device Flags” section under Common Output Fields Description.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface. Possible values are described in the “Interface Flags” section under Common Output Fields Description.</td>
<td>detail extensive brief none</td>
</tr>
<tr>
<td>Link type</td>
<td>Physical interface link type: full duplex or half duplex.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link. Possible values are described in the “Links Flags” section under Common Output Fields Description.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Physical Info</td>
<td>Physical interface information.</td>
<td>All levels</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Hardware address</td>
<td>MAC address of the hardware.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Alternate link address</td>
<td>Backup address of the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hours:minutes:seconds timezone (hours:minutes:seconds ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface were last set to zero.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 321: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Input bytes</strong>—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Output bytes</strong>—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Input packets</strong>—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Output packets</strong>—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Errors</strong>—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Drops</strong>—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Framing errors</strong>—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Runt</strong>s—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Giants</strong>—Number of frames received that are larger than the giant threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Policed discards</strong>—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>Carrier transitions</strong>—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the DPC is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

**Logical Interface**
Table 321: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface (which reflects its initialization sequence).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number of the logical interface.</td>
<td>none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>“Logical Interface Flags” section under Common Output Fields Description.</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Speed at which the interface is running.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Routing instance IRB is configured under.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Bridging Domain</td>
<td>Bridging domain IRB is participating in.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the logical</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>Number of IPv6 transit bytes and packets received and transmitted on the logical</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>interface if IPv6 statistics tracking is enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Statistics for traffic received from and transmitted to the Routing Engine.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Statistics for traffic transiting the router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family configured on the local interface. Possible values are described</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>in the “Protocol Field” section under Common Output Fields Description.</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Maximum labels</td>
<td>Maximum number of MPLS labels configured for the MPLS protocol family on the</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>logical interface.</td>
<td>none</td>
</tr>
</tbody>
</table>
Table 321: show interfaces irb Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about address flags. Possible values are described in the &quot;Addresses Flags&quot; section under Common Output Fields Description.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Policer</td>
<td>The policer that is to be evaluated when packets are received or transmitted on the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface. Possible values are described in the &quot;Logical Interface Flags&quot; section under Common Output Fields Description.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

show interfaces irb extensive

user@host> show interfaces irb extensive
Physical interface: irb, Enabled, Physical link is Up
    Interface index: 129, SNMP ifIndex: 23, Generation: 130
    Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified, Speed: Unspecified
    Device flags   : Present Running
    Interface flags: SNMP-Traps
    Link type      : Full-Duplex
    Link flags     : None
    Physical info  : Unspecified
    Hold-times     : Up 0 ms, Down 0 ms
    Current address: 02:00:00:00:00:30, Hardware address: 02:00:00:00:00:30
    Alternate link address: Unspecified
    Last flapped   : Never
    Statistics last cleared: Never
    Traffic statistics:
        Input bytes : 0
        Output bytes : 0
        Input packets: 0
        Output packets: 0
    IPv6 transit statistics:
        Input bytes : 0
        Output bytes : 0
        Input packets: 0
        Output packets: 0
    Input errors:
        Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0, Resource errors: 0
    Output errors:
        Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0

Logical interface irb.0 (Index 68) (SNMP ifIndex 70) (Generation 143)
    Flags: Hardware-Down SNMP-Traps 0x4000 Encapsulation: ENET2
    Bandwidth: 1000mbps
    Routing Instance: customer_0 Bridging Domain: bd0
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 0  0 bps
Output bytes : 0  0 bps
Input packets: 0  0 pps
Output packets: 0  0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, MTU: 1500, Generation: 154, Route table: 0
 Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
   Destination: 10.51.1/24, Local: 10.51.1.2, Broadcast: 10.51.1.255,
   Generation: 155
Protocol multiservice, MTU: 1500, Generation: 155, Route table: 0
 Flags: Is-Primary
 Policer: Input: __default_arp_policer

show interfaces irb snmp-index

user@host> show interfaces irb snmp-index 25
Physical interface: irb, Enabled, Physical link is Up
 Interface index: 128, SNMP ifIndex: 25
 Type: Ethernet, Link-level type: Ethernet, MTU: 1514
 Device flags : Present Running
 Interface flags: SNMP-Traps
 Link type : Full-Duplex
 Link flags : None
 Current address: 02:00:00:00:00:30, Hardware address: 02:00:00:00:00:30
 Last flapped : Never
 Input packets : 0
 Output packets: 0

Logical interface irb.0 (Index 68) (SNMP ifIndex 70)
 Flags: Hardware-Down SNMP-Traps Ox4000 Encapsulation: ENET2
 Bandwidth: 1000mbps
 Routing Instance: customer_0 Bridging Domain: bd0
 Input packets : 0
 Output packets: 0
 Protocol inet, MTU: 1500
 Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
   Destination: 10.51.1/24, Local: 10.51.1.2, Broadcast: 10.51.1.255
 Protocol multiservice, MTU: 1500
 Flags: Is-Primary
**show interfaces me0**

**Syntax**

```
show interfaces me0
<brief | detail | extensive | terse>
<descriptions>
<media>
<routing-instance>
<statistics>
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display status information about the management Ethernet interface.

**Options**

- **none**—Display standard information about the management Ethernet interface.
- **brief | detail | extensive | terse**—(Optional) Display the specified level of output.
- **descriptions**—(Optional) Display interface description strings.
- **media**—(Optional) Display media-specific information about network interfaces.
- **routing-instance**—(Optional) Display the name of the routing instance.
- **statistics**—(Optional) Display static interface statistics.

**Required Privilege**

`view`

**Related Documentation**

- Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch on page 4179
- Configuring Firewall Filters (CLI Procedure) on page 4192

**List of Sample Output**

- `show interfaces me0` on page 2515
- `show interfaces me0 brief` on page 2515
- `show interfaces me0 detail` on page 2515
- `show interfaces me0 extensive` on page 2516

**Output Fields**

Table 322 on page 2511 lists the output fields for the `show interfaces me0` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Physical interface</strong></td>
<td>Name of the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>State of the interface; <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface index</strong></td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
<td><strong>detail extensive</strong> none</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Table 322: show interfaces me0 Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP ifindex</td>
<td>SNMP index number for the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Description</td>
<td>Optional user-specified description.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>Type</td>
<td>Information about the type of functional interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface. The default is 1514.</td>
<td>All levels</td>
</tr>
<tr>
<td>Clocking</td>
<td>Interface that acts as a clock source. This field is not supported on EX Series switches and the default value is always <strong>Unspecified</strong>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>All levels</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface flags</td>
<td>Information about the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link type</td>
<td>Information about whether the link is duplex and whether the negotiation is manual or automatic.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Physical info</td>
<td>Information about the device dependent physical interface selector. This field is applied only when a clocking option is specified. This field is not supported on EX Series switches and the default value is always <strong>Unspecified</strong>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in milliseconds.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Hardware address</td>
<td>MAC address of the hardware.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Alternate link address</td>
<td>Information about alternate hardware address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from down to up. The format is <strong>Last flapped: year-month-day hour:minute:second timezone (weeks:days:hour:minute:second ago)</strong>. For example, Last flapped: 2008–01–16 10:52:40 UTC (3w:3d 22:58 ago).</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Time when the statistics for the interface was last set to zero. The format is <strong>Last flapped: year-month-day hour:minute:second timezone (weeks:days:hour:minute:second ago)</strong>. For example, Last flapped: 2008–01–16 10:52:40 UTC (3w:3d 22:58 ago).</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 322: show interfaces me0 Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>Following are fields in Traffic statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>Number and rate of bytes and IPv6 packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>Following are fields in IPv6 transit statistics:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface.</td>
<td></td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Errors—Sum of the incoming frame aborts and frame checksum (FCS) errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped by the input queue of the I/O Manager ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Framing errors—Number of packets received with an invalid FCS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Runts—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Giants—Number of packets that exceed the size for the medium. For example, if the medium is Ethernet, the Giant field shows the count of packets with size greater than 1518 bytes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource errors—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Output errors</td>
<td>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Carrier transitions—Number of times the interface has gone from down to up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This number does not normally increment quickly. It increases only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increment quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Errors—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Drops—Number of packets dropped by the output queue of the I/O Manager ASIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MTU errors—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Resource errors—Sum of transmit drops.</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Table 322: show interfaces me0 Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifindex</td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received (input) and transmitted (output) on the specified interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>IPv6 transit statistics</td>
<td>If IPv6 statistics tracking is enabled, number of IPv6 bytes and packets received and transmitted on the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local statistics</td>
<td>Number and rate of bytes and packets destined to and exiting from the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Table</td>
<td>Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input Filter</td>
<td>Ingress filter name.</td>
<td>extensive</td>
</tr>
<tr>
<td>Output Filter</td>
<td>Egress filter name.</td>
<td>extensive</td>
</tr>
<tr>
<td>Addresses</td>
<td>Information about the management interface addresses.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the address flags.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Sample Output

show interfaces me0

user@switch> show interfaces me0
Physical interface: me0, Enabled, Physical link is Up
  Interface index: 1, SNMP ifIndex: 33
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps
  Device flags : Present Running
  Interface flags: SNMP-Traps
  Link type : Full-Duplex
  Current address: 00:1f:12:35:3c:bf, Hardware address: 00:1f:12:35:3c:bf
  Last flapped : 2010-07-31 23:45:50 PDT (5d 00:32 ago)
    Input packets : 1661830
    Output packets: 3200

Logical interface me0.0 (Index 3) (SNMP ifIndex 34)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets : 1661830
  Output packets: 3200
  Protocol inet
    Flags: Is-Primary
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 10.204.32/20, Local: 10.204.33.103,
      Broadcast: 10.204.47.255
  Protocol inet6
    Flags: Is-Primary
    Addresses, Flags: Is-Preferred
      Destination: fe80::/64, Local: fe80::21f:12ff:fe35:3cbf

show interfaces me0 brief

user@switch> show interfaces me0 brief
Physical interface: me0, Enabled, Physical link is Up
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 1000mbps
  Device flags : Present Running
  Interface flags: SNMP-Traps

Logical interface me0.0
  Flags: SNMP-Traps Encapsulation: ENET2
  inet 10.204.33.103/20
  inet6 fe80::21f:12ff:fe35:3cbf/64

show interfaces me0 detail

user@switch> show interfaces me0 detail
Physical interface: me0, Enabled, Physical link is Up
  Interface index: 1, SNMP ifIndex: 33, Generation: 1
  Type: Ethernet, Link-level type: Ethernet, MTU: 1514, Clocking: Unspecified,
  Speed: 1000mbps
  Device flags : Present Running
  Interface flags: SNMP-Traps
  Link type : Full-Duplex
  Physical info : Unspecified
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:1f:12:35:3c:bf, Hardware address: 00:1f:12:35:3c:bf
  Alternate link address: Unspecified
  Last flapped : 2010-07-31 23:45:50 PDT (5d 00:37 ago)
  Statistics last cleared: Never
Traffic statistics:
| Input bytes | 366663167 |
| Output bytes | 498590 |
| Input packets | 1664031 |
| Output packets | 3259 |

IPv6 transit statistics:
| Input bytes | 0 |
| Output bytes | 0 |
| Input packets | 0 |
| Output packets | 0 |

Logical interface me0.0 (Index 3) (SNMP ifIndex 34) (Generation 1)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
| Input bytes | 36665637 |
| Output bytes | 500569 |
| Input packets | 1664048 |
| Output packets | 3275 |

IPv6 transit statistics:
| Input bytes | 0 |
| Output bytes | 0 |
| Input packets | 0 |
| Output packets | 0 |

Local statistics:
| Input bytes | 366665637 |
| Output bytes | 500569 |
| Input packets | 1664048 |
| Output packets | 3275 |

Protocol inet, Generation: 1, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Preferred Is-Primary
Destination: 10.204.32/20, Local: 10.204.33.103, Broadcast: 10.204.47.255, Generation: 1

Protocol inet6, Generation: 2, Route table: 0
Flags: Is-Primary
Addresses, Flags: Is-Preferred
Destination: fe80::/64, Local: fe80::21f:12ff:fe35:3cbf, Generation: 2
Input bytes : 0
Output bytes : 0
Input packets : 0
Output packets : 0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0
Logical interface me0.0 (Index 3) (SNMP ifIndex 34) (Generation 1)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
  Input bytes : 82310392
  Output bytes : 1966952
  Input packets : 110453
  Output packets : 17747
Local statistics:
  Input bytes : 82310392
  Output bytes : 1966952
  Input packets : 110453
  Output packets : 17747
Protocol inet, Generation: 1, Route table: 0
  Flags: Is-Primary
  Input Filters: mgmt_filter,
  Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 10.204.96/20, Local: 10.204.96.234,
    Broadcast: 10.204.111.255, Generation: 1
show interfaces queue

Syntax

show interfaces queue
<both-ingress-egress>
<egress>
<forwarding-class forwarding-class>
<ingress>
@interface-name>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display class-of-service (CoS) queue information for physical interfaces.

Options

none—Show detailed CoS queue statistics for all physical interfaces.

both-ingress-egress—(Optional) Show both ingress and egress queue statistics. (Ingress statistics are not available for all interfaces.)

egress—(Optional) Show egress queue statistics only.

forwarding-class forwarding-class—(Optional) Show queue statistics only for the specified forwarding class.

ingress—(Optional) Show ingress queue statistics only. (Ingress statistics are not available for all interfaces.)

@interface-name—(Optional) Show queue statistics for the specified interface.

Required Privilege Level

view

Related Documentation

- Monitoring Interface Status and Traffic on page 2463
- Monitoring Interfaces That Have CoS Components on page 1978
- Defining CoS Schedulers and Scheduler Maps (CLI Procedure) on page 1929
- Configuring CoS Traffic Classification for Ingress Queuing on Oversubscribed Ports on EX8200 Line Cards (CLI Procedure) on page 1945

List of Sample Output

show interfaces queue ge-0/0/0 (EX2200 Switch) on page 2520
show interfaces queue xe-6/0/39 (Line Card with Oversubscribed Ports in an EX8200 Switch) on page 2521

Output Fields

Table 323 on page 2518 lists the output fields for the show interfaces queue command. Output fields are listed in the approximate order in which they appear.

Table 323: show interfaces queue Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical interface</td>
<td>Name of the physical interface.</td>
</tr>
</tbody>
</table>
Table 323: show interfaces queue Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>State of the interface. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Administratively down, Physical link is Down</strong>—The interface is turned off, and the physical link is inoperable.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Administratively down, Physical link is Up</strong>—The interface is turned off, but the physical link is operational and can pass packets when it is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled, Physical link is Down</strong>—The interface is turned on, but the physical link is inoperable and cannot pass packets.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled, Physical link is Up</strong>—The interface is turned on, and the physical link is operational and can pass packets.</td>
</tr>
<tr>
<td>Interface index</td>
<td>Index number of the physical interface, which reflects its initialization sequence.</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP index number for the physical interface.</td>
</tr>
<tr>
<td>Description</td>
<td>User-configured interface description.</td>
</tr>
<tr>
<td>Forwarding classes</td>
<td>Number of forwarding classes supported and in use for the interface.</td>
</tr>
<tr>
<td>Ingress queues</td>
<td>Number of input queues supported and in use on the specified interface. For an interface on a line card with oversubscribed ports, the ingress queue handles low priority traffic on the interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Transmission statistics for the queue:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Packets</strong>—Number of packets transmitted by this queue.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bytes</strong>—Number of bytes transmitted by this queue.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Tail-dropped packets</strong>—Number of packets dropped because the queue buffers were full.</td>
</tr>
<tr>
<td>PFE chassis queues</td>
<td>For an interface on a line card with oversubscribed ports, the number of Packet Forwarding Engine chassis queues supported and in use for the port group to which the interface belongs. The Packet Forwarding Engine chassis queue for a port group handles high priority traffic from all the interfaces in the port group.</td>
</tr>
<tr>
<td>Egress queues</td>
<td>Number of output queues supported and in use on the specified interface.</td>
</tr>
<tr>
<td>Queue</td>
<td>CoS queue number.</td>
</tr>
<tr>
<td>Queued</td>
<td>This counter is not supported on EX Series switches.</td>
</tr>
</tbody>
</table>
Table 323: show interfaces queue Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmitted</td>
<td>Number of packets and bytes transmitted by this queue. Information on transmitted packets and bytes can include:</td>
</tr>
<tr>
<td></td>
<td>• Packets—Number of packets transmitted.</td>
</tr>
<tr>
<td></td>
<td>• Bytes—Number of bytes transmitted.</td>
</tr>
<tr>
<td></td>
<td>• Tail-dropped packets—Number of arriving packets dropped because output queue buffers were full.</td>
</tr>
<tr>
<td></td>
<td>• RED-dropped packets—Number of packets dropped because of random early detection (RED).</td>
</tr>
<tr>
<td></td>
<td>• Low—Number of low loss priority packets dropped because of RED.</td>
</tr>
<tr>
<td></td>
<td>• High—Number of high loss priority packets dropped because of RED.</td>
</tr>
<tr>
<td></td>
<td>• RED-dropped bytes—Number of bytes dropped because of random early detection (RED).</td>
</tr>
<tr>
<td></td>
<td>• Low—Number of low loss priority bytes dropped because of RED.</td>
</tr>
<tr>
<td></td>
<td>• High—Number of high loss priority bytes dropped because of RED.</td>
</tr>
</tbody>
</table>

Packet Forwarding Engine Chassis Queues

For an interface on a line card with oversubscribed ports, the number of Packet Forwarding Engine chassis queues supported and in use for the port group to which the interface belongs. The queue statistics reflect the traffic flowing on all the interfaces in the port group.

Sample Output

show interfaces queue ge-0/0/0 (EX2200 Switch)

```
user@switch>  show interfaces queue ge–0/0/0
Physical interface: ge-0/0/0, Enabled, Physical link is Down
            Interface index: 130, SNMP ifIndex: 501
            Forwarding classes: 16 supported, 4 in use
            Egress queues: 8 supported, 4 in use
            Queue: 0, Forwarding classes: best-effort
            Queued:
            Transmitted:
            Packets : 0
            Bytes : 0
            Tail-dropped packets : 0
            Queue: 1, Forwarding classes: assured-forwarding
            Queued:
            Transmitted:
            Packets : 0
            Bytes : 0
            Tail-dropped packets : 0
            Queue: 5, Forwarding classes: expedited-forwarding
            Queued:
            Transmitted:
            Packets : 0
            Bytes : 0
            Tail-dropped packets : 0
            Queue: 7, Forwarding classes: network-control
            Queued:
            Transmitted:
            Packets : 0
```
show interfaces queue xe-6/0/39 (Line Card with Oversubscribed Ports in an EX8200 Switch)

<table>
<thead>
<tr>
<th>Bytes</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tail-dropped packets</td>
<td>0</td>
</tr>
</tbody>
</table>

```
user@switch> show interfaces queue xe-6/0/39

Physical interface: xe-6/0/39, Enabled, Physical link is Up
  Interface index: 291, SNMP ifIndex: 1641
  Forwarding classes: 16 supported, 7 in use
  Ingress queues: 1 supported, 1 in use
    Transmitted:
      Packets : 337069086018
      Bytes   : 43144843010304
      Tail-dropped packets : 8003867575
  PFE chassis queues: 1 supported, 1 in use
    Transmitted:
      Packets : 0
      Bytes   : 0
      Tail-dropped packets : 0
  Forwarding classes: 16 supported, 7 in use
  Egress queues: 8 supported, 7 in use
    Queue: 0, Forwarding classes: best-effort
      Queued:
      Transmitted:
        Packets : 334481399932
        Bytes   : 44151544791024
        Tail-dropped packets : 0
      Queue: 1, Forwarding classes: assured-forwarding
      Queued:
      Transmitted:
        Packets : 0
        Bytes   : 0
        Tail-dropped packets : 0
      Queue: 2, Forwarding classes: mcast-be
      Queued:
      Transmitted:
        Packets : 274948977
        Bytes   : 36293264964
        Tail-dropped packets : 0
      Queue: 4, Forwarding classes: mcast-ef
      Queued:
      Transmitted:
        Packets : 0
        Bytes   : 0
        Tail-dropped packets : 0
      Queue: 5, Forwarding classes: expedited-forwarding
      Queued:
      Transmitted:
        Packets : 0
        Bytes   : 0
        Tail-dropped packets : 0
      Queue: 6, Forwarding classes: mcast-af
      Queued:
      Transmitted:
        Packets : 0
        Bytes   : 0
        Tail-dropped packets : 0
      Queue: 7, Forwarding classes: network-control
      Queued:
      Transmitted:
```
<table>
<thead>
<tr>
<th>Packet Count</th>
<th>Bytes</th>
<th>Tail-dropped Packets</th>
<th>RED-dropped Packets</th>
<th>Low</th>
<th>High</th>
<th>RED-dropped Bytes</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packets</strong></td>
<td>46714</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Bytes</strong></td>
<td>6901326</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tail-dropped Packets</strong></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Packet Forwarding Engine Chassis Queues:**

Queue: 0, Forwarding classes: best-effort

**Queued:**

**Transmitted:**
- Packets: 739338141426
- Bytes: 94635282101928
- Tail-dropped packets: 0
- RED-dropped packets: 5606426444
- Low: 5606426444
- High: 0
- RED-dropped bytes: 683262846464
- Low: 683262846464
- High: 0

Queue: 1, Forwarding classes: assured-forwarding

**Queued:**

**Transmitted:**
- Packets: 0
- Bytes: 0
- Tail-dropped packets: 0
- RED-dropped packets: 0
- Low: 0
- High: 0
- RED-dropped bytes: 0
- Low: 0
- High: 0

Queue: 2, Forwarding classes: mcast-be

**Queued:**

**Transmitted:**
- Packets: 0
- Bytes: 0
- Tail-dropped packets: 0
- RED-dropped packets: 0
- Low: 0
- High: 0
- RED-dropped bytes: 0
- Low: 0
- High: 0

Queue: 4, Forwarding classes: mcast-ef

**Queued:**

**Transmitted:**
- Packets: 0
- Bytes: 0
- Tail-dropped packets: 0
- RED-dropped packets: 0
- Low: 0
- High: 0
- RED-dropped bytes: 0
- Low: 0
- High: 0

Queue: 5, Forwarding classes: expedited-forwarding

**Queued:**

**Transmitted:**
- Packets: 0
- Bytes: 0
- Tail-dropped packets: 0
- RED-dropped packets: 0
Queue: 6, Forwarding classes: mcast-af
  Queued:
  Transmitted:
    Packets : 0
    Bytes : 0
    Tail-dropped packets : 0
    RED-dropped packets : 0
    Low : 0
    High : 0
    RED-dropped bytes : 0
    Low : 0
    High : 0

Queue: 7, Forwarding classes: network-control
  Queued:
  Transmitted:
    Packets : 97990
    Bytes : 14987506
    Tail-dropped packets : 0
    RED-dropped packets : 0
    Low : 0
    High : 0
    RED-dropped bytes : 0
    Low : 0
    High : 0
show interfaces xe-

Syntax

```
show interfaces xe-fpc/pic/port
<brief | detail | extensive | terse>
<media>
<statistics>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display status information about the specified 10-Gigabit Ethernet interface.

**NOTE:** You must have a transceiver plugged into an SFP+ or an XFP port before information about the interface can be displayed.

**NOTE:** On an EX Series switch, the traffic statistics for a LAG might vary slightly from the cumulative traffic statistics of the member interfaces of the LAG. This difference is more likely to be seen when the traffic is bursty in nature, and because the statistics are not fetched from the LAG and the members in the same instant. For accurate traffic statistics for a LAG, use the aggregated Ethernet counters.

Options

```
xepc/pic/port — Display standard information about the specified 10-Gigabit Ethernet interface.

brief | detail | extensive | terse — (Optional) Display the specified level of output.

media — (Optional) Display media-specific information about network interfaces. For 10-Gigabit Ethernet interfaces, using the media option does not provide you with new or additional information. The output is the same as when the media option is not used.

statistics — (Optional) Display static interface statistics. For 10-Gigabit Ethernet interfaces, using the statistics option does not provide you with new or additional information. The output is the same as when the statistics option is not used.
```

Required Privilege Level

view

Related Documentation

- Monitoring Interface Status and Traffic on page 2463
- Troubleshooting Network Interfaces on EX3200 Switches
- Troubleshooting Network Interfaces on EX4200 Switches
- Troubleshooting an Aggregated Ethernet Interface on page 2545
- Junos OS Ethernet Interfaces Configuration Guide
List of Sample Output

- `show interfaces xe-4/1/0` on page 2533
- `show interfaces xe-0/1/0 brief` on page 2534
- `show interfaces xe-4/1/0 detail` on page 2534
- `show interfaces xe-6/0/39 extensive` on page 2535

**Output Fields**

Table 324 on page 2525 lists the output fields for the `show interfaces xe-` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fields for the Terse Output Level Only</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the physical or logical interface.</td>
<td>terse</td>
</tr>
<tr>
<td>Admin</td>
<td>Administrative state of the interface.</td>
<td>terse</td>
</tr>
<tr>
<td>Link</td>
<td>State of the physical link.</td>
<td>terse</td>
</tr>
<tr>
<td>Proto</td>
<td>Protocol family configured on the logical interface.</td>
<td>terse</td>
</tr>
<tr>
<td>Local</td>
<td>Local IP address of the logical interface.</td>
<td>terse</td>
</tr>
<tr>
<td>Remote</td>
<td>Remote IP address of the logical interface.</td>
<td>terse</td>
</tr>
</tbody>
</table>

| **Fields for the Physical Interface** |                                   |                 |
| Physical interface | Name of the physical interface.                                                   | brief detail extensive none |

| Enabled      | State of the interface. Can be one of the following:                              | brief detail extensive none |
|             | • Administratively down, Physical link is Down—The interface is turned off, and the physical link is inoperable and cannot pass packets even when it is enabled. |
|             | • Administratively down, Physical link is Up—The interface is turned off, but the physical link is operational and can pass packets when it is enabled. |
|             | • Enabled, Physical link is Down—The interface is turned on, but the physical link is inoperable and cannot pass packets. |
|             | • Enabled, Physical link is Up—The interface is turned on, and the physical link is operational and can pass packets. |

| Interface index | Index number of the physical interface, which reflects its initialization sequence. | detail extensive none |
| SNMP ifIndex    | SNMP index number for the physical interface.                                      | detail extensive none |

| Generation     | Unique number for use by Juniper Networks technical support only.                 | detail extensive    |
Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>User-configured interface description.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Link-level type</td>
<td>Encapsulation being used on the physical interface.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size on the physical interface.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Speed</td>
<td>Speed at which the interface is running.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Duplex</td>
<td>Duplex mode of the interface.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>BPDU Error</td>
<td>Not supported on EX Series switches.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>MAC-REWRITE Error</td>
<td>Not supported on EX Series switches.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Loopback</td>
<td>Loopback status: Enabled or Disabled. If loopback is enabled, type of loopback: Local or Remote.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Source filtering</td>
<td>Source filtering status: Enabled or Disabled.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Flow control</td>
<td>Flow control status: Enabled or Disabled.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Device flags</td>
<td>Information about the physical device.</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td></td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
</tbody>
</table>
Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface flags</td>
<td>Information about the interface.</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive none</td>
</tr>
<tr>
<td>Link flags</td>
<td>Information about the link.</td>
<td>brief detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive none</td>
</tr>
<tr>
<td>CoS queues</td>
<td>Number of CoS queues configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Hold-times</td>
<td>Current interface hold-time up and hold-time down, in</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>milliseconds.</td>
<td>none</td>
</tr>
<tr>
<td>Current address</td>
<td>Configured MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Hardware address</td>
<td>Hardware MAC address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the interface went from</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>down to up.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>The format is year-month-day hour:minute:second timezone (weeksdays hours:minutes:seconds ago). For example, 2008-01-16 10:52:40 UTC (3d 22:58 ago).</td>
<td></td>
</tr>
<tr>
<td>Input Rate</td>
<td>Input rate in bits per second (bps) and packets per</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>second (pps).</td>
<td>none</td>
</tr>
<tr>
<td>Output Rate</td>
<td>Output rate in bps and pps.</td>
<td>none</td>
</tr>
<tr>
<td>Statistics last cleared</td>
<td>Date, time, and how long ago the statistics for the interface were cleared. The format is year-month-day hour:minute:second timezone (weeksdays hours:minutes:seconds ago). For example, 2010-05-17 07:51:28 PDT (00:04:33 ago).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received and transmitted on the physical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Input bytes—Number of bytes received on the interface and rate in bits per second.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output bytes—Number of bytes transmitted on the interface and rate in bits per second.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input packets—Number of packets received on the interface and rate in packets per second.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Output packets—Number of packets transmitted on the interface and rate in packets per second.</td>
<td></td>
</tr>
</tbody>
</table>
Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 transit statistics</td>
<td>EX Series switches do not support the collection and reporting of IPv6 transit statistics.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Input errors</td>
<td>Input errors on the interface:</td>
<td>extensive</td>
</tr>
<tr>
<td>• Errors—Sum of the incoming frame aborts and FCS errors.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Framing errors—Number of packets received with an invalid frame checksum (FCS).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Runs—Number of frames received that are smaller than the runt threshold.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• L3 incompletes—Number of incoming packets discarded because they failed Layer 3 sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored if you configure the ignore-l3-incompletes statement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• L2 channel errors—Number of times the software did not find a valid logical interface for an incoming frame.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• L2 mismatch timeouts—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FIFO errors—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Resource errors—Sum of transmit drops.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output errors</td>
<td>Output errors on the interface:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Carrier transitions</strong>—Number of times the interface has gone from <strong>down</strong> to <strong>up</strong>. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Errors</strong>—Sum of the outgoing frame aborts and FCS errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Drops</strong>—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Collisions</strong>—Number of Ethernet collisions. A 10-Gigabit Ethernet interface supports only full-duplex operation, so for 10-Gigabit Ethernet interfaces, this number should always remain 0. If it is nonzero, there is a software bug.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Aged packets</strong>—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>FIFO errors</strong>—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>HS link CRC errors</strong>—Number of errors on the high-speed links between the ASICs responsible for handling the switch interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU errors</strong>—Number of packets whose size exceeded the MTU of the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Resource errors</strong>—Sum of transmit drops.</td>
<td></td>
</tr>
<tr>
<td>Ingress queues</td>
<td>Number of CoS ingress queues supported on the specified interface. Displayed only for an interface on a line card with oversubscribed ports.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Egress queues</td>
<td>Number of CoS egress queues supported on the specified interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>PFE Egress queues</td>
<td>Number of Packet Forwarding Engine egress queues shared by the interfaces in a port group. Displayed only for an interface on a line card with oversubscribed ports.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Queue counters</td>
<td>Statistics for queues:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Queued packets</strong>—Number of queued packets. This counter is not supported on EX switches and always contains 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Transmitted packets</strong>—Number of transmitted packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Dropped packets</strong>—Number of packets dropped by the ASIC’s RED mechanism.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active alarms and</td>
<td>Ethernet-specific defects that can prevent the interface from passing packets.</td>
<td>detail</td>
</tr>
<tr>
<td>Active defects</td>
<td>When a defect persists for a certain amount of time, it is promoted to an alarm.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>Based on the switch configuration, an alarm can ring the red or yellow alarm</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>bell on the switch or turn on the red or yellow alarm LED on the front of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch. These fields can contain the value None or Link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• None—There are no active defects or alarms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link—Interface has lost its link state, which usually means that the cable is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unplugged, the far-end system has been turned off, or the PIC is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>malfunctioning.</td>
<td></td>
</tr>
<tr>
<td>MAC statistics</td>
<td>Receive and Transmit statistics reported by the PIC’s MAC subsystem.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Total octets and total packets—Total number of octets and packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unicast packets, Broadcast packets, and Multicast packets—Number of unicast,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>broadcast, and multicast packets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CRC/Align errors—Total number of packets received that had a length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(excluding framing bits, but including FCS octets) of between 64 and 1518</td>
<td></td>
</tr>
<tr>
<td></td>
<td>octets, inclusive, and had either a bad FCS with an integral number of octets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FIFO error—Number of FIFO errors that are reported by the ASIC on the PIC.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If this value is ever nonzero, the PIC is probably malfunctioning.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC control frames—Number of MAC control frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MAC pause frames—Number of MAC control frames with pause operational code.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Oversized frames—Number of frames that exceed 1518 octets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Jabber frames—Number of frames that were longer than 1518 octets (excluding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>framing bits, but including FCS octets), and had either an FCS error or an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>alignment error. This definition of jabber is different from the definition in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These</td>
<td></td>
</tr>
<tr>
<td></td>
<td>documents define jabber as the condition in which any packet exceeds 20 ms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The allowed range to detect jabber is from 20 ms to 150 ms.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fragment frames—Total number of packets that were less than 64 octets in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>length (excluding framing bits, but including FCS octets), and had either an</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FCS error or an alignment error. Fragment frames normally increment because both</td>
<td></td>
</tr>
<tr>
<td></td>
<td>runts (which are normal occurrences caused by collisions) and noise hits are</td>
<td></td>
</tr>
<tr>
<td></td>
<td>counted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Code violations—Number of times an event caused the PHY to indicate “Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reception error” or “invalid data symbol error.”</td>
<td></td>
</tr>
<tr>
<td>Packet Forwarding</td>
<td>Information about the configuration of the Packet Forwarding Engine:</td>
<td>extensive</td>
</tr>
<tr>
<td>Engine configuration</td>
<td>• Destination slot—FPC slot number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On standalone switches with built-in interfaces, the slot number refers to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the switch itself and is always 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On Virtual Chassis composed of switches with built-in interfaces, the slot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>number refers to the member ID of the switch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On switches with line cards or on Virtual Chassis composed of switches with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>line cards, the slot number refers to the line card slot number on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>switch or Virtual Chassis.</td>
<td></td>
</tr>
</tbody>
</table>
Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CoS Information</strong></td>
<td>Scheduler information for the CoS egress queues on the physical interface:</td>
<td>extensive</td>
</tr>
<tr>
<td>• <strong>Direction</strong>—Queue direction, always Output.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>CoS transmit queue</strong>—Queue number and its associated user-configured</td>
<td></td>
<td></td>
</tr>
<tr>
<td>forwarding class name.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Bandwidth</strong>—Information about bandwidth allocated to the queue:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• %—Bandwidth allocated to the queue as a percentage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• bps—Bandwidth allocated to the queue in bps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Buffer</strong>—Information about buffer space allocated to the queue:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• %—Buffer space allocated to the queue as a percentage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• usec—Buffer space allocated to the queue in microseconds. This value is</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nonzero only if the buffer size is configured in terms of time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Priority</strong>—Queue priority: low or high.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Limit</strong>—Displayed if rate limiting is configured for the queue. Possible</td>
<td></td>
<td></td>
</tr>
<tr>
<td>values are none and exact. If exact is configured, the queue transmits only up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to the configured bandwidth, even if excess bandwidth is available. If none is</td>
<td></td>
<td></td>
</tr>
<tr>
<td>configured, the queue transmits beyond the configured bandwidth if bandwidth is</td>
<td></td>
<td></td>
</tr>
<tr>
<td>available.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fields for MACSec statistics**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected Packets</td>
<td>The number of packets sent from the interface that were secured using MACSec when encryption was</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>disabled.</td>
<td>extensive</td>
</tr>
<tr>
<td>Encrypted Packets</td>
<td>The number of packets sent from the interface that were secured and encrypted using MACSec.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td>Protected Bytes</td>
<td>The number of bytes sent from the interface that were secured using MACSec, but not encrypted.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td>Encrypted Bytes</td>
<td>The number of packets sent from the interface that were secured and encrypted using MACSec.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>extensive</td>
</tr>
<tr>
<td>Accepted Packets</td>
<td>The number of received packets that have been accepted on the interface. A packet is considered</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>accepted for this counter when it has been received by this interface and it has passed the</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>MACSec integrity check. This counter increments for traffic that is and is not encrypted using</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MACSec.</td>
<td></td>
</tr>
<tr>
<td>Validated Bytes</td>
<td>The number of bytes that have been validated by the MACSec integrity check and received on the</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>Decrypted Bytes</td>
<td>The number of bytes received on the interface that have been decrypted. An encrypted byte has to</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>be decrypted before it can be received on the receiving interface. The decrypted bytes counter</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>is incremented for received traffic that was encrypted using MACSec.</td>
<td></td>
</tr>
</tbody>
</table>

**Fields for Logical Interfaces**
### Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical interface</td>
<td>Name of the logical interface.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of the logical interface, which reflects its initialization sequence.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>SNMP ifIndex</td>
<td>SNMP interface index number for the logical interface.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Description</td>
<td>User-configured description of the interface.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the logical interface.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Encapsulation on the logical interface.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Traffic statistics</td>
<td>Number and rate of bytes and packets received (input) and transmitted (output) on the specified interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For logical interfaces on EX Series switches, the traffic statistics fields in <code>show interfaces</code> commands show only control traffic; the traffic statistics do not include data traffic.</td>
<td></td>
</tr>
<tr>
<td>Local statistics</td>
<td>Number and rate of bytes and packets destined to and from the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td>Transit statistics</td>
<td>Number and rate of bytes and packets transiting the switch.</td>
<td>extensive</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol family.</td>
<td>detail extensive none</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

2532  Copyright © 2013, Juniper Networks, Inc.
Table 324: show interfaces xe- Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Table</td>
<td>Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>none</td>
</tr>
<tr>
<td>Input Filters</td>
<td>Names of any input filters applied to this interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Output Filters</td>
<td>Names of any output filters applied to this interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about protocol family flags.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>If unicast reverse-path forwarding (RPF) is explicitly configured on the specified interface, the uRPF flag is displayed. If unicast RPF was configured on a different interface (and therefore is enabled on all switch interfaces) but was not explicitly configured on the specified interface, the uRPF flag is not displayed even though unicast RPF is enabled.</td>
<td>none</td>
</tr>
<tr>
<td>Addresses, Flags</td>
<td>Information about the address flags.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>protocol-family</td>
<td>Protocol family configured on the logical interface. If the protocol is inet, the IP address of the interface is also displayed.</td>
<td>brief</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the address flags.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Destination</td>
<td>IP address of the remote side of the connection.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Local</td>
<td>IP address of the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Broadcast address of the logical interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Generation</td>
<td>Unique number for use by Juniper Networks technical support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

show interfaces xe-4/1/0

user@switch show interfaces xe-4/1/0
Physical interface: xe-4/1/0, Enabled, Physical link is Up
Interface index: 387, SNMP ifIndex: 369
Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, Duplex: Full-Duplex,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags    : Present Running
Interface flags: SNMP-Traps Internal: 0x0
Link flags      : None
CoS queues      : 8 supported, 8 maximum usable queues
Current address: 00:23:9c:03:8e:70, Hardware address: 00:23:9c:03:8e:70
Last flapped    : 2009-05-12 08:01:04 UTC (00:13:49 ago)
Input rate      : 36432 bps (3 pps)
Output rate     : 0 bps (0 pps)
Active alarms   : None
Active defects  : None

Logical interface xe-4/1/0.0 (Index 66) (SNMP ifIndex 417)
Flags: SNMP-Traps Encapsulation: ENET2
Input packets   : 0
Output packets  : 0
Protocol eth-switch
Flags: None
Egress queues: 8 supported, 4 in use

<table>
<thead>
<tr>
<th>Queue counters:</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms: None
Active defects: None

Logical interface xe-4/1/0.0 (Index 66) (SNMP ifIndex 417) (Generation 158)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Local statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Transit statistics:
Input bytes: 0 0 bps
Output bytes: 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps

Protocol eth-switch, Generation: 174, Route table: 0
Flags: None
Input Filters: f1,
Output Filters: f2,...

show interfaces xe-6/0/39 extensive

user@switch> show interfaces xe-6/0/39 extensive
Physical interface: xe-6/0/39, Enabled, Physical link is Up
Interface index: 291, SNMP ifIndex: 1641, Generation: 316
Link-level type: Ethernet, MTU: 1514, Speed: 10Gbps, Duplex: Full-Duplex,
BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags: Present Running
Interface flags: SNMP-Traps Internal: 0x0
Link flags: None
CoS queues: 8 supported, 8 maximum usable queues
Hold-times: Up 0 ms, Down 0 ms
Current address: 00:19:e2:72:f2:88, Hardware address: 00:19:e2:72:f2:88
Last flapped: 2010-05-13 14:49:43 PDT (1d 00:14 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes: 49625962140160 4391057408 bps
Output bytes: 47686985710805 4258984960 bps
Input packets: 387702829264 4288139 pps
Output packets: 372554570944 4159166 pps
IPv6 transit statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, FIFO errors: 0, Resource errors: 0

Output errors:
Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0, FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0

Ingress queues: 2 supported, 2 in use

<table>
<thead>
<tr>
<th>Queue counters: Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low priority</td>
<td>0</td>
<td>336342805223</td>
</tr>
<tr>
<td>High priority</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Egress queues: 8 supported, 8 in use

<table>
<thead>
<tr>
<th>Queue counters: Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low priority</td>
<td>0</td>
<td>33760130103</td>
</tr>
<tr>
<td>High priority</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

PFE Egress queues: 8 supported, 8 in use

<table>
<thead>
<tr>
<th>Queue counters: Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low priority</td>
<td>0</td>
<td>73760130103</td>
</tr>
<tr>
<td>High priority</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Active alarms: None
Active defects: None

MAC statistics:

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>49625962140160</td>
<td>47686985710805</td>
</tr>
<tr>
<td>Total packets</td>
<td>387702829264</td>
<td>372554570944</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>387702829264</td>
<td>372554518472</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>0</td>
<td>52470</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FIFO errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC control frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Code violations</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Packet Forwarding Engine configuration:

| Destination slot: 6 |

CoS information:

<table>
<thead>
<tr>
<th>Direction: Output</th>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>%</td>
<td>bps</td>
<td>%</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>75</td>
<td>75000000000</td>
<td>0</td>
<td>low</td>
</tr>
<tr>
<td>2 mcast-be</td>
<td>20</td>
<td>2000000000</td>
<td>0</td>
<td>low</td>
</tr>
<tr>
<td>7 network-cont</td>
<td>5</td>
<td>500000000</td>
<td>0</td>
<td>low</td>
</tr>
</tbody>
</table>

Logical interface xe-6/0/39.0 (Index 1810) (SNMP ifIndex 2238) (Generation 1923)
Flags: SNMP-Traps 0x0 Encapsulation: ENET2
Traffic statistics:
  Input bytes : 0
  Output bytes : 9375416
  Input packets: 0
  Output packets: 48901
Local statistics:
  Input bytes : 0
  Output bytes : 9375416
  Input packets: 0
  Output packets: 48901
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
Protocol eth-switch, Generation: 1937, Route table: 0
Flags: Trunk-Mode
show lACP interfaces

Syntax

show lACP interfaces
<interface-name>

Release Information

Command introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display Link Aggregation Control Protocol (LACP) information about the specified aggregated Ethernet or Gigabit Ethernet interface.

Options

none—Display LACP information for all interfaces.

interface-name—(Optional) Display LACP information for the specified interface:

Aggregated Ethernet—ae
Gigabit Ethernet—ge-fpc/pic/port
10-Gigabit Ethernet—xe-fpc/pic/port

Required Privilege

view

Related Documentation

• Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
• Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
• Example: Configuring Link Aggregation Between a QFX Series Product and an Aggregation Switch
• Configuring Aggregated Ethernet Links (CLI Procedure) on page 2335
• Configuring Link Aggregation
• Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
• Configuring Aggregated Ethernet LACP
• Configuring LACP Link Protection of Aggregated Ethernet Interfaces (CLI Procedure) on page 2340
• Understanding Aggregated Ethernet Interfaces and LACP
• Understanding Aggregated Ethernet Interfaces and LACP
• Junos OS Interfaces Fundamentals Configuration Guide

List of Sample Output

show lACP interfaces (EX Series Switches) on page 2540
show lACP interfaces (QFX Series) on page 2541

Output Fields

Table 325 on page 2539 lists the output fields for the show lACP interfaces command. Output fields are listed in the approximate order in which they appear.
### Table 325: show lacp interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated interface</td>
<td>Aggregated Ethernet interface name.</td>
</tr>
<tr>
<td>LACP State</td>
<td>LACP state information for each aggregated Ethernet interface:</td>
</tr>
<tr>
<td></td>
<td>• For a child interface configured with the <strong>force-up</strong> statement, LACP state displays <strong>FUP</strong> along with the interface name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Role</strong>—Role played by the interface. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Actor</strong>—Local device participating in the LACP negotiation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Partner</strong>—Remote device participating in the LACP negotiation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Exp</strong>—Expired state. <strong>Yes</strong> indicates that the actor or partner is in an expired state. <strong>No</strong> indicates that the actor or partner is not in an expired state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Def</strong>—Default. <strong>Yes</strong> indicates that the actor’s receive machine is using the default operational partner information, which is administratively configured for the partner. <strong>No</strong> indicates that the operational partner information in use has been received in an LACP PDU.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dist</strong>—Distribution of outgoing frames. <strong>No</strong> indicates that the distribution of outgoing frames on the link is currently disabled and is not expected to be enabled. Otherwise, the value is <strong>Yes</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Col</strong>—Collection of incoming frames. <strong>Yes</strong> indicates that the collection of incoming frames on the link is currently enabled and is not expected to be disabled. Otherwise, the value is <strong>No</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Syn</strong>—Synchronization. If the value is <strong>Yes</strong>, the link is considered to be synchronized. The link has been allocated to the correct link aggregation group, the group has been associated with a compatible aggregator, and the identity of the link aggregation group is consistent with the system ID and operational key information transmitted. If the value is <strong>No</strong>, the link is not synchronized. The link is currently not in the right aggregation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Aggr</strong>—Ability of the aggregation port to aggregate (<strong>Yes</strong>) or to operate only as an individual link (<strong>No</strong>).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Timeout</strong>—LACP timeout preference. Periodic transmissions of LACP PDUs occur at either a slow or a fast transmission rate, depending upon the expressed LACP timeout preference (<strong>Long Timeout</strong> or <strong>Short Timeout</strong>).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Activity</strong>—Actor’s or partner’s port activity. <strong>Passive</strong> indicates the port’s preference for not transmitting LAC PDUs unless its partner’s control value is <strong>Active</strong>. <strong>Active</strong> indicates the port’s preference to participate in the protocol regardless of the partner’s control value.</td>
</tr>
</tbody>
</table>
Table 325: show lacp interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACP Protocol</td>
<td>LACP protocol information for each aggregated interface:</td>
</tr>
</tbody>
</table>

- Link state (active or standby) indicated in parentheses next to the interface when link protection is configured.
- **Receive State**—One of the following values:
  - **Current**—The state machine receives an LACP PDU and enters the *Current* state.
  - **Defaulted**—If no LACP PDU is received before the timer for the *Current* state expires a second time, the state machine enters the *Defaulted* state.
  - **Expired**—If no LACP PDU is received before the timer for the *Current* state expires once, the state machine enters the *Expired* state.
  - **Initialize**—When the physical connectivity of a link changes or a Begin event occurs, the state machine enters the *Initialize* state.
  - **LACP Disabled**—If the port is operating in half duplex, the operation of LACP is disabled on the port, forcing the state to *LACP Disabled*. This state is similar to the *Defaulted* state, except that the port is forced to operate as an individual port.
  - **Port Disabled**—If the port becomes inoperable and a Begin event has not occurred, the state machine enters the *Port Disabled* state.
- **Transmit State**—Transmit state of the state machine. The transmit state is one of the following values:
  - **Fast periodic**—Periodic transmissions are enabled at a fast transmission rate.
  - **No periodic**—Periodic transmissions are disabled.
  - **Periodic timer**—Transitory state entered when the periodic timer expires.
  - **Slow periodic**—Periodic transmissions are enabled at a slow transmission rate.
- **Mux State**—State of the multiplexer state machine for the aggregation port. The state is one of the following values:
  - **Attached**—The multiplexer state machine initiates the process of attaching the port to the selected aggregator.
  - **Collecting**—Yes indicates that the receive function of this link is enabled with respect to its participation in an aggregation. Received frames are passed to the aggregator for collection. No indicates the receive function of this link is not enabled.
  - **Collecting distributing**—Collecting and distributing states are merged together to form a combined state (coupled control). Because independent control is not possible, the coupled control state machine does not wait for the partner to signal that collection has started before enabling both collection and distribution.
  - **Detached**—Process of detaching the port from the aggregator is in progress.
  - **Distributing**—Yes indicates that the transmit function of this link is enabled with respect to its participation in an aggregation. Frames can be passed down from the aggregator’s distribution function for transmission. No indicates the transmit function of this link is not enabled.
  - **Waiting**—The multiplexer state machine is in a holding process, awaiting an outcome.

**Sample Output**

`show lacp interfaces (EX Series Switches)`

```
user@switch> show lacp interfaces ae5
Aggregated interface: ae5

LACP state: Role Exp Def Dist Col Syn Aggr Timeout Activity
xe-2/0/7 Actor No No Yes Yes Yes Yes Fast Active
xe-2/0/7 Partner No No Yes Yes Yes Yes Fast Passive
```
### LACP State

<table>
<thead>
<tr>
<th>Interface</th>
<th>Role</th>
<th>Exp</th>
<th>Def</th>
<th>Dist</th>
<th>Col</th>
<th>Syn</th>
<th>Aggr</th>
<th>Timeout</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-4/0/7</td>
<td>Actor</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Fast</td>
<td>Active</td>
</tr>
<tr>
<td></td>
<td>Partner</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Fast</td>
<td>Passive</td>
</tr>
</tbody>
</table>

### LACP Protocol

<table>
<thead>
<tr>
<th>Interface</th>
<th>Receive State</th>
<th>Transmit State</th>
<th>Mux State</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-2/0/7</td>
<td>Current</td>
<td>Fast periodic</td>
<td>Collecting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>distributing</td>
</tr>
<tr>
<td>xe-34/0/7</td>
<td>Current</td>
<td>Fast periodic</td>
<td>Waiting</td>
</tr>
</tbody>
</table>

### show lacp interfaces (QFX Series)

```
user@switch> show lacp interfaces nodegroup1:ae0 extensive
Aggregated interface: nodegroup1:ae0
LACP state: Role Exp Def Dist Col Syn Aggr Timeout Activity
node1:xe-0/0/1FUP    Actor    No   Yes    No   No   No   Yes     Fast     Active
node1:xe-0/0/1FUP  Partner    No   Yes    No   No   No   Yes     Fast     Passive
node2:xe-0/0/2       Actor    No   Yes    No   No   No   Yes     Fast     Active
node2:xe-0/0/2     Partner    No   Yes    No   No   No   Yes     Fast     Passive
```
<table>
<thead>
<tr>
<th>LACP protocol:</th>
<th>Receive State</th>
<th>Transmit State</th>
<th>Mux State</th>
</tr>
</thead>
<tbody>
<tr>
<td>node1:xe-0/0/1FUP</td>
<td>Current</td>
<td>Fast periodic</td>
<td>Collecting</td>
</tr>
<tr>
<td></td>
<td>distributing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>node2:xe-0/0/2</td>
<td>Current</td>
<td>Fast periodic</td>
<td>Collecting</td>
</tr>
<tr>
<td></td>
<td>distributing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>node1:xe-0/0/1 (active)</td>
<td>Current</td>
<td>Fast periodic</td>
<td>Collecting</td>
</tr>
<tr>
<td></td>
<td>distributing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>node2:xe-0/0/2 (standby)</td>
<td>Current</td>
<td>Fast periodic</td>
<td>WAITING</td>
</tr>
</tbody>
</table>
**test interface restart-auto-negotiation**

**Syntax**

```
test interface restart-auto-negotiation interface-name
```

**Release Information**

Command introduced in Junos OS Release 7.6.  
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Restarts auto-negotiation on a Fast Ethernet or Gigabit Ethernet interface.

**Options**

`interface-name`—Interface name: `fe-fpc/pic/port` or `ge-fpc/pic/port`.

**Required Privilege**

View

**List of Sample Output**

```
test interface restart-auto-negotiation on page 2543
```

**Output Fields**

Use the `show interfaces extensive` command to see the state for auto-negotiation.

**Sample Output**

```
test interface restart-auto-negotiation

user@host> test interface restart-auto-negotiation fe-1/0/0
```
CHAPTER 47

Troubleshooting Procedures

• Troubleshooting an Aggregated Ethernet Interface on page 2545
• Troubleshooting Interface Configuration and Cable Faults on page 2546
• Troubleshooting Unicast RPF on page 2547
• Diagnosing a Faulty Twisted-Pair Cable (CLI Procedure) on page 2547

Troubleshooting an Aggregated Ethernet Interface

Troubleshooting issues for aggregated Ethernet interfaces:

• Show Interfaces Command Shows the LAG is Down on page 2545
• Logical Interface Statistics Do Not Reflect All Traffic on page 2545
• IPv6 Interface Traffic Statistics Are Not Supported on page 2546

Show Interfaces Command Shows the LAG is Down

Problem  The show interfaces terse command shows that the LAG is down.

Solution  Check the following:

• Verify that there is no configuration mismatch.
• Verify that all member ports are up.
• Verify that a LAG is part of family ethernet—switching (Layer 2 LAG) or family inet (Layer 3 LAG).
• Verify that the LAG member is connected to the correct LAG at the other end.
• Verify that the LAG members belong to the same switch (or the same Virtual Chassis).

Logical Interface Statistics Do Not Reflect All Traffic

Problem  The traffic statistics for a logical interface do not include all of the traffic.

Solution  Traffic statistics fields for logical interfaces in show interfaces commands show only control traffic; the traffic statistics do not include data traffic. You can view the statistics for all traffic only per physical interface.
IPv6 Interface Traffic Statistics Are Not Supported

Problem The IPv6 transit statistics in the show interfaces command display all 0 values.

Solution EX Series switches do not support the collection and reporting of IPv6 transit statistics.

Related Documentation
- Verifying the Status of a LAG Interface on page 2465
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch

Troubleshooting Interface Configuration and Cable Faults

Troubleshooting interface configuration and connectivity on the EX Series switch:

1. Interface Configuration or Connectivity Is Not Working on page 2546

Interface Configuration or Connectivity Is Not Working

Problem You encounter errors when you attempt to configure an interface on the switch, or the interface is exhibiting connectivity problems.

Solution Use the port troubleshooter feature in the J-Web interface to identify and rectify port configuration and connectivity related problems.

To use the J-Web interface port troubleshooter:

1. Select the option Troubleshoot from the main menu.
2. Click Troubleshoot Port. The Port Troubleshooting wizard is displayed. Click Next.
3. Select the ports to troubleshoot.
4. Select the test cases to be executed on the selected port. Click Next.

When the selected test cases are executed, the final result and the recommended action is displayed.

If there is a cable fault, the port troubleshooter displays details and the recommended action. For example, the cable must be replaced.

If the port configuration needs to be modified, the port troubleshooter displays details and the recommended action.

Related Documentation
- Monitoring Interface Status and Traffic on page 2463
- Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
Troubleshooting Unicast RPF

Troubleshooting issues for unicast reverse-path forwarding (RPF) on EX Series switches include:

1. Legitimate Packets Are Discarded on page 2547

Legitimate Packets Are Discarded

**Problem**  The switch filters valid packets from legitimate sources, which results in the switch’s discarding packets that should be forwarded.

**Solution**  The interface or interfaces on which legitimate packets are discarded are asymmetrically routed interfaces. An asymmetrically routed interface uses different paths to send and receive packets between the source and the destination, so the interface that receives a packet is not the same interface the switch uses to reply to the packet’s source.

Unicast RPF works properly only on symmetrically routed interfaces. A symmetrically routed interface is an interface that uses the same route in both directions between the source and the destination. Unicast RPF filters packets by checking the forwarding table for the best return path to the source of an incoming packet. If the best return path uses the same interface as the interface that received the packet, the switch forwards the packet. If the best return path uses a different interface than the interface that received the packet, the switch discards the packet.

---

**NOTE:** On EX3200, EX4200, and EX4300 switches, unicast RPF works properly only if all switch interfaces—including aggregated Ethernet interfaces (also referred to as link aggregation groups or LAGs), integrated routing and bridging (IRB) interfaces, and routed VLAN interfaces (RVIs)—are symmetrically routed, because unicast RPF is enabled globally on all switch interfaces.

---

**Related Documentation**

- Verifying Unicast RPF Status on page 2467
- Understanding Unicast RPF for EX Series Switches on page 2276

Diagnosing a Faulty Twisted-Pair Cable (CLI Procedure)

**Problem**  A 10/100/1000BASE-T Ethernet interface has connectivity problems that you suspect might be caused by a faulty cable.
**Solution**

Use the time domain reflectometry (TDR) test to determine whether a twisted-pair Ethernet cable is faulty.

The TDR test:

- Detects and reports faults for each twisted pair in an Ethernet cable. Faults detected include open circuits, short circuits, and impedance mismatches.
- Reports the distance to fault to within 1 meter.
- Detects and reports pair swaps, pair polarity reversals, and excessive pair skew.

The TDR test is supported on the following switches and interfaces:

- EX2200, EX3200, EX3300, and EX4200 switches—RJ-45 network interfaces. The TDR test is not supported on management interfaces and SFP interfaces.
- EX6200 and EX8200 switches—RJ-45 network interfaces on line cards.

---

**NOTE:** We recommend running the TDR test on an interface when there is no traffic on the interface.

---

To diagnose a cable problem by running the TDR test:

1. Run the `request diagnostics tdr` command.
   
   ```text
   user@switch> request diagnostics tdr start interface ge-0/0/10
   Interface TDR detail:
   Test status : Test successfully executed ge-0/0/10
   ```

2. View the results of the TDR test with the `show diagnostics tdr` command.
   
   ```text
   user@switch> show diagnostics tdr interface ge-0/0/10
   Interface TDR detail:
   Interface name : ge-0/0/10
   Test status : Passed
   Link status : Down
   MDI pair : 1-2
   Cable status : Normal
   Distance fault : 0 Meters
   Polarity swap : N/A
   Skew time : N/A
   MDI pair : 3-6
   Cable status : Normal
   Distance fault : 0 Meters
   Polarity swap : N/A
   Skew time : N/A
   MDI pair : 4-5
   Cable status : Open
   Distance fault : 1 Meters
   Polarity swap : N/A
   Skew time : N/A
   MDI pair : 7-8
   Cable status : Normal
   ```
3. Examine the **Cable status** field for the four MDI pairs to determine if the cable has a fault. In the preceding example, the twisted pair on pins 4 and 5 is broken or cut at approximately one meter from the **ge-0/0/10** port connection.

**NOTE:** The **Test Status** field indicates the status of the TDR test, not the cable. The value **Passed** means the test completed—it does not mean that the cable has no faults.

The following is additional information about the TDR test:

- The TDR test can take some seconds to complete. If the test is still running when you execute the **show diagnostics tdr** command, the **Test status** field displays **Started**. For example:

  ```
  user@switch> show diagnostics tdr interface ge-0/0/22
  Interface TDR detail:
  Interface name                  : ge-0/0/22
  Test status                     : Started
  ```

- You can terminate a running TDR test before it completes by using the **request diagnostics tdr abort interface interface-name** command. The test terminates with no results, and the results from any previous test are cleared.

- You can display summary information about the last TDR test results for all interfaces on the switch that support the TDR test by not specifying an interface name with the **show diagnostics tdr** command. For example:

  ```
  user@switch> show diagnostics tdr
  ```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Test status</th>
<th>Link status</th>
<th>Cable status</th>
<th>Max distance fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/8</td>
<td>Passed</td>
<td>Down</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/10</td>
<td>Passed</td>
<td>Down</td>
<td>Fault</td>
<td>1</td>
</tr>
<tr>
<td>ge-0/0/11</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/12</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/13</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/14</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/15</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/16</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Interface</td>
<td>Status</td>
<td>State</td>
<td>Status</td>
<td>Count</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>--------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>ge-0/0/17</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/18</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/19</td>
<td>Passed</td>
<td>Down</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/20</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/21</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ge-0/0/22</td>
<td>Passed</td>
<td>UP</td>
<td>OK</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/23</td>
<td>Not Started</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Troubleshooting Interface Configuration and Cable Faults on page 2546
- request diagnostics tdr on page 2479
- show diagnostics tdr on page 2481
PART 16

BGP

- Overview on page 2553
- Configuration on page 2557
- Administration on page 2649
CHAPTER 48

Overview

- Layer 3 Protocols on page 2553

Layer 3 Protocols

- Layer 3 Protocols Supported on EX Series Switches on page 2553
- Layer 3 Protocols Not Supported on EX Series Switches on page 2554

Layer 3 Protocols Supported on EX Series Switches

EX Series switches support the Junos OS Layer 3 features and configuration statements listed in Table 326 on page 2553:

Table 326: Supported Junos OS Layer 3 Protocol Statements and Features

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Fully supported.</td>
<td>[Junos OS Routing Protocols Configuration Guide]</td>
</tr>
<tr>
<td>BFD</td>
<td>Fully supported.</td>
<td>[Junos OS Routing Protocols Configuration Guide]</td>
</tr>
<tr>
<td>ICMP</td>
<td>Fully supported.</td>
<td>[Junos OS Routing Protocols Configuration Guide]</td>
</tr>
<tr>
<td>IGMPv1, v2, and v3</td>
<td>Fully supported.</td>
<td>[Junos OS Multicast Protocols Configuration Guide]</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>[Junos OS Routing Protocols Configuration Guide]</td>
</tr>
<tr>
<td>MLD</td>
<td>Fully supported (MLD versions 1 and 2).</td>
<td>[Junos OS Multicast Protocols Configuration Guide]</td>
</tr>
<tr>
<td>MPLS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>[Junos OS MPLS Applications Configuration Guide]</td>
</tr>
<tr>
<td>OSPFv1, v2 and v3</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>[Junos OS Routing Protocols Configuration Guide]</td>
</tr>
</tbody>
</table>
### Table 326: Supported Junos OS Layer 3 Protocol Statements and Features (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td>Fully supported on EX3200, EX3300, EX4200, EX6200, and EX8200 switches.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>PPM</td>
<td>Supported. See “EX Series Switch Software Features Overview” on page 27 for specific platform information.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIPng</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>SNMP</td>
<td>Fully supported.</td>
<td>Junos OS Network Management Configuration Guide</td>
</tr>
<tr>
<td>VRRP</td>
<td>Fully supported.</td>
<td>See “Understanding VRRP on EX Series Switches” on page 2220. See also Junos OS High Availability Guide.</td>
</tr>
</tbody>
</table>

### Related Documentation
- Layer 3 Protocols Not Supported on EX Series Switches on page 2554
- EX Series Switch Software Features Overview on page 27

### Layer 3 Protocols Not Supported on EX Series Switches

EX Series switches do not support the Junos OS Layer 3 protocols and features listed in Table 327 on page 2554:

### Table 327: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVMRP</td>
<td>• <em>dvmrp</em> and subordinate statements</td>
</tr>
<tr>
<td>Flow aggregation (cflowd)</td>
<td>• <em>cflow</em> and subordinate statements</td>
</tr>
<tr>
<td>IPSec</td>
<td>•  <em>edit services</em> statements related to IPSec</td>
</tr>
<tr>
<td>IS-IS:</td>
<td>•  <em>cns-routing</em> statement</td>
</tr>
<tr>
<td>• ES-IS</td>
<td>•  <em>ipv6-multicast</em> statement</td>
</tr>
<tr>
<td>• IPv6 in multicast routing protocols</td>
<td>•  <em>lsp-interval</em> statement</td>
</tr>
<tr>
<td></td>
<td>•  <em>label-switched-path</em> statement</td>
</tr>
<tr>
<td></td>
<td>•  <em>lsp-lifetime</em> statement</td>
</tr>
<tr>
<td></td>
<td>•  <em>te-metric</em> statement</td>
</tr>
<tr>
<td>Logical routers</td>
<td>•  <em>logical-routers</em> and subordinate statements</td>
</tr>
</tbody>
</table>
Table 327: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS:</td>
<td>• Fast Reroute (FRR)</td>
</tr>
<tr>
<td></td>
<td>• Label Distribution Protocol (LDP) (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 VPNs (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• Multiprotocol BGP (MP-BGP) for VPN-IPv4 family</td>
</tr>
<tr>
<td></td>
<td>• Pseudowire emulation (PWE3)</td>
</tr>
<tr>
<td></td>
<td>• Routing policy statements related to Layer 3 VPNs and MPLS (except on EX8200</td>
</tr>
<tr>
<td></td>
<td>switches)</td>
</tr>
<tr>
<td></td>
<td>• Virtual Private LAN Service (VPLS)</td>
</tr>
<tr>
<td></td>
<td>• nat and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• Policy statements related to NAT</td>
</tr>
<tr>
<td>OSPF</td>
<td>• demand-circuit statement</td>
</tr>
<tr>
<td></td>
<td>• label-switched-path and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• neighbor statement within an OSPF area</td>
</tr>
<tr>
<td></td>
<td>• peer-interface and subordinate statements within an OSPF area</td>
</tr>
<tr>
<td></td>
<td>• sham-link statement</td>
</tr>
<tr>
<td></td>
<td>• te-metric statement</td>
</tr>
<tr>
<td>PIM SM</td>
<td>• Not supported on EX2200 switches</td>
</tr>
<tr>
<td>PIM SSM</td>
<td>• Not supported on EX2200 switches</td>
</tr>
<tr>
<td>PIM DM</td>
<td>• Not supported on EX2200 or EX4500 switches</td>
</tr>
<tr>
<td>PIM:</td>
<td>• inet6 family (EX2200 and EX4500 switches)</td>
</tr>
<tr>
<td>I Pv6</td>
<td></td>
</tr>
<tr>
<td>PPM</td>
<td>• Not supported on EX2200 and EX3300 switches</td>
</tr>
<tr>
<td>Routing instances:</td>
<td>• l2vpn and subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• ldp and subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• vpls and subordinate statements</td>
</tr>
<tr>
<td>Routed VLAN interfaces (RVIs)</td>
<td>• family mpls statement</td>
</tr>
</tbody>
</table>
Table 327: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP and SDP</td>
<td>• sap and all subordinate statements</td>
</tr>
<tr>
<td>General routing options in the routing-options hierarchy:</td>
<td>• auto-export and subordinate statements</td>
</tr>
<tr>
<td>• MPLS and label-switched-paths</td>
<td>• dynamic-tunnels and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• lsp-next-hop and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• multicast and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• p2mp-lsp-next-hop and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• route-distinguisher-id statement (except on EX8200 switches)</td>
</tr>
<tr>
<td>Traffic sampling and forwarding in the forwarding-options hierarchy</td>
<td>• accounting and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• family mpls and family multiservice under hash-key hierarchy</td>
</tr>
<tr>
<td></td>
<td>• Under monitoring group-name family inet output hierarchy:</td>
</tr>
<tr>
<td></td>
<td>• cflowd statement</td>
</tr>
<tr>
<td></td>
<td>• export-format-cflowd-version-5 statement</td>
</tr>
<tr>
<td></td>
<td>• flow-active-timeout statement</td>
</tr>
<tr>
<td></td>
<td>• flow-export-destination statement</td>
</tr>
<tr>
<td></td>
<td>• flow-inactive-timeout statement</td>
</tr>
<tr>
<td></td>
<td>• interface statement</td>
</tr>
<tr>
<td></td>
<td>• port-mirroring statement (On EX Series switches, port mirroring is implemented using the analyzer statement.)</td>
</tr>
<tr>
<td></td>
<td>• sampling and subordinate statements</td>
</tr>
</tbody>
</table>

Related Documentation
• Layer 3 Protocols Supported on EX Series Switches on page 2553
• EX Series Switch Software Features Overview on page 27
You can use the J-Web interface to create BGP peering sessions on a routing device.

**NOTE:** To configure BGP sessions, you must have a license for BGP installed on the EX Series switch.

To configure a BGP peering session:

1. Select **Configure > Routing > BGP**.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Add**—Adds a BGP group. Enter information into the configuration page as described in Table 328 on page 2558.
   - **Edit**—Modifies an existing BGP group. Enter information into the configuration page as described in Table 328 on page 2558.
   - **Delete**—Deletes an existing BGP group.
   - **Disable**—Disables BGP configuration.
3. To modify BGP global settings, click **Edit** in the Global Information section. Enter information as described in [Table 329 on page 2559](#).

### Table 328: BGP Routing Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Type</td>
<td>Specifies whether the group is an internal BGP (IBGP) group or an external BGP (EBGP) group.</td>
<td>Select the option: <strong>Internal</strong> or <strong>External</strong>.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Specifies the name for the group.</td>
<td>Type a new name or select and edit the name.</td>
</tr>
<tr>
<td>ASN</td>
<td>Sets the unique numeric identifier of the AS in which the routing device is configured.</td>
<td>Type the routing device’s 32-bit AS number, in dotted decimal notation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3, the value assigned to the AS is 0.0.0.3.</td>
</tr>
<tr>
<td>Preference</td>
<td>Specifies the degree of preference for an external route. The route with the highest local preference value is preferred.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Cluster Id</td>
<td>Specifies the cluster identifier to be used by the route reflector cluster in an internal BGP group.</td>
<td>Type or select and edit the IPv6 or IPv4 address to be used as the identifier.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the text description of the global, group, or neighbor configuration.</td>
<td>Type or select and edit the description.</td>
</tr>
<tr>
<td>Damping</td>
<td>Specifies whether route flap damping is enabled or not.</td>
<td>To enable route flap damping, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To disable route flap damping do not select the check box.</td>
</tr>
<tr>
<td>Advertise Inactive Routes</td>
<td>Specifies whether BGP advertises the best route even if the routing table did not select it to be an active route.</td>
<td>To enable advertising inactive routes, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To disable advertising inactive routes, do not select the check box.</td>
</tr>
<tr>
<td>Advertise Peer AS Routes</td>
<td>Specifies whether to disable the default behavior of suppressing AS routes.</td>
<td>To enable advertising peer AS routes, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To disable advertising peer AS routes, do not select the check box.</td>
</tr>
<tr>
<td><strong>Neighbors tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Neighbors</td>
<td>Configures a neighbor (peer).</td>
<td>Type the IPv4 address of the peer.</td>
</tr>
</tbody>
</table>
To configure a static neighbor:
1. Specify the IP address.
2. Specify the address of the local end of a BGP session.
3. Specify the degree of preference for an external route.
4. Enter a description.
5. Specify the hold-time value to use when negotiating a connection with the peer.
6. Specify how long a route must be present in the routing table before it is exported to BGP. Use this time delay to help bundle routing updates.
7. Select **Passive** if you do not want to send active open messages to the peer.
8. Select the option to compare the AS path of an incoming advertised route with the AS number of the BGP peer under the group and replace all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer.
9. Specify an import policy and export policy.
10. Click **OK**.

### Policies tab

**Import Policy**
- Specifies one or more routing policies to routes being imported into the routing table from BGP.
- Click **Add** to add an import policy. Select the policy and click **OK**.
- Click **Move up** or **Move down** to move the selected policy up or down the list of policies.
- Select the policy and click **Remove**.

**Export Policy**
- Specifies one or more policies to routes being exported from the routing table into BGP.
- Click **Add** to add an export policy. Select the policy and click **OK**.
- Click **Move up** or **Move down** to move the selected policy up or down the list of policies.
- Select the policy and click **Remove**.

### Table 329: BGP Global Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router ASN</td>
<td>Specifies the routing device’s AS number.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Router Identifier</td>
<td>Specify the routing device’s IP address.</td>
<td>Type or select and edit the IP address.</td>
</tr>
</tbody>
</table>
Table 329: BGP Global Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Status</td>
<td>Enables or disables BGP.</td>
<td>• To enable BGP, select <strong>Enabled</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable BGP, select <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes of the global, group, or neighbor configuration.</td>
<td>Type or select and edit the description.</td>
</tr>
<tr>
<td>Confederation Number</td>
<td>Specifies the routing device's confederation AS number.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Confederation Members</td>
<td>Specifies the AS numbers for the confederation members.</td>
<td>To add a member AS number, click <strong>Add</strong> and enter the number in the <strong>Member ASN</strong> box. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To modify a confederation member's AS number, select the member click <strong>Edit</strong> and, enter the number and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a confederation member, select the member and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Advance Options</td>
<td>You can configure the following:</td>
<td>Select <strong>All</strong> or <strong>None</strong> to configure Keep Routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Keep routes</strong>—Specifies whether routes learned from a BGP peer must be retained in the routing table even if they contain an AS number that was exported from the local AS.</td>
<td>Enter a value in the <strong>TCP MSS</strong> box.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TCP MSS</strong>—Configures the maximum segment size (MSS) for the TCP connection for BGP neighbors.</td>
<td>Click to enable <strong>MTU Discovery</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MTU Discovery</strong>—Select to configure MTU discovery.</td>
<td>Click to enable <strong>Remove Private ASN</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove Private ASN</strong>—Select to have the local system strip private AS numbers from the AS path when advertising AS paths to remote systems.</td>
<td>Enter the time period for a graceful restart and the maximum time that stale routes must be kept.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Graceful Restart</strong>—Specifies the time period when the restart is expected to be complete. Specify the maximum time that stale routes are kept during restart.</td>
<td>To configure Multihop, select <strong>Nexthop Change</strong> to allow unconnected third-party next hops. Enter a TTL value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Multihop</strong>—Configures the maximum time-to-live (TTL) value for the TTL in the IP header of BGP packets.</td>
<td>Select the authentication algorithm. If you select None, specify an authentication key (password).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Authentication Type</strong>—Select the authentication algorithm: None, MD5, SHA1, AES.</td>
<td></td>
</tr>
</tbody>
</table>

Policies tab

| Import Policy        | Specifies one or more routing policies to routes being imported into the routing table from BGP. | Click **Add** to add an import policy.                                           |
|                      |                                                                                                   | Click **Move up** or **Move down** to move the selected policy up or down the list of policies. |
|                      |                                                                                                   | Click **Remove** to remove an import policy.                                     |
### Table 329: BGP Global Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Policy</td>
<td>Specifies one or more policies to routes being exported from the routing table into BGP.</td>
<td>Click <strong>Add</strong> to add an export policy. Click <strong>Move up</strong> or <strong>Move down</strong> to move the selected policy up or down the list of policies. Click <strong>Remove</strong> to remove an export policy.</td>
</tr>
</tbody>
</table>

#### Trace Options tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>Specifies the name of the file to receive the output of the tracing operation.</td>
<td>Type or select and edit the name.</td>
</tr>
<tr>
<td>Number of Files</td>
<td>Specifies the maximum number of trace files.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>File Size</td>
<td>Specifies the maximum size for each trace file.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>World Readable</td>
<td>Specifies whether the trace file can be read by any user or not.</td>
<td>Select <strong>True</strong> to allow any user to read the file. Select <strong>False</strong> to disallow all users being able to read the file.</td>
</tr>
</tbody>
</table>

| Flags         | Specifies the tracing operation to perform.                              | Select a value from the list.                                                |

#### Related Documentation
- Monitoring BGP Routing Information on page 2649
- Layer 3 Protocols Supported on EX Series Switches on page 2553
Configuration Statements

accept-remote-nexthop

Syntax

accept-remote-nexthop;

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Specify that a single-hop EBGP peer accepts a remote next hop with which it does not share a common subnet. Configure a separate import policy on the EBGP peer to specify the remote next hop. You cannot configure multihop and accept-remote-nexthop statements for the same EPBG peer.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Single-Hop EBGP Peers to Accept Remote Next Hops
- Understanding Route Advertisement
- multipath on page 2624
advertise-external

Syntax
advertise-external [conditional];

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information
Statement introduced in Junos OS Release 9.3.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Specify BGP to advertise the best external route into an IBGP mesh group, a route reflector cluster, or an AS confederation even if the best route is an internal route.

In general, deployed BGP implementations do not advertise the external route with the highest local preference value to internal peers unless it is the best route. Although this behavior was required by an earlier version of the BGP version 4 specification, RFC 1771, it was typically not followed in order to minimize the amount of advertised information and to prevent routing loops. However, there are scenarios in which advertising the best external route is beneficial, in particular, situations that can result in IBGP route oscillation.

The advertise-external statement is supported at both the group and neighbor level. If you configure the statement at the neighbor level, you must configure it for all neighbors in a group. Otherwise, the group is automatically split into different groups.

In a confederation, when advertising a route to a confederation border router, any route from a different confederation sub-AS is considered external. When configuring the advertise-external statement for an AS confederation, it is recommended that EBGP peers belonging to different autonomous systems are configured in a separate EBGP peer group. This ensures consistency while BGP sends the best external route to peers in the configured peer group.

To configure the advertise-external statement on a route reflector, you must disable intracluster reflection with the no-client-reflect statement.

When a routing device is configured as a route reflector for a cluster, a route advertised by the route reflector is considered internal if it is received from an internal peer with the same cluster identifier or if both peers have no cluster identifier configured. A route received from an internal peer that belongs to another cluster, that is, with a different cluster identifier, is considered external.

The conditional option causes BGP to advertise the external route only if the route selection process reaches the point where the multiple exit discriminator (MED) metric
is evaluated. As a result, an external route with an AS path longer than that of the active path is not advertised.

Junos OS also provides support for configuring a BGP export policy that matches on the state of an advertised route. You can match on either active or inactive routes.

**Default**

BGP does not advertise the external route with the highest local preference value to internal peers unless it is the best route.

**Options**

conditional—(Optional) Advertise the best external path only if the route selection process reaches the point at which the multiple exit discriminator (MED) metric is evaluated. The conditional option restricts advertisement to when the best external path and the active path are equal until the MED step of the route selection process. This implies that external routes with a longer AS path length than the active path, for instance, are not advertised. The criteria used for selecting the best external path is the same whether or not the conditional option is configured.

**Required Privilege**

routing—To view this statement in the configuration.

route-control—To add this statement to the configuration.

**Related Documentation**

- advertise-inactive on page 2565
advertise-inactive

Syntax
advertise-inactive;

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure the routing table to export to BGP the best route learned by BGP even if Junos OS did not select this route to be an active route.

One way to achieve multivendor compatibility is to include the advertise-inactive statement in the external BGP (EBGP) configuration. By default, BGP stores the route information it receives from update messages in the Junos OS routing table, and the routing table exports only active routes into BGP, which BGP then advertises to its peers. The advertise-inactive statement causes Junos OS to advertise the best BGP route that is inactive because of IGP preference. When you use the advertise-inactive statement, the Junos OS device uses, for example, the OSPF route for forwarding, and the other vendor’s device uses the EBGP route for forwarding. However, from the perspective of an EBGP peer in a neighboring AS, both vendors’ devices appear to behave the same way.

Default
By default, BGP stores the route information it receives from update messages in the Junos OS routing table, and the routing table exports only active routes into BGP, which BGP then advertises to its peers.

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Example: Setting BGP to Advertise Inactive Routes
• Example: Configuring the Preference Value for BGP Routes
• Example: Configuring BGP Route Preference (Administrative Distance)
advertise-peer-as

Syntax  
advertise-peer-as;

Hierarchy Level  
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Disable the default behavior of suppressing AS routes.

If you include the `advertise-peer-as` statement in the configuration, BGP advertises routes learned from one external BGP (EBGP) peer back to another EBGP peer in the same autonomous system (AS).

Another way to disable the route suppression default behavior is with the `as-override` statement. If you include both the `as-override` and `no-advertise-peer-as` statements in the configuration, the `no-advertise-peer-as` statement is ignored.

Default  
By default, Junos OS does not advertise the routes learned from one EBGP peer back to the same external BGP (EBGP) peer. In addition, the software does not advertise those routes back to any EBGP peers that are in the same AS as the originating peer, regardless of the routing instance.

Required Privilege  
Level  
routing—to view this statement in the configuration.

routing-control—to add this statement to the configuration.

Related Documentation  
• Example: Disabling Suppression of Route Advertisements
• Example: Configuring a Layer 3 VPN with Route Reflection and AS Override
• no-advertise-peer-as
aggregate-label

Syntax
aggregate-label {
    community community-name;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp family inet labeled-unicast],
[edit logical-systems logical-system-name protocols bgp family inet6 labeled-unicast],
[edit logical-systems logical-system-name protocols bgp family inet-vpn unicast],
[edit logical-systems logical-system-name protocols bgp family inet-vpn6 unicast],
[edit protocols bgp family inet labeled-unicast],
[edit protocols bgp family inet6 labeled-unicast],
[edit protocols bgp family inet-vpn unicast],
[edit protocols bgp family inet-vpn6 unicast]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Specify matching criteria (in the form of a community) such that all routes which match are assigned the same VPN label, selected from one of the several routes in the set defined by this criteria. This reduces the number of VPN labels that the router must consider, and aggregates the received labels.

Options
community community-name—Specify the name of the community to which to apply the aggregate label.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Aggregate Labels for VPNs
allow

Syntax  
allow (all | [ network/mask-length ]);  

Hierarchy Level  
[edit logical-systems logical-system-name protocols bgp group group-name],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],  
[edit protocols bgp group group-name],  
[edit routing-instances routing-instance-name protocols bgp group group-name]  

Release Information  
Statement introduced before Junos OS Release 7.4,  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.  

Description  
Implicitly configure BGP peers, allowing peer connections from any of the specified networks or hosts. To configure multiple BGP peers, configure one or more networks and hosts within a single allow statement or include multiple allow statements.

NOTE: You cannot define a BGP group with dynamic peers with BGP authentication enabled.

Options  
all—Allow all addresses, which is equivalent to 0.0.0.0/0 (or ::/0).

network/mask-length—IPv6 or IPv4 network number of a single address or a range of allowable addresses for BGP peers, followed by the number of significant bits in the subnet mask.

NOTE: You cannot define a BGP group with dynamic peers with authentication enabled.

Required Privilege Level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.  

Related Documentation  
• neighbor on page 2625
as-override

Syntax

Syntax: as-override;

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Compare the AS path of an incoming advertised route with the AS number of the BGP peer under the group and replace all occurrences of the peer AS number in the AS path with its own AS number before advertising the route to the peer.

NOTE: The as-override statement is specific to a particular BGP group. This statement does not affect peers from the same remote AS configured in different groups.

Enabling the AS override feature allows routes originating from an AS to be accepted by a router residing in the same AS. Without AS override enabled, the routing device refuses the route advertisement once the AS path shows that the route originated from its own AS. This is done by default to prevent route loops. The as-override statement overrides this default behavior.

Note that enabling the AS override feature may result in routing loops. Use this feature only for specific applications that require this type of behavior, and in situations with strict network control. One application is the IGP protocol between the provider edge routing device and the customer edge routing device in a virtual private network.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring a Layer 3 VPN with Route Reflection and AS Override
- Junos OS VPNs Library for Routing Devices
## authentication-algorithm

**Syntax**

```
authentication-algorithm algorithm;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ldp session session-address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit protocols ldp session session-address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols ldp session session-address]
```

**Release Information**

- Statement introduced in Junos OS Release 7.6.
- Statement introduced for BGP in Junos OS Release 8.0.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure an authentication algorithm type.

**Options**

- `algorithm`—Specify one of the following types of authentication algorithms:
  - `aes-128-cmac-96`—Cipher-based message authentication code (AES128, 96 bits).
  - `hmac-sha-1-96`—Hash-based message authentication code (SHA1, 96 bits).
  - `md5`—Message digest 5.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Route Authentication for BGP
authentication-key (Protocols BGP)

Syntax  

```
authentication-key key;
```

Hierarchy Level
- `[edit logical-systems logical-system-name protocols bgp]`
- `[edit logical-systems logical-system-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]`
- `[edit protocols bgp group group-name]`
- `[edit protocols bgp group group-name neighbor address]`
- `[edit protocols bgp group group-name neighbor address]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]`

Release Information
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure an MD5 authentication key (password). Neighboring routing devices use the same password to verify the authenticity of BGP packets sent from this system.

Options
- `key`—Authentication password. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (“ “).

Required Privilege Level
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation
- Example: Configuring Route Authentication for BGP
authentication-key-chain (Protocols BGP)

Syntax

authentication-key-chain key-chain;

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Apply and enable an authentication keychain to the routing device. Note that the referenced key chain must be defined. When configuring the authentication key update mechanism for BGP, you cannot commit the 0.0.0.0/allow statement with authentication keys or key chains. The CLI issues a warning and fails to commit such configurations.

Options

key-chain—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (" ").

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring Route Authentication for BGP
• Example: Configuring BFD Authentication for Static Routes
• Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols
autonomous-system

Syntax
autonomous-system autonomous-system <asdot-notation> <loops number> { independent-domain <no-attrset>;
}

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
asdot-notation option introduced in Junos OS Release 9.3.
asdot-notation option introduced in Junos OS Release 9.3 for EX Series switches.
no-attrset option introduced in Junos OS Release 10.4.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description
Specify the routing device’s AS number.

An autonomous system (AS) is a set of routing devices that are under a single technical administration and that generally use a single interior gateway protocol (IGP) and metrics to propagate routing information within the set of routing devices. An AS appears to other ASs to have a single, coherent interior routing plan and presents a consistent picture of what destinations are reachable through it. ASs are identified by a number that is assigned by the Network Information Center (NIC) in the United States (http://www.isi.edu).

If you are using BGP on the routing device, you must configure an AS number.

The AS path attribute is modified when a route is advertised to an EBGP peer. Each time a route is advertised to an EBGP peer, the local routing device prepends its AS number to the existing path attribute, and a value of 1 is added to the AS number.

In Junos OS Release 9.1 and later, the numeric range is extended to provide BGP support for 4-byte AS numbers as defined in RFC 4893, BGP Support for Four-octet AS Number Space. RFC 4893 introduces two new optional transitive BGP attributes, AS4_PATH and AS4_AGGREGATOR. These new attributes are used to propagate 4-byte AS path information across BGP speakers that do not support 4-byte AS numbers. RFC 4893 also introduces a reserved, well-known, 2-byte AS number, AS 23456. This reserved AS number is called AS_TRANS in RFC 4893. All releases of Junos OS support 2-byte AS numbers.

In Junos OS Release 9.3 and later, you can also configure a 4-byte AS number using the AS-dot notation format of two integer values joined by a period: <16-bit high-order value in decimal>.<16-bit low-order value in decimal>. For example, the 4-byte AS number of 65,546 in plain-number format is represented as 110 in the AS-dot notation format.

Options
autonomous-system—AS number. Use a number assigned to you by the NIC.
Range: 1 through 4,294,967,295 \( (2^{32} - 1) \) in plain-number format for 4-byte AS numbers

In this example, the 4-byte AS number 65,546 is represented in plain-number format:

```
[edit]
  routing-options {
    autonomous-system 65546;
  }
```

Range: 0.0 through 65535.65535 in AS-dot notation format for 4-byte numbers

In this example, 1.10 is the AS-dot notation format for 65,546:

```
[edit]
  routing-options {
    autonomous-system 1.10;
  }
```

Range: 1 through 65,535 in plain-number format for 2-byte AS numbers (this is a subset of the 4-byte range)

In this example, the 2-byte AS number 60,000 is represented in plain-number format:

```
[edit]
  routing-options {
    autonomous-system 60000;
  }
```

Asdot-notation—(Optional) Display the configured 4-byte autonomous system number in the AS-dot notation format.

Default: Even if a 4-byte AS number is configured in the AS-dot notation format, the default is to display the AS number in the plain-number format.

Loops number—(Optional) Specify the number of times detection of the AS number in the AS_PATH attribute causes the route to be discarded or hidden. For example, if you configure loops 1, the route is hidden if the AS number is detected in the path one or more times. This is the default behavior. If you configure loops 2, the route is hidden if the AS number is detected in the path two or more times.

Range: 1 through 10

Default: 1

NOTE: When you specify the same AS number in more than one routing instance on the local routing device, you must configure the same number of loops for the AS number in each instance. For example, if you configure a value of 3 for the loops statement in a VRF routing instance that uses the same AS number as that of the master instance, you must also configure a value of 3 loops for the AS number in the master instance.

Use the independent-domain option if the loops statement must be enabled only on a subset of routing instances.

The remaining statement is explained separately.
Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Examples: Configuring External BGP Peering
- Examples: Configuring Internal BGP Peering
**bfd-liveness-detection (Protocols BGP)**

**Syntax**

```
bfd-liveness-detection {  
  authentication {  
    algorithm algorithm-name;  
    key-chain key-chain-name;  
    loose-check;  
  }  
  detection-time {  
    threshold milliseconds;  
  }  
  hold-down-interval milliseconds;  
  minimum-interval milliseconds;  
  minimum-receive-interval milliseconds;  
  multiplier number;  
  no-adaptation;  
  session-mode (automatic | multihop | single-hop);  
  transmit-interval {  
    minimum-interval milliseconds;  
    threshold milliseconds;  
  }  
  version (1 | automatic);  
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols bgp],  
[edit logical-systems logical-system-name protocols bgp group group-name],  
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],  
[edit protocols bgp],  
[edit protocols bgp group group-name],  
[edit protocols bgp group group-name neighbor address],  
[edit routing-instances routing-instance-name protocols bgp],  
[edit routing-instances routing-instance-name protocols bgp group group-name],  
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

**Release Information**

Statement introduced in Junos OS Release 8.1.
Support for logical routers introduced in Junos OS Release 8.3.
Support for IBGP and multihop EBGP sessions introduced in Junos OS Release 8.3.
**hold-down-interval** statement introduced in Junos OS Release 8.5. You can configure this statement only for EBGP peers at the [edit protocols bgp group group-name neighbor address] hierarchy level.
**no-adaptation** statement introduced in Junos OS Release 9.0.
Support for BFD on IPv6 interfaces with BGP introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Configure bidirectional failure detection (BFD) timers and authentication for BGP.

For IBGP and multihop EBGP support, configure the `bfd-liveness-detection` statement at the global `[edit bgp protocols]` hierarchy level. You can also configure IBGP and multihop support for a routing instance or a logical system.
Options

**authenticationalgorithm algorithm-name** (Optional)—Configure the algorithm used to authenticate the specified BFD session: simple-password, keyed-md5, keyed-sha-1, meticulous-keyed-md5, meticulous-keyed-sha-1.

**authenticationkey-chain key-chain-name** (Optional)—Associate a security key with the specified BFD session using the name of the security keychain. The keychain name must match one of the keychains configured in the **authentication-key-chains key-chain** statement at the [edit security] hierarchy level.

**authenticationloose-check**—(Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication may not be configured at both ends of the BFD session.

**detection-time threshold milliseconds** (Optional)—Configure a threshold. When the BFD session detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

**holddown-interval milliseconds** (Optional)—Configure an interval specifying how long a BFD session must remain up before a state change notification is sent. When you configure the hold-down interval for the BFD protocol for EBGP, the BFD session is unaware of the BGP session during this time. In this case, if the BGP session goes down during the configured hold-down interval, BFD already assumes it is down and does not send a state change notification. The **holddown-interval** statement is supported only for EBGP peers at the [edit protocols bgp group group-name neighbor address] hierarchy level. If the BFD session goes down and then comes back up during the configured hold-down interval, the timer is restarted. You must configure the hold-down interval on both EBGP peers. If you configure the hold-down interval for a multihop EBGP session, you must also configure a local IP address by including the **local-address** statement at the [edit protocols bgp group group-name] hierarchy level.

**Range:** 0 through 255,000

**Default:** 0

**minimum-interval milliseconds** (Required)—Configure the minimum intervals at which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session. You can configure a value in the range from 1 through 255,000 milliseconds. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately (using the **minimum-receive-interval** and **transmit-interval** statements).

**Range:** 1 through 255,000

**minimum-receive-interval milliseconds** (Optional)—Configure only the minimum interval at which the local routing device expects to receive a reply from a neighbor with which it has established a BFD session.

**Range:** 1 through 255,000
**multiplier number** (Optional)—Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.

**Range:** 1 through 255  
**Default:** 3

**no-adaptation** (Optional)—Configure BFD sessions not to adapt to changing network conditions. We recommend that you not disable BFD adaptation unless it is preferable to not to have BFD adaptation enabled in your network.

**transmit-interval threshold milliseconds** (Optional)—Configure a threshold. When the BFD session transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent. The interval threshold must be greater than the minimum transmit interval.

**Range:** 0 through 4,294,967,295 ($2^{32} - 1$)

**transmit-interval minimum-interval milliseconds** (Optional)—Configure only the minimum interval at which the local routing device transmits hello packets to a neighbor with which it has established a BFD session.

**Range:** 1 through 255,000

**version** (Optional)—Configure the BFD version to detect.

**Range:** 1 or **automatic** (autodetect the BFD version)  
**Default:** automatic

The remaining statements are explained separately.

**Required Privilege Level**  
 routing—To view this statement in the configuration.  
 routing-control—To add this statement to the configuration.

**Related Documentation**  
• **Example: Configuring BFD for Static Routes**  
• **Example: Configuring BFD Authentication for Static Routes**  
• **Example: Configuring BFD on Internal BGP Peer Sessions**  
• **Example: Configuring BFD Authentication for BGP**  
• **Understanding BFD for BGP**
bgp

Syntax  

\texttt{bgp \{ ... \}}

Hierarchy Level  

[edit logical-systems \textit{logical-system-name} protocols bgp],  
[edit logical-systems \textit{logical-system-name} routing-instances \textit{routing-instance-name} protocols bgp],  
[edit protocols],  
[edit routing-instances \textit{routing-instance-name} protocols]

Release Information  

Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  

Enable BGP on the routing device or for a routing instance.

Default  

BGP is disabled.

Required Privilege Level  

rout -To view this statement in the configuration.  
rtng-control-To add this statement to the configuration.

Related Documentation  

• \textit{BGP Feature Guide for Routing Devices}
**bgp-orf-cisco-mode**

**Syntax**
```
bgp-orf-cisco-mode;
```

**Hierarchy Level**
- `edit logical-systems logical-system-name protocols bgp outbound-route-filter`
- `edit logical-systems logical-system-name protocols bgp group group-name outbound-route-filter`
- `edit logical-systems logical-system-name protocols bgp group group-name neighbor address outbound-route-filter`
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp outbound-route-filter`
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name outbound-route-filter`
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address outbound-route-filter`
- `edit logical-systems logical-system-name routing-instances routing-instance-name routing-options outbound-route-filter`
- `edit logical-systems logical-system-name routing-options outbound-route-filter`
- `edit protocols bgp outbound-route-filter`
- `edit protocols bgp group group-name outbound-route-filter`
- `edit protocols bgp group group-name neighbor address outbound-route-filter`
- `edit routing-instances routing-instance-name protocols bgp outbound-route-filter`
- `edit routing-instances routing-instance-name protocols bgp group group-name outbound-route-filter`
- `edit routing-instances routing-instance-name protocols bgp group group-name neighbor address outbound-route-filter`
- `edit routing-instances routing-instance-name routing-options outbound-route-filter`
- `edit routing-instance-name protocols bgp group group-name neighbor address outbound-route-filter`
- `edit routing-instance-name routing-options outbound-route-filter`

**Release Information**
- Statement introduced in Junos OS Release 9.2.
- Statement introduced in Junos OS Release 9.2 for EX Series switches.
- Support for the BGP group and neighbor hierarchy levels introduced in Junos OS Release 9.2.
- Support for the BGP group and neighbor hierarchy levels introduced in Junos OS Release 9.3 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**
Enable interoperability with routing devices that use the vendor-specific outbound route filter compatibility code of 130 and code type of 128.

**NOTE:** To enable interoperability for all BGP peers configured on the routing device, include the statement at the [edit routing-options outbound-route-filter] hierarchy level.

**Default**
Disabled

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.
Related Documentation

- Example: Configuring BGP Prefix-Based Outbound Route Filtering
cluster

Syntax  
cluster cluster-identifier;

Hierarchy Level  
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Specify the cluster identifier to be used by the route reflector cluster in an internal BGP group.

CAUTION:
If you configure both route reflection and VPNs on the same routing device, the following modifications to the route reflection configuration cause current BGP sessions to be reset:

- Adding a cluster ID—If a BGP session shares the same AS number with the group where you add the cluster ID, all BGP sessions are reset regardless of whether the BGP sessions are contained in the same group.
- Creating a new route reflector—If you have an IBGP group with an AS number and create a new route reflector group with the same AS number, all BGP sessions in the IBGP group and the new route reflector group are reset.

NOTE:  If you change the address family specified in the [edit protocols bgp family] hierarchy level, all current BGP sessions on the routing device are dropped and then reestablished.
Options  

cluster-identifier—4-byte identifier (such as an IPv4 address).

Required Privilege
Level

routing—To view this statement in the configuration.
route-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring BGP Route Refectors
• Understanding External BGP Peering Sessions
• no-client-reflect on page 2629
damping (Protocols BGP)

Syntax  damping:

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp family family],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name family family],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family family],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family family],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family family],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp family family],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name family family],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name family family],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address family family],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address family family],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address family family],
[edit protocols bgp],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name family family],
[edit protocols bgp group group-name neighbor address],
[edit protocols bgp group group-name neighbor address family family],
[edit protocols bgp group group-name neighbor address family family],
[edit protocols bgp group group-name neighbor address family family],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp family family],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name family family],
[edit routing-instances routing-instance-name protocols bgp group group-name family family],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address family family],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address family family],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address family family]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Support for flap damping at the address family level introduced in Junos OS Release 12.2.

Description
Enable route flap damping. BGP route flapping describes the situation in which BGP systems send an excessive number of update messages to advertise network reachability information. Flap damping reduces the number of update messages sent between BGP
peers, thereby reducing the load on these peers, without adversely affecting the route convergence time for stable routes.

You typically apply flap damping to external BGP (EBGP) routes (that is, to routes in different ASs). You can also apply it within a confederation, between confederation member ASs. Because routing consistency within an AS is important, do not apply flap damping to internal BGP (IBGP) routes. (If you do, it is ignored.) The exception to this rule is when flap damping is applied at the address family level. When you apply flap damping at the address family level, it works for both IBGP and EBGP.

**Default**
Flap damping is disabled on the routing device.

**Required Privilege**
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Examples: Configuring BGP Flap Damping
- Example: Configuring BGP Route Flap Damping Based on the MBGP MVPN Address Family
description (Protocols BGP)

Syntax  
```
description text-description;
```

Hierarchy Level  
```
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Provide a description of the global, group, or neighbor configuration. If the text includes one or more spaces, enclose it in quotation marks (" "). The test is displayed in the output of the `show` command and has no effect on the configuration.

Options  
`text-description`—Text description of the configuration. It is limited to 255 characters.

Required Privilege Level  
```
routing—To view this statement in the configuration.
routeing-control—To add this statement to the configuration.
```

Related Documentation  
- *BGP Feature Guide for Routing Devices*
### disable (Protocols BGP)

**Syntax**
```plaintext
disable;
```

**Hierarchy Level**
- `[edit logical-systems logical-system-name protocols bgp]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]`
- `[edit protocols bgp]`
- `[edit routing-instances routing-instance-name protocols bgp]`

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Disable BGP on the system.

**Required Privilege Level**
- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.
explicit-null (Protocols BGP)

Syntax

```bash
explicit-null;
```

Hierarchy Level

- `[edit logical-systems logical-system-name protocols mpls]`
- `[edit logical-systems logical-system-name protocols bgp family inet labeled-unicast]`
- `[edit logical-systems logical-system-name protocols bgp family inet6 labeled-unicast]`
- `[edit logical-systems logical-system-name protocols bgp group group-name family inet labeled-unicast]`
- `[edit logical-systems logical-system-name protocols bgp group group-name family inet6 labeled-unicast]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family inet labeled-unicast]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family inet6 labeled-unicast]`
- `[edit logical-systems logical-system-name protocols ldp]`
- `[edit logical-systems logical-system-name routing-instances instance-name protocols bgp family inet labeled-unicast]`
- `[edit logical-systems logical-system-name routing-instances instance-name protocols bgp family inet6 labeled-unicast]`
- `[edit logical-systems logical-system-name routing-instances instance-name protocols bgp group group-name family inet labeled-unicast]`
- `[edit logical-systems logical-system-name routing-instances instance-name protocols bgp group group-name family inet6 labeled-unicast]`
- `[edit logical-systems logical-system-name routing-instances instance-name protocols bgp group group-name neighbor address family inet labeled-unicast]`
- `[edit logical-systems logical-system-name routing-instances instance-name protocols bgp group group-name neighbor address family inet6 labeled-unicast]`
- `[edit logical-systems logical-system-name routing-instances instance-name protocols ldp]`
- `[edit protocols mpls]`
- `[edit protocols bgp family inet labeled-unicast]`
- `[edit protocols bgp family inet6 labeled-unicast]`
- `[edit protocols bgp group group-name family inet labeled-unicast]`
- `[edit protocols bgp group group-name family inet6 labeled-unicast]`
- `[edit protocols bgp group group-name neighbor address family inet labeled-unicast]`
- `[edit protocols bgp group group-name neighbor address family inet6 labeled-unicast]`
- `[edit protocols ldp]`
- `[edit routing-instances instance-name protocols bgp family inet labeled-unicast]`
- `[edit routing-instances instance-name protocols bgp family inet6 labeled-unicast]`
- `[edit routing-instances instance-name protocols bgp group group-name family inet labeled-unicast]`
- `[edit routing-instances instance-name protocols bgp group group-name family inet6 labeled-unicast]`
- `[edit routing-instances instance-name protocols bgp group group-name neighbor address family inet labeled-unicast]`
- `[edit routing-instances instance-name protocols bgp group group-name neighbor address family inet6 labeled-unicast]`
- `[edit routing-instances instance-name protocols ldp]`

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Advertise label 0 to the egress routing device of an LSP.
<table>
<thead>
<tr>
<th>Default</th>
<th>If you do not include the <strong>explicit-null</strong> statement in the configuration, label 3 (implicit null) is advertised.</th>
</tr>
</thead>
</table>
| Required Privilege Level | routing—To view this statement in the configuration.  
                          | routing-control—To add this statement to the configuration.                                           |
| Related Documentation | • Advertising Explicit Null Labels to BGP Peers                                                      |
export (Protocols BGP)

Syntax

export [ policy-names ];

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Apply one or more policies to routes being exported from the routing table into BGP. If you specify more than one policy, they are evaluated in the order specified, from left to right, and the first matching filter is applied to the route. If no routes match the filters, the routing table exports into BGP only the routes that it learned from BGP. If an action specified in one of the policies manipulates a route characteristic, the policy framework software carries the new route characteristic forward during the evaluation of the remaining policies. For example, if the action specified in the first policy of a chain sets a route’s metric to 500, this route matches the criterion of metric 500 defined in the next policy.

Options

policy-names—Name of one or more policies.

Required Privilege

Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Understanding Route Advertisement
• Routing Policy Feature Guide for Routing Devices
• import on page 2604
family (Protocols BGP)

Syntax

family {
  (inet | inet6 | inet-vpn | inet6-vpn | iso-vpn) {
  (any | flow | labeled-unicast | multicast | unicast) {
    accepted-prefix-limit {
      maximum number;
      teardown <percentage-threshold> idle-timeout (forever | minutes);
    }
    add-path {
      send {
        path-count number;
        prefix-policy [ policy-names ];
      }
      receive;
    }
    aigp [disable];
    loops number;
    prefix-limit {
      maximum number;
      teardown <percentage> <idle-timeout (forever | minutes)>;
    }
    protection;
    rib-group group-name;
    topology name {
      community {
        target identifier;
      }
    }
    flow {
      no-validate policy-name;
    }
    labeled-unicast {
      accepted-prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>;
      }
      aggregate-label {
        community community-name:
      }
      explicit-null {
        connected-only;
      }
      prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>;
      }
    }
    resolve-vpn;
    rib (inet.3 | inet6.3);
    rib-group group-name;
    traffic-statistics {
      file filename <world-readable | no-world-readable>;
      interval seconds;
    }
}
route-target {
    accepted-prefix-limit {
        maximum number;
        proxy-generate <route-target-policy route-target-policy-name>;
        teardown <percentage> <idle-timeout (forever | minutes)>;
    }
    advertise-default;
    external-paths number;
    prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>;
    }
}

(evpn | inet-mdt | inet-mvpn | inet6-mvpn | l2vpn) {
    signaling {
        accepted-prefix-limit {
            maximum number;
            teardown <percentage-threshold> idle-timeout (forever | minutes);
        }
        add-path {
            send {
                path-count number;
                prefix-policy [ policy-names ];
            }
            receive;
        }
        aigp [disable];
        damping;
        loops number;
        prefix-limit {
            maximum number;
            teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        rib-group group-name;
    }
}
Enable multiprotocol BGP (MP-BGP) by configuring BGP to carry network layer reachability information (NLRI) for address families other than unicast IPv4, to specify MP-BGP to carry NLRI for the IPv6 address family, or to carry NLRI for VPNs.
Options

any—Configure the family type to be both unicast and multicast.

evpn—Configure NLRI parameters for Ethernet VPNs (EVPNs).

inet—Configure NLRI parameters for IPv4.

inet6—Configure NLRI parameters for IPv6.

inet-mdt—Configure NLRI parameters for the multicast distribution tree (MDT) subaddress family identifier (SAFI) for IPv4 traffic in Layer 3 VPNs.

inet-mvpn—Configure NLRI parameters for IPv4 for multicast VPNs.

inet6-mvpn—Configure NLRI parameters for IPv6 for multicast VPNs.

inet-vpn—Configure NLRI parameters for IPv4 for Layer 3 VPNs.

inet6-vpn—Configure NLRI parameters for IPv6 for Layer 3 VPNs.

iso-vpn—Configure NLRI parameters for IS-IS for Layer 3 VPNs.

l2vpn—Configure NLRI parameters for IPv4 for MPLS-based Layer 2 VPNs and VPLS.

labeled-unicast—Configure the family type to be labeled-unicast. This means that the BGP peers are being used only to carry the unicast routes that are being used by labeled-unicast for resolving the labeled-unicast routes. This statement is supported only with inet and inet6.

multicast—Configure the family type to be multicast. This means that the BGP peers are being used only to carry the unicast routes that are being used by multicast for resolving the multicast routes.

unicast—Configure the family type to be unicast. This means that the BGP peers only carry the unicast routes that are being used for unicast forwarding purposes. The default family type is unicast.

The remaining statements are explained separately.

Required Privilege

Level
routing—to view this statement in the configuration.

routing-control—to add this statement to the configuration.

Related Documentation

• Configuring IBGP Sessions Between PE Routers in VPNs

• Understanding Multiprotocol BGP

• autonomous-system on page 2573

• local-as on page 2613
graceful-restart (Protocols BGP)

Syntax

graceful-restart {
  disable;
  restart-time seconds;
  stale-routes-time seconds;
}

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Enable graceful restart for BGP. Graceful restart allows a routing device undergoing a restart to inform its adjacent neighbors and peers of its condition. Graceful restart is disabled by default.

To configure the duration of the BGP graceful restart period, include the restart-time statement at the [edit protocols bgp graceful-restart] hierarchy level. To set the length of time the router waits to receive messages from restarting neighbors before declaring them down, include the stale-routes-time statement at the [edit protocols bgp graceful-restart] hierarchy level.

NOTE: If you configure graceful restart after a BGP session has been established, the BGP session restarts and the peers negotiate graceful restart capabilities.

For graceful restart to function properly, graceful restart must be enabled at the [edit routing-instance instance-name routing-options] or [edit routing-options] hierarchy level as well as in the protocol level.

For example:

  protocols {
    bgp {
      group ext {
        graceful-restart;
      }
    }
  }
  routing-options {
    graceful-restart;
  }
Graceful restart is enabled both at the `[edit routing-options]` hierarchy level, as well as at the routing protocol level. If graceful restart is not configured in both sections, the peer might have its route removed after a restart, which is not the intended behavior.

The remaining statements are explained separately.

**Required Privilege Level**
- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**
- Configuring Graceful Restart Options for BGP
- Configuring Graceful Restart for QFabric Systems
- Junos OS High Availability Library for Routing Devices
**group (Protocols BGP)**

**Syntax**

```plaintext
group group-name {
  advertise-inactive;
  allow [ network/mask-length ];
  authentication-key key;
  cluster cluster-identifier;
  damping;
  description text-description;
  export [ policy-names ];
  family {
    (inet | inet6 | inet-vpn | inet6-vpn | l2-vpn) {
      (any | multicast | unicast | signaling) {
        accepted-prefix-limit {
          maximum number;
          teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        add-path {
          send {
            path-count number;
            prefix-policy [ policy-names ];
          }
          receive;
        }
        aigp [disable];
        damping;
        prefix-limit {
          maximum number;
          teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        rib-group group-name;
        topology name {
          community {
            target identifier;
          }
        }
      }
    }
  }
  flow {
    no-validate policy-name;
  }
  labeled-unicast {
    accepted-prefix-limit {
      maximum number;
      teardown <percentage> <idle-timeout (forever | minutes)>;
    }
    explicit-null {
      connected-only;
    }
    prefix-limit {
      maximum number;
      teardown <percentage> <idle-timeout (forever | minutes)>;
    }
    resolve-vpn;
    rib inet.3;
  }
}```
rib-group group-name;
}
}
route-target {
    accepted-prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>
    }
    advertise-default;
    external-paths number;
    prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>
    }
}
}
hold-time seconds;
import [ policy-names ];
ipsec-sa ipsec-sa;
keep (all | none);
local-address address;
local-as autonomous-system <private>;
local-preference local-preference;
log-updown;
metric-out metric;
multipath <ttl-value>;
multipath {
    multipath [ multiple-as;
}
no-aggregator-id;
no-client-reflect;
out-delay seconds;
passive;
peer-as autonomous-system;
preference preference;
remove-private;
tcp-mss segment-size;
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
type type;
neighbor address {
    ... peer-specific-options ...
}
}

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit protocols bgp],
[edit routing-instances routing-instance-name protocols bgp]
| **Release Information** | Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series. |
|------------------------|--------------------------------------------------------------------------------------------------|
| **Description**        | Define a BGP peer group. BGP peer groups share a common type, peer autonomous system (AS) number, and cluster ID, if present. To configure multiple BGP groups, include multiple `group` statements.  
By default, the group's options are identical to the global BGP options. To override the global options, include group-specific options within the `group` statement.  
The `group` statement is one of the statements you must include in the configuration to run BGP on the routing device.  
Each group must contain at least one peer. |
| **Options**            | `group-name`—Name of the BGP group.  
The remaining statements are explained separately. |
| **Required Privilege** | routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration. |
| **Related Documentation** |  
• *BGP Feature Guide for Routing Devices* |
hold-time (Protocols BGP)

Syntax

```
hold-time seconds;
```

Hierarchy Level

- `[edit logical-systems logical-system-name protocols bgp]`
- `[edit logical-systems logical-system-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]`
- `[edit protocols bgp]`
- `[edit protocols bgp group group-name]`
- `[edit protocols bgp group group-name neighbor address]`
- `[edit routing-instances routing-instance-name protocols bgp]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]`

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Specify the hold-time value to use when negotiating a connection with the peer. The hold-time value is advertised in open packets and indicates to the peer the length of time that it should consider the sender valid. If the peer does not receive a keepalive, update, or notification message within the specified hold time, the BGP connection to the peer is closed and routing devices through that peer become unavailable.

The hold time is three times the interval at which keepalive messages are sent.

BGP on the local routing device uses the smaller of either the local hold-time value or the peer's hold-time value received in the open message as the hold time for the BGP connection between the two peers.

Starting in Junos OS Release 12.3, the BGP hold-time value can be zero (0). This implies that the speaker does not expect keepalive messages from its peer to maintain the BGP session. When negotiating between two peers, if one side requests a nonzero hold time and the other requests a zero hold time, the negotiation settles on the nonzero value and keepalive intervals are determined accordingly. Both sides must be set to zero for keepalive messages to stop being sent.

Options

- `seconds`—Hold time.
  - Range: 10 through 65,535 seconds (or 0 for infinite hold time)
  - Default: 90 seconds
TIP: When you set a hold-time value of 1 through 19 seconds, we recommend that you also configure the BGP precision-timers statement. The precision-timers statement ensures that if scheduler slip messages occur, the routing device continues to send keepalive messages. When the precision-timers statement is included, keepalive message generation is performed in a dedicated kernel thread, which helps to prevent BGP session flaps.

Required Privilege
Level
Routing—To view this statement in the configuration.
Routing-control—To add this statement to the configuration.

Related Documentation
• BGP Messages Overview
• precision-timers
idle-after-switch-over

Syntax
idle-after-switch-over (forever | seconds);

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address]

Release Information
Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure the routing device so that it does not automatically reestablish BGP peer sessions after a nonstop active routing (NSR) switchover. This feature is particularly useful if you are using dynamic routing policies because the dynamic database is not synchronized with the backup Routing Engine when NSR is enabled.

Options
forever—Do not reestablish a BGP peer session after an non-stop routing switchover until the clear bgp neighbor command is issued.

seconds—Do not reestablish a BGP peer session after an non-stop routing switchover until after the specified period.

Range: 1 through 4,294,967,295 ($2^{32} - 1$)

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Preventing Automatic Reestablishment of BGP Peer Sessions After NSR Switchovers
- Routing Policy Feature Guide for Routing Devices
- Junos OS High Availability Library for Routing Devices
import (Protocols BGP)

Syntax

```
import [ policy-names ];
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Apply one or more routing policies to routes being imported into the Junos OS routing table from BGP.

If you specify more than one policy, they are evaluated in the order specified, from left to right, and the first matching filter is applied to the route. If no match is found, BGP places into the routing table only those routes that were learned from BGP routing devices. The policy framework software evaluates the routing policies in a chain sequentially. If an action specified in one of the policies manipulates a route characteristic, the policy framework software carries the new route characteristic forward during the evaluation of the remaining policies. For example, if the action specified in the first policy of a chain sets a route’s metric to 500, this route matches the criterion of `metric 500` defined in the next policy.

It is also important to understand that in Junos OS, although an import policy (inbound route filter) might reject a route, not use it for traffic forwarding, and not include it in an advertisement to other peers, the router retains these routes as hidden routes. These hidden routes are not available for policy or routing purposes. However, they do occupy memory space on the router. A service provider filtering routes to control the amount of information being kept in memory and processed by a router might want the router to entirely drop the routes being rejected by the import policy.

Hidden routes can be viewed by using the `show route receive-protocol bgp neighbor-address hidden` command. The hidden routes can then be retained or dropped from the routing table by configuring the `keep all | none` statement at the `[edit protocols bgp]` or `[edit protocols bgp group group-name]` hierarchy level.
The rules of BGP route retention are as follows:

- By default, all routes learned from BGP are retained, except those where the AS path is looped. (The AS path includes the local AS.)
- By configuring the `keep all` statement, all routes learned from BGP are retained, even those with the local AS in the AS path.
- By configuring the `keep none` statement, all routes received are discarded. When this statement is configured and the inbound policy changes, Junos OS re-advertises all the routes advertised by the peer.

**Options**

`policy-names`—Name of one or more policies.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring BGP Interactions with IGPs
- Understanding Route Advertisement
- Routing Policy Feature Guide for Routing Devices
- export on page 2591
include-mp-next-hop

Syntax
include-mp-next-hop;

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Enable multiprotocol updates to contain next-hop reachability information.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Examples: Configuring Multiprotocol BGP
keep

Syntax
keep (all | none);

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Control whether or not Junos OS keeps in memory and hides certain routes.

If the keep none statement is used, Junos OS does not retain in memory and hide routes that are rejected because of a BGP import policy. Nor does BGP keep in memory and hide routes that are declared unfeasible due to BGP sanity checks. The keep none statement causes Junos OS to discard from memory the routes that are rejected due to BGP-specific logic or BGP evaluation. When a route is rejected because of some non-BGP-specific reason, the keep none statement has no effect on this route. This rejected route is retained in memory and hidden even though keep none is configured. An example of this type of hidden route is a route for which the protocol nexthop is unresolved.

The routing table can retain the route information learned from BGP in one of the following ways:

- Default (omit the keep statement)—Keep all route information that was learned from BGP, except for routes whose AS path is looped and whose loop includes the local AS.
- keep all—Keep all route information that was learned from BGP.
- keep none—Discard routes that were received from a peer and that were rejected by import policy or other sanity checking, such as AS path or next hop. When you configure keep none for the BGP session and the inbound policy changes, Junos OS forces readvertisement of the full set of routes advertised by the peer.
In an AS path healing situation, routes with looped paths theoretically could become usable during a soft reconfiguration when the AS path loop limit is changed. However, there is a significant memory usage difference between the default and keep all.

Consider the following scenarios:

- A peer readvertises routes back to the peer from which it learned them.
  
  This can happen in the following cases:

  - Another vendor's routing device advertises the routes back to the sending peer.
  - The Junos OS peer's default behavior of not readvertising routes back to the sending peer is overridden by configuring advertise-peer-as.

- A provider edge (PE) routing device discards any VPN route that does not have any of the expected route targets.

When keep all is configured, the behavior of discarding routes received in the above scenarios is overridden.

**CAUTION:** When you configure keep (all | none), the associated BGP sessions are restarted.

**Default**

By default, BGP retains incoming rejected routes in memory and hides them. If you do not include the keep statement, most routes are retained in the routing table. BGP keeps all route information that was learned from BGP, except for routes whose AS path is looped and whose loop includes the local AS.

**Options**

- **all**—Retain all routes.

- **none**—Discard routes that were received from a peer and that were rejected by import policy or other sanity checking. When keep none is configured for the BGP session and the inbound policy changes, Junos OS forces readvertisement of the full set of routes advertised by the peer.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- out-delay on page 2632
- Interprovider VPN Example—MP-EBGP Between ISP Peer Routers
- Example: Configuring Conditional Installation of Prefixes in a Routing Table
labeled-unicast (Protocols BGP)

Syntax

```plaintext
labeled-unicast {
  accepted-prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>
  };
  aggregate-label {
    community community-name;
  }
  explicit-null {
    connected-only;
  }
  prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>
  }
  protection;
  resolve-vpn;
  rib (inet.3 | inet6.3);
  rib-group group-name;
}
```

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp family (inet | inet6)],
[edit logical-systems logical-system-name protocols bgp group group-name family (inet | inet6)],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp family (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name family (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address family (inet | inet6)],
[edit protocols bgp family (inet | inet6)],
[edit protocols bgp group group-name family (inet | inet6)],
[edit protocols bgp group group-name neighbor address family (inet | inet6)],
[edit routing-instances routing-instance-name protocols bgp family (inet | inet6)],
[edit routing-instances routing-instance-name protocols bgp group group-name family (inet | inet6)],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address family (inet | inet6)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure the family type to be labeled-unicast.

The remaining statements are explained separately.

Required Privilege

Level routing—To view this statement in the configuration.
Level routing-control—To add this statement to the configuration.
Related Documentation

- Examples: Configuring Multiprotocol BGP
**local-address (Protocols BGP)**

**Syntax**
local-address address;

**Hierarchy Level**
- [edit logical-systems logical-system-name protocols bgp]
- [edit logical-systems logical-system-name protocols bgp group group-name]
- [edit logical-systems logical-system-name protocols bgp group group-name neighbor address]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]
- [edit protocols bgp]
- [edit protocols bgp group group-name]
- [edit protocols bgp group group-name neighbor address]
- [edit routing-instances routing-instance-name protocols bgp]
- [edit routing-instances routing-instance-name protocols bgp group group-name]
- [edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
- [edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Specify the address of the local end of a BGP session. This address is used to accept incoming connections to the peer and to establish connections to the remote peer. When none of the operational interfaces are configured with the specified local address, a session with a BGP peer is placed in the idle state.

You generally configure a local address to explicitly configure the system's IP address from BGP's point of view. This IP address can be either an IPv6 or IPv4 address. Typically, an IP address is assigned to a loopback interface, and that IP address is configured here.

For internal BGP (IBGP) peering sessions, generally the loopback interface (lo0) is used to establish connections between the IBGP peers. The loopback interface is always up as long as the device is operating. If there is a route to the loopback address, the IBGP peering session stays up. If a physical interface address is used instead and that interface goes up and down, the IBGP peering session also goes up and down. Thus, the loopback interface provides fault tolerance in case the physical interface or the link goes down, if the device has link redundancy.

When a device peers with a remote device's loopback interface address, the local device expects BGP update messages to come from (be sourced by) the remote device's loopback interface address. The local-address statement enables you to specify the source information in BGP update messages. If you omit the local-address statement, the expected source of BGP update messages is based on the device's source address selection rules, which normally result in the egress interface address being the expected source of update messages. When this happens, the peering session is not established because a mismatch exists between the expected source address (the egress interface
of the peer) and the actual source (the loopback interface of the peer). To ensure that the expected source address matches the actual source address, specify the loopback interface address in the `local-address` statement.

**NOTE:** Although a BGP session can be established when only one of the paired routing devices has local-address configured, we strongly recommend that you configure local-address on both paired routing devices for IBGP and multihop EBGP sessions. The local-address statement ensures that deterministic fixed addresses are used for the BGP session end-points.

If you include the `default-address-selection` statement in the configuration, the software chooses the system default address as the source for most locally generated IP packets. For protocols in which the local address is unconstrained by the protocol specification, for example IBGP and multihop EBGP, if you do not configure a specific local address when configuring the protocol, the local address is chosen using the same methods as other locally generated IP packets.

**Default**  
If you do not configure a local address, BGP uses the routing device's source address selection rules to set the local address.

**Options**  
`address`—IPv6 or IPv4 address of the local end of the connection.

**Required Privilege Level**  
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring Internal BGP Peering Sessions on Logical Systems
- Example: Configuring Internal BGP Peer Sessions
- Understanding Internal BGP Peering Sessions
- router-id on page 3111
## local-as

**Syntax**

```plaintext
local-as autonomous-system <loops number> <private | alias> <no-prepend-global-as>;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols bgp]`
- `[edit logical-systems logical-system-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]`
- `[edit protocols bgp]`
- `[edit protocols bgp group group-name]`
- `[edit protocols bgp group group-name neighbor address]`
- `[edit routing-instances routing-instance-name protocols bgp]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]`

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- `alias` option introduced in Junos OS Release 9.5.

**Description**

Specify the local autonomous system (AS) number. An AS is a set of routing devices that are under a single technical administration and generally use a single interior gateway protocol (IGP) and metrics to propagate routing information within the set of routing devices.

Internet service providers (ISPs) sometimes acquire networks that belong to a different AS. When this occur, there is no seamless method for moving the BGP peers of the acquired network to the AS of the acquiring ISP. The process of configuring the BGP peers with the new AS number can be time-consuming and cumbersome. In this case, it might not be desirable to modify peer arrangements or configuration. During this kind of transition period, it can be useful to configure BGP-enabled devices in the new AS to use the former AS number in BGP updates. This former AS number is called a `local AS`.

---

**NOTE:** If you are using BGP on the routing device, you must configure an AS number before you specify the local as number.

In Junos OS Release 9.1 and later, the AS numeric range in plain-number format is extended to provide BGP support for 4-byte AS numbers, as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*.

In Junos OS Release 9.3 and later, you can also configure a 4-byte AS number using the AS-dot notation format of two integer values joined by a period: `<16-bit high-order value in decimal>.<16-bit low-order value in decimal>`. For
example, the 4-byte AS number of 65546 in plain-number format is represented as 1.10 in the AS-dot notation format.

**Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>(Optional) Configure the local AS as an alias of the global AS number configured for the router at the [edit routing-options] hierarchy level. As a result, a BGP peer considers any local AS to which it is assigned as equivalent to the primary AS number configured for the routing device. When you use the alias option, only the AS (global or local) used to establish the BGP session is prepended in the AS path sent to the BGP neighbor.</td>
</tr>
<tr>
<td>autonomous-system</td>
<td>AS number. Range: 1 through 4,294,967,295 ((2^{32} - 1)) in plain-number format Range: 0.0 through 65535.65535 in AS-dot notation format</td>
</tr>
<tr>
<td>loops number</td>
<td>(Optional) Specify the number of times detection of the AS number in the AS_PATH attribute causes the route to be discarded or hidden. For example, if you configure loops 1, the route is hidden if the AS number is detected in the path one or more times. This is the default behavior. If you configure loops 2, the route is hidden if the AS number is detected in the path two or more times.</td>
</tr>
</tbody>
</table>

**NOTE:** If you configure the local AS values for any BGP group, the detection of routing loops is performed using both the AS and the local AS values for all BGP groups.

If the local AS for the E-BGP or I-BGP peer is the same as the current AS, do not use the local-as statement to specify the local AS number.

When you configure the local AS within a VRF, this impacts the AS path loop-detection mechanism. All of the local-as statements configured on the device are part of a single AS domain. The AS path loop-detection mechanism is based on looking for a matching AS present in the domain.

<table>
<thead>
<tr>
<th>Range</th>
<th>1 through 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-prepend-global-as</td>
<td>(Optional) Specify to strip the global AS and to prepend only the local AS in AS paths sent to external peers.</td>
</tr>
<tr>
<td>private</td>
<td>(Optional) Configure to use the local AS only during the establishment of the BGP session with a BGP neighbor but to hide it in the AS path sent to external BGP peers. Only the global AS is included in the AS path sent to external peers.</td>
</tr>
</tbody>
</table>

**NOTE:** The private and alias options are mutually exclusive. You cannot configure both options with the same local-as statement.
**Required Privilege**

**Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- *Examples: Configuring BGP Local AS*
- *Example: Configuring a Local AS for EBGP Sessions*
- *autonomous-system on page 2573*
- *family on page 2592*

---

**local-interface (IPv6)**

**Syntax**

```
local-interface interface-name;
```

**Hierarchy Level**

[edit logical-systems logical-system-name protocols bgp group group-name neighbor ipv6-link-local-address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor ipv6-link-local-address],
[edit protocols bgp group group-name neighbor ipv6-link-local-address],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor ipv6-link-local-address]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Specify the interface name of the EBGP peer that uses IPv6 link-local addresses. This peer is link-local in scope.

**Options**

- `interface-name`—Interface name of the EBGP IPv6 peer.

**Required Privilege**

**Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring Internal BGP Peering Sessions on Logical Systems*
- *Example: Configuring Internal BGP Peer Sessions*
- *Example: Configuring External BGP on Logical Systems with IPv6 Interfaces*
- *Understanding Internal BGP Peering Sessions*
**local-preference**

**Syntax**

```
local-preference local-preference;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Modify the value of the **LOCAL_PREF** path attribute, which is a metric used by BGP sessions to indicate the degree of preference for an external route. The route with the highest local preference value is preferred.

The **LOCAL_PREF** path attribute always is used in inbound routing policy and is advertised to internal BGP peers and to neighboring confederations. It is never advertised to external BGP peers.

**Default**

If you omit this statement, the **LOCAL_PREF** path attribute, if present, is not modified.

**Options**

**local-preference**—Preference to assign to routes learned from BGP or from the group or peer.

**Range:** 0 through 4,294,967,295 (\(2^{32} - 1\))

**Default:** If the **LOCAL_PREF** path attribute is present, do not modify its value. If a BGP route is received without a **LOCAL_PREF** attribute, the route is handled locally (it is stored in the routing table and advertised by BGP) as if it were received with a **LOCAL_PREF** value of 100. By default, non-BGP routes that are advertised by BGP are advertised with a **LOCAL_PREF** value of 100.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring the Local Preference Value for BGP Routes
- Understanding Internal BGP Peering Sessions
log-updown (Protocols BGP)

Syntax

log-updown;

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Specify to generate a log a message whenever a BGP peer makes a state transition. Messages are logged using the system logging mechanism located at the [edit system syslog] hierarchy level.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Preventing BGP Session Resets
• Junos OS Administration Library for Routing Devices
• traceoptions on page 2645

• preference on page 2638
**metric-out (Protocols BGP)**

**Syntax**
```
metric-out (metric | minimum-igp offset | igp (delay-med-update | offset));
```

**Hierarchy Level**
- [edit logical-systems logical-system-name protocols bgp],
- [edit logical-systems logical-system-name protocols bgp group group-name],
- [edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
- [edit protocols bgp],
- [edit protocols bgp group group-name],
- [edit protocols bgp group group-name neighbor address],
- [edit routing-instances routing-instance-name protocols bgp],
- [edit routing-instances routing-instance-name protocols bgp group group-name],
- [edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Option `delay-med-update` introduced in Junos OS Release 9.0.

**Description**
Specify the metric for all routes sent using the multiple exit discriminator (MED, or MULTI_EXIT_DISC) path attribute in update messages. This path attribute is used to discriminate among multiple exit points to a neighboring AS. If all other factors are equal, the exit point with the lowest metric is preferred.

You can specify a constant metric value by including the `metric` option. For configurations in which a BGP peer sends third-party next hops that require the local system to perform next-hop resolution—IBGP configurations, configurations within confederation peers, or EBGP configurations that include the `multihop` command—you can specify a variable metric by including the `minimum-igp` or `igp` option.

You can increase or decrease the variable metric calculated from the IGP metric (either from the `igp` or `minimum-igp` statement) by specifying a value for `offset`. The metric is increased by specifying a positive value for `offset`, and decreased by specifying a negative value for `offset`.

In Junos OS Release 9.0 and later, you can specify that a BGP group or peer not advertise updates for the MED path attributes used to calculate IGP costs for BGP next hops unless the MED is lower. You can also configure an interval to delay when MED updates are sent by including the `med-igp-update-interval minutes` statement at the `[edit routing-options]` hierarchy level.

**Options**
- `delay-med-update`—Specify that a BGP group or peer configured with the `metric-out igp` statement not advertise MED updates unless the current MED value is lower than
the previously advertised MED value, or another attribute associated with the route has changed, or the BGP peer is responding to a refresh route request.

NOTE: You cannot configure the `delay-med-update` statement at the global BGP level.

**igp**—Set the metric to the most recent metric value calculated in the IGP to get to the BGP next hop. Routes learned from an EBGP peer usually have a next hop on a directly connected interface and thus the IGP value is equal to zero. This is the value advertised.

**metric**—Primary metric on all routes sent to peers.

Range: 0 through 4,294,967,295 \((2^{32} - 1)\)

Default: No metric is sent.

**minimum-igp**—Set the metric to the minimum metric value calculated in the IGP to get to the BGP next hop. If a newly calculated metric is greater than the minimum metric value, the metric value remains unchanged. If a newly calculated metric is lower, the metric value is lowered to that value. When you change a neighbor’s export policy from any configuration to a configuration that sets the minimum IGP offset on an exported route, the advertised MED is not updated if the value would increase as a result, even if the previous configuration does not use a minimum IGP-based MED value. This behavior helps to prevent unnecessary route flapping when an IGP cost changes, by not forcing a route update if the metric value increases past the previous lowest known value.

**offset**—Increases or decreases the metric by this value.

Range: \(-2^{31}\) through \(2^{31} - 1\)

Default: None

**Required Privilege**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- *Example: Associating the MED Path Attribute with the IGP Metric and Delaying MED Updates*
- *Examples: Configuring BGP MED*
- *Example: Configuring the MED Attribute Directly*
- *Understanding the MED Attribute*
- *med-igp-update-interval on page 3078*
**mtu-discovery**

**Syntax**

```plaintext
mtu-discovery;
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure TCP path maximum transmission unit (MTU) discovery.

TCP path MTU discovery enables BGP to automatically discover the best TCP path MTU for each BGP session. In Junos OS, TCP path MTU discovery is disabled by default for all BGP neighbor sessions.

When MTU discovery is disabled, TCP sessions that are not directly connected transmit packets of 512-byte maximum segment size (MSS). These small packets minimize the chances of packet fragmentation at a device along the path to the destination. However, because most links use an MTU of at least 1500 bytes, 512-byte packets do not result in the most efficient use of link bandwidth. For directly connected EBGP sessions, MTU mismatches prevent the BGP session from being established. As a workaround, enable path MTU discovery within the EBGP group.

Path MTU discovery dynamically determines the MTU size on the network path between the source and the destination, with the goal of avoiding IP fragmentation. Path MTU discovery works by setting the Don’t Fragment (DF) bit in the IP headers of outgoing packets. When a device along the path has an MTU that is smaller than the packet, the device drops the packet. The device also sends back an ICMP Fragmentation Needed (Type 3, Code 4) message that contains the device’s MTU, thus allowing the source to reduce its path MTU appropriately. The process repeats until the MTU is small enough to traverse the entire path without fragmentation.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.
Related Documentation

- Example: Limiting TCP Segment Size for BGP
- Configuring the Junos OS for IPv6 Path MTU Discovery
- Configuring the Junos OS for Path MTU Discovery on Outgoing GRE Tunnel Connections
**multihop**

**Syntax**

```plaintext
multihop {
    no-nexthop-change;
    ttl ttl-value;
}
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols bgp]`
- `[edit logical-systems logical-system-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]`
- `[edit protocols bgp]`
- `[edit protocols bgp group group-name]`
- `[edit protocols bgp group group-name neighbor address]`
- `[edit routing-instances routing-instance-name protocols bgp]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]`

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure an EBGP multihop session.

For Layer 3 VPNs, you configure the EBGP multihop session between the PE and CE routing devices. This allows you to configure one or more routing devices between the PE and CE routing devices.

An external confederation peer is a special case that allows unconnected third-party next hops. You do not need to configure multihop sessions explicitly in this particular case because multihop behavior is implied.

If you have external BGP confederation peer-to-loopback addresses, you still need the multihop configuration.

---

**NOTE:** You cannot configure the accept-remote-nexthop statement at the same time.

---

**Default**

If you omit this statement, all EBGP peers are assumed to be directly connected (that is, you are establishing a nonmultihop, or “regular,” BGP session), and the default time-to-live (TTL) value is 1.
The remaining statements are explained separately.

<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>routing-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

Related Documentation

- Example: Configuring EBGP Multihop Sessions
- Configuring EBGP Multihop Sessions Between PE and CE Routers in Layer 3 VPNs
- accept-remote-nexthop on page 2562
- no-nexthop-change
- ttl
multipath (Protocols BGP)

Syntax

```
multipath {
  multiple-as;
  vpn-unequal-cost equal-external-internal;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Allow load sharing among multiple EBGP paths and multiple IBGP paths. A path is considered a BGP equal-cost path (and will be used for forwarding) if a tie-break is performed. The tie-break is performed after the BGP route path selection step that chooses the next-hop path that is resolved through the IGP route with the lowest metric. All paths with the same neighboring AS, learned by a multipath-enabled BGP neighbor, are considered.

Options

- `multiple-as`—Disable the default check requiring that paths accepted by BGP multipath must have the same neighboring AS.

- `vpn-unequal-cost equal-external-internal`—Enable load-balancing in a Layer 3 VPN with unequal cost paths.

Required Privilege Level

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation

- Understanding BGP Path Selection
- Example: Load Balancing BGP Traffic
neighbor (Protocols BGP)

Syntax

neighbor address {
    accept-remote-nexthop;
    advertise-external <conditional>;
    advertise-inactive;
    (advertise-peer-as | no-advertise-peer-as);
    as-override;
    authentication-algorithm algorithm;
    authentication-key key;
    authentication-key-chain key-chain;
    cluster cluster-identifier;
    damping;
    description text-description;
    export [policy-names ];
    family {
        (inet | inet6 | inet-mvpn | inet6-mpvn | inet-vpn | iso-vpn | l2-vpn) {
            (any | flow | multicast | unicast | signaling) {
                accepted-prefix-limit {
                    maximum number;
                    teardown <percentage> <idle-timeout (forever | minutes)>;
                }
                damping;
                prefix-limit {
                    maximum number;
                    teardown <percentage> <idle-timeout (forever | minutes)>;
                }
                rib-group group-name;
                topology name {
                    community {
                        target identifier;
                    }
                }
            }
            flow {
                no-validate policy-name;
            }
            labeled-unicast {
                accepted-prefix-limit {
                    maximum number;
                    teardown <percentage> <idle-timeout (forever | minutes)>;
                }
                aggregate-label {
                    community community-name:
                }
                explicit-null {
                    connected-only;
                }
                prefix-limit {
                    maximum number;
                    teardown <percentage> <idle-timeout (forever | minutes)>;
                }
            }
            resolve-vpn;
            rib inet.3;
rib-group group-name;
topology name {
   community {
      target identifier;
   }
}
}
route-target {
   advertise-default;
   external-paths number;
   accepted-prefix-limit {
      maximum number;
      teardown <percentage> <idle-timeout (forever | minutes)>;
   }
   prefix-limit {
      maximum number;
      teardown <percentage> <idle-timeout (forever | minutes)>;
   }
}
signaling {
   prefix-limit {
      maximum number;
      teardown <percentage> <idle-timeout (forever | minutes)>;
   }
}
}
graceful-restart {
   disable;
   restart-time seconds;
   stale-routes-time seconds;
}
hold-time seconds;
import [ policy-names ];
ipsec-sa ipsec-sa;
keep (all | none);
local-address address;
local-as autonomous-system <private>;
local-interface interface-name;
local-preference preference;
log-updown;
metric-out ( metric | minimum-igp <offset> | igp <offset> );
mtu-discovery;
multipath <ttl-value>;
multipath {
   multiple-as;
}
no-aggregator-id;
no-client-reflect;
out-delay seconds;
passive;
peer-as autonomous-system;
preference preference;
tcp-mss segment-size;
traceoptions {
   file filename <files number> <size size> <world-readable | no-world-readable>;}
flag flag <flag-modifier> <disable>;
}  
vpn-apply-export;
}

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Explicitly configure a neighbor (peer). To configure multiple BGP peers, include multiple neighbor statements.

By default, the peer’s options are identical to those of the group. You can override these options by including peer-specific option statements within the neighbor statement.

The neighbor statement is one of the statements you can include in the configuration to define a minimal BGP configuration on the routing device. (You can include an allow all statement in place of a neighbor statement.)

Options

address—IPv6 or IPv4 address of a single peer.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• BGP Feature Guide for Routing Devices
**no-aggregator-id**

**Syntax**
```
no-aggregator-id;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Prevent different routing devices within an AS from creating aggregate routes that contain different AS paths.

Junos OS performs route aggregation, which is the process of combining the characteristics of different routes so that only a single route is advertised. Aggregation reduces the amount of information that BGP must store and exchange with other BGP systems. When aggregation occurs, the local routing device adds the local AS number and the router ID to the aggregator path attribute. The `no-aggregator-id` statement causes Junos OS to place a 0 in the router ID field and thus eliminate the possibility of having multiple aggregate advertisements in the network, each with different path information.

**Default**
If you omit this statement, the router ID is included in the BGP aggregator path attribute.

**Required Privilege Level**
```
route—To view this statement in the configuration.
route-control—To add this statement to the configuration.
```

**Related Documentation**
- BGP Messages Overview
no-client-reflect

**Syntax**

```plaintext
no-client-reflect;
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Disable intracluster route redistribution by the system acting as the route reflector. Include this statement when the client cluster is fully meshed to prevent the sending of redundant route advertisements. Route reflection provides a way to decrease BGP control traffic and minimizing the number of update messages sent within the AS.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring BGP Route Reflectors
- cluster on page 2583
no-validate

Syntax: no-validate policy-name;

Hierarchy Level: [edit protocols bgp group group-name family (inet | inet flow)],
[edit protocols bgp group group-name neighbor address family (inet | inet flow)],
[edit routing-instances routing-instance-name protocols bgp group group-name family (inet | inet flow)],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address family (inet | inet flow)]

Release Information: Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description: When BGP is carrying flow-specification network layer reachability information (NLRI) messages, the no-validate statement omits the flow route validation procedure after packets are accepted by a policy.

The receiving BGP-enabled device accepts a flow route if it passes the following criteria:

- The originator of a flow route matches the originator of the best match unicast route for the destination address that is embedded in the route.
- There are no more specific unicast routes, when compared to the destination address of the flow route, for which the active route has been received from a different next-hop autonomous system.

The first criterion ensures that the filter is being advertised by the next-hop used by unicast forwarding for the destination address embedded in the flow route. For example, if a flow route is given as 10.1.1.1, proto=6, port=80, the receiving BGP-enabled device selects the more specific unicast route in the unicast routing table that matches the destination prefix 10.1.1.1/32. On a unicast routing table containing 10.1/16 and 10.1.1/24, the latter is chosen as the unicast route to compare against. Only the active unicast route entry is considered. This follows the concept that a flow route is valid if advertised by the originator of the best unicast route.

The second criterion addresses situations in which a given address block is allocated to different entities. Flows that resolve to a best-match unicast route that is an aggregate route are only accepted if they do not cover more specific routes that are being routed to different next-hop autonomous systems.

You can bypass the validation process and use your own specific import policy. To disable the validation procedure and use an import policy instead, include the no-validate statement in the configuration.

Flow routes configured for VPNs with family inet-vpn are not automatically validated, so the no-validate statement is not supported at the [edit protocols bgp group group-name family inet-vpn] hierarchy level. No validation is needed if the flow routes are configured locally between devices in a single AS.
Options  *policy-name*—Import policy to match NLRI messages.

**Required Privilege**

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring Flow Routes*
**out-delay**

**Syntax**

```
out-delay seconds;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name
 neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Control how often BGP and the routing table exchange route information by specifying how long a route must be present in the Junos OS routing table before it is exported to BGP. Use this time delay to help bundle routing updates and to avoid sending updates too often.

Alternatively or in addition, external BGP (EBGP) sessions can also use the route-flap damping mechanism upon the reception of BGP messages coming from an external neighbor.

BGP stores the route information it receives from update messages in the routing table, and the routing table exports active routes from the routing table into BGP. BGP then advertises the exported routes to its peers. The `out-delay` statement enables a form of rate limiting. The delay is added to each update for each prefix individually. When a routing device changes its best path to a destination prefix, the device does not inform its peer about the change unless the route has been present in its routing table for the specified `out-delay`. If you use `out-delay` to perform rate-limiting, you can expect a less bursty pattern of updates. You will see a pattern in which updates arrive in a steady flow, and two updates for the same prefix are always spaced by at least the `out-delay` timer value (for example, 30 seconds). Thus, the `out-delay` setting is useful for limiting oscillation (sometimes called churn) in a network. Keep in mind that, regardless of the `out-delay` setting, BGP peers exchange routes immediately after neighbor establishment. The `out-delay` setting is only designed to delay the exchange of routes between BGP and the local routing table.
Caution is warranted because an **out-delay** can delay convergence. If your network is configured in a way that avoids oscillation, setting an **out-delay** is not necessary.

When configured, the **out-delay** value displays as Outbound Timer when using `show bgp group` or `show bgp group neighbor` commands.

**Default**

By default, the exchange of route information between BGP and the routing table occurs immediately after the routes are received. This immediate exchange of route information might cause instabilities in the network reachability information. If you omit this statement, routes are exported to BGP immediately after they have been added to the routing table.

**Options**

- **seconds**—Output delay time.
  - **Range:** 0 through 65,535 seconds
  - **Default:** 0 seconds

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- keep on page 2607
outbound-route-filter

Syntax

outbound-route-filter {
    bgp-orf-cisco-mode;
    prefix-based {
        accept {
            (inet | inet6);
        }
    }
}

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure a BGP peer to accept outbound route filters from a remote peer.

Options

accept—Specify that outbound route filters from a BGP peer be accepted.
inet—Specify that IPv4 prefix-based outbound route filters be accepted.
inet6—Specify that IPv6 prefix-based outbound route filters be accepted.

NOTE: You can specify that both IPv4 and IPv6 outbound route filters be accepted.

prefix-based—Specify that prefix-based filters be accepted.

The bgp-orf-cisco-mode statement is explained separately.

Required Privilege

routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.
passive (Protocols BGP)

Syntax

```plaintext
passive;
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols bgp],
- [edit logical-systems logical-system-name protocols bgp group group-name],
- [edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
- [edit protocols bgp],
- [edit protocols bgp group group-name],
- [edit protocols bgp group group-name neighbor address],
- [edit routing-instances routing-instance-name protocols bgp],
- [edit routing-instances routing-instance-name protocols bgp group group-name],
- [edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure the routing device so that active open messages are not sent to the peer. Once you configure the routing device to be passive, the routing device will wait for the peer to issue an open request before a message is sent.

Default

If you omit this statement, all explicitly configured peers are active, and each peer periodically sends open requests until its peer responds.

Required Privilege Level

- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

Related Documentation

- Example: Preventing BGP Session Flaps When VPN Families Are Configured
**peer-as (Protocols BGP)**

**Syntax**

```
peer-as autonomous-system;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols bgp]
  `[edit logical-systems logical-system-name protocols bgp group group-name]
  `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address]
  `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]
  `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]
  `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]
  `[edit protocols bgp]
  `[edit protocols bgp group group-name]
  `[edit protocols bgp group group-name neighbor address]
  `[edit routing-instances routing-instance-name protocols bgp]
  `[edit routing-instances routing-instance-name protocols bgp group group-name]
  `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Specify the neighbor (peer) autonomous system (AS) number.

For EBGP, the peer is in another AS, so the AS number you specify in the `peer-as` statement must be different from the local router's AS number, which you specify in the `autonomous-system` statement. For IBGP, the peer is in the same AS, so the two AS numbers that you specify in the `autonomous-system` and `peer-as` statements must be the same.

The AS numeric range in plain-number format has been extended in Junos OS Release 9.1 to provide BGP support for 4-byte AS numbers, as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*. RFC 4893 introduces two new optional transitive BGP attributes, AS4_PATH and AS4_AGGREGATOR. These new attributes are used to propagate 4-byte AS path information across BGP speakers that do not support 4-byte AS numbers. RFC 4893 also introduces a reserved, well-known, 2-byte AS number, AS 23456. This reserved AS number is called AS_TRANS in RFC 4893. All releases of the Junos OS support 2-byte AS numbers.

In Junos OS Release 9.2 and later, you can also configure a 4-byte AS number using the AS-dot notation format of two integer values joined by a period: `<16-bit high-order value in decimal>.<16-bit low-order value in decimal>`. For example, the 4-byte AS number of 65,546 in plain-number format is represented as 1.10 in the AS-dot notation format.

With the introduction of 4-byte AS numbers, you might have a combination of routers that support 4-byte AS numbers and 2-byte AS numbers. For more information about what happens when establishing BGP peer relationships between 4-byte and 2-byte capable routers, see the following topics:
- *Using 4-Byte Autonomous System Numbers in BGP Networks Technology Overview.*

**Options**  
**autonomous-system**—AS number.  
**Range:** 1 through 4,294,967,295 \( (2^{32} - 1) \) in plain-number format for 4-byte AS numbers  
**Range:** 1 through 65,535 in plain-number format for 2-byte AS numbers (this is a subset of the 4-byte range)  
**Range:** 0.0 through 65535.65535 in AS-dot notation format for 4-byte AS numbers

**Required Privilege**  
**Level**  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**
**preference (Protocols BGP)**

**Syntax**

```
preference preference;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols bgp]`
- `[edit logical-systems logical-system-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]`
- `[edit protocols bgp]`
- `[edit protocols bgp group group-name]`
- `[edit protocols bgp group group-name neighbor address]`
- `[edit routing-instances routing-instance-name protocols bgp]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]`

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Specify the preference for routes learned from BGP.

At the BGP global level, the preference statement sets the preference for routes learned from BGP. You can override this preference in a BGP group or peer preference statement.

At the group or peer level, the preference statement sets the preference for routes learned from the group or peer. Use this statement to override the preference set in the BGP global preference statement when you want to favor routes from one group or peer over those of another.

**Options**

- `preference`—Preference to assign to routes learned from BGP or from the group or peer.
- **Range:** 0 through 4,294,967,295 (\(2^{32} - 1\))
- **Default:** 170 for the primary preference

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [local-preference on page 2616](#)
- [Example: Configuring the Preference Value for BGP Routes](#)
prefix-limit

Syntax

prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>;
}

Hierarchy Level

[edit logical-systems logical-system-name protocols bgp family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit logical-systems logical-system-name protocols bgp group group-name family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit protocols bgp family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit protocols bgp group group-name family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit protocols bgp group group-name neighbor address family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit routing-instances routing-instance-name protocols bgp family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit routing-instances routing-instance-name protocols bgp group group-name family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address family (inet | inet6) (any | flow | labeled-unicast | multicast | unicast)],

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Limit the number of prefixes received on a BGP peer session and a rate-limit logging when injected prefixes exceed a set limit.

This functionality is identical to the accepted-prefix-limit functionality except that it operates against received prefixes rather than accepted prefixes.

Options

maximum number—When you set the maximum number of prefixes, a message is logged when that number is exceeded.

Range: 1 through 4,294,967,295 ($2^{32} - 1$)

teardown <percentage>—If you include the teardown statement, the session is torn down when the maximum number of prefixes is reached. If you specify a percentage, messages are logged when the number of prefixes exceeds that percentage. After the session is torn down, it is reestablished in a short time unless you include the idle-timeout statement. Then the session can be kept down for a specified amount of time.
of time, or forever. If you specify forever, the session is reestablished only after you issue a clear bgp neighbor command.

Range: 1 through 100

idle-timeout (forever | timeout-in-minutes)—(Optional) If you include the idle-timeout statement, the session is torn down for a specified amount of time, or forever. If you specify a period of time, the session is allowed to reestablish after this timeout period. If you specify forever, the session is reestablished only after you intervene with a clear bgp neighbor command.

Range: 1 through 2400

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- accepted-prefix-limit
- Understanding Multiprotocol BGP
remove-private

Syntax
remove-private all replace nearest;

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp],
[edit logical-systems logical-system-name protocols bgp group group-name],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address],
[edit protocols bgp],
[edit protocols bgp group group-name],
[edit protocols bgp group group-name neighbor address],
[edit routing-instances routing-instance-name protocols bgp],
[edit routing-instances routing-instance-name protocols bgp group group-name],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
When advertising AS paths to remote systems, have the local system strip private AS numbers from the AS path. The numbers are stripped from the AS path starting at the left end of the AS path (the end where AS paths have been most recently added). The routing device stops searching for private ASs when it finds the first nonprivate AS or a peer's private AS. If the AS path contains the AS number of the external BGP (EBGP) neighbor, BGP does not remove the private AS number.

NOTE: As of Junos OS 10.0R2 and higher, if there is a need to send prefixes to an EBGP peer that has an AS number that matches an AS number in the AS path, consider using the as-override statement instead of the remove-private statement.

The operation takes place after any confederation member ASs have already been removed from the AS path, if applicable.

The Junos OS recognizes the set of AS numbers that is considered private, a range that is defined in the Internet Assigned Numbers Authority (IANA) assigned numbers document.

The set of reserved AS numbers is in the range from 64,512 through 65,535.

Options
all—Remove all private AS numbers from the original path. Do not stop the process of removing private AS numbers, even if a public AS number is encountered.
nearest—When you use the all and replace options, choose the last (right-most) public AS number encountered in the original AS path for the replacement value, as the AS path is processed from left to right. If no public AS number is encountered, the default replacement value is used. (See the replace option for information about the default replacement value.)

replace—When you use the all option, instead of removing private AS numbers, perform a replace operation. The default replacement value for the private AS number is the local AS number at the BGP group level for the BGP peer. If you are unsure about the replacement value, check the local AS value displayed in the output of the show bgp group group-name command.

Required Privilege
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Example: Removing Private AS Numbers from AS Paths
rib-group (Protocols BGP)

Syntax  
rib-group group-name;

Hierarchy Level
[edit logical-systems logical-system-name protocols bgp family inet (labeled-unicast | unicast | multicast)],
[edit logical-systems logical-system-name protocols bgp group group-name family inet (labeled-unicast | unicast | multicast)],
[edit logical-systems logical-system-name protocols bgp group group-name neighbor address family inet (labeled-unicast | unicast | multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp family inet (labeled-unicast | unicast | multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name family inet (labeled-unicast | unicast | multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address family inet (labeled-unicast | unicast | multicast)],
[edit protocols bgp family inet (labeled-unicast | unicast | multicast)],
[edit protocols bgp group group-name family inet (labeled-unicast | unicast | multicast)],
[edit protocols bgp group group-name neighbor address family inet (labeled-unicast | unicast | multicast)],
[edit routing-instances routing-instance-name protocols bgp family inet (labeled-unicast | unicast | multicast)],
[edit routing-instances routing-instance-name protocols bgp group group-name family inet (labeled-unicast | unicast | multicast)],
[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address family inet (labeled-unicast | unicast | multicast)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Add unicast prefixes to unicast and multicast tables.

Options
\textit{group-name}—Name of the routing table group. The name must start with a letter and can include letters, numbers, and hyphens. You generally specify only one routing table group.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- \textit{Example: Exporting Specific Routes from One Routing Table Into Another Routing Table}
- \textit{Example: Importing Direct and Static Routes Into a Routing Instance}
- \textit{Understanding Multiprotocol BGP}
tcp-mss (Protocols BGP)

Syntax  tcp-mss segment-size;

Hierarchy Level  [edit logical-systems logical-system-name protocols bgp],
                 [edit logical-systems logical-system-name protocols bgp group group-name],
                 [edit logical-systems logical-system-name protocols bgp group group-name neighbor neighbor-name],
                 [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp],
                 [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
                 [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor neighbor-name],
                 [edit protocols bgp],
                 [edit protocol bgp group group-name],
                 [edit protocols bgp group group-name neighbor neighbor-name],
                 [edit routing-instances routing-instance-name protocols bgp],
                 [edit routing-instances routing-instance-name protocols bgp group group-name],
                 [edit routing-instances routing-instance-name protocols bgp group group-name neighbor neighbor-name]

                      Statement introduced in Junos OS Release 9.0 for EX Series switches.
                      Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Configure the maximum segment size (MSS) for the TCP connection for BGP neighbors.
              The MSS is only valid in increments of 2 KB. The value used is based on the value set, but
              is rounded down to the nearest multiple of 2048.

Options  segment-size—MSS for the TCP connection.

Range:  1 through 4096

Required Privilege Level  routing—To view this statement in the configuration.
                          routing-control—To add this statement to the configuration.

Related Documentation  • Example: Limiting TCP Segment Size for BGP
traceoptions (Protocols BGP)

Syntax

```
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

- `[edit logical-systems logical-system-name protocols bgp]`
- `[edit logical-systems logical-system-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address]`
- `[edit protocols bgp]`
- `[edit protocols bgp group group-name]`
- `[edit protocols bgp group group-name neighbor address]`
- `[edit routing-instances routing-instance-name protocols bgp]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address]`

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
`4byte-as` statement introduced in Junos OS Release 9.2.
`4byte-as` statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Configure BGP protocol-level tracing options. To specify more than one tracing operation, include multiple flag statements.

**NOTE:** The `traceoptions` statement is not supported on QFabric systems.

Default

The default BGP protocol-level tracing options are inherited from the routing protocols `traceoptions` statement included at the `[edit routing-options]` hierarchy level. The default group-level trace options are inherited from the BGP protocol-level `traceoptions` statement. The default peer-level trace options are inherited from the group-level `traceoptions` statement.

Options

- **disable**—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as `all`.
- **file name**—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. We recommend that you place BGP tracing output in the file `bgp-log`.
files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Range: 2 through 1000 files
Default: 10 files

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

BGP Tracing Flags

• 4byte-as—4-byte AS events.
• bfd—BFD protocol events.
• damping—Damping operations.
• graceful-restart—Graceful restart events.
• keepalive—BGP keepalive messages. If you enable the the BGP update flag only, received keepalive messages do not generate a trace message.
• nsr-synchronization—Nonstop routing synchronization events.
• open—Open packets. These packets are sent between peers when they are establishing a connection.
• packets—All BGP protocol packets.
• refresh—BGP refresh packets.
• update—Update packets. These packets provide routing updates to BGP systems. If you enable only this flag, received keepalive messages do not generate a trace message. Use the keepalive flag to generate a trace message for keepalive messages.

Global Tracing Flags

• all—All tracing operations
• general—A combination of the normal and route trace operations
• normal—All normal operations

Default: If you do not specify this option, only unusual or abnormal operations are traced.

• policy—Policy operations and actions
• route—Routing table changes
• state—State transitions
• task—Routing protocol task processing
• timer—Routing protocol timer processing
flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Provide detailed trace information.
- **filter**—Provide filter trace information. Applies only to `route`, `damping`, and `update` tracing flags.
- **receive**—Trace the packets being received.
- **send**—Trace the packets being transmitted.

no-world-readable—(Optional) Prevent any user from reading the log file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When the `trace-file` again reaches its maximum size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option.

**Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

**Range:** 10 KB through the maximum file size supported on your system

**Default:** 128 KB

world-readable—(Optional) Allow any user to read the log file.

**Required Privilege Level**
- routing and trace—To view this statement in the configuration.
- routing-control and trace-control—To add this statement to the configuration.

**Related Documentation**
- log-updown on page 2617 statement
- Understanding Trace Operations for BGP Protocol Traffic
- Configuring OSPF Refresh and Flooding Reduction in Stable Topologies
type (Protocols BGP)

Syntax  

```
type type;
```

Hierarchy Level  

- [edit logical-systems logical-system-name protocols bgp group group-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name],
- [edit protocols bgp group group-name],
- [edit routing-instances routing-instance-name protocols bgp group group-name]

Release Information  

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  

Specify the type of BGP peer group.

When configuring a BGP group, you can indicate whether the group is an IBGP group or an EBGP group. All peers in an IBGP group are in the same AS, while peers in an EBGP group are in different ASs and normally share a subnet.

Options  

```
type—Type of group:
```
- **external**—External group, which allows inter-AS BGP routing
- **internal**—Internal group, which allows intra-AS BGP routing

Required Privilege Level  

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

Related Documentation  

- [BGP Feature Guide for Routing Devices](#)
Routine Monitoring

Monitoring BGP Routing Information

Purpose
Use the monitoring functionality to monitor BGP routing information on the routing device.

Action
To view BGP routing information in the J-Web interface, select Monitor > Routing > BGP Information.

To view BGP routing information in the CLI, enter the following commands:

- `show bgp summary`
- `show bgp neighbor`

Meaning
Table 330 on page 2649 summarizes key output fields in the BGP routing display in the J-Web interface.

Table 330: Summary of Key BGP Routing Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Peer Summary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Groups</td>
<td>Number of BGP groups.</td>
<td></td>
</tr>
<tr>
<td>Total Peers</td>
<td>Number of BGP peers.</td>
<td></td>
</tr>
<tr>
<td>Down Peers</td>
<td>Number of unavailable BGP peers.</td>
<td></td>
</tr>
<tr>
<td>Unconfigured Peers</td>
<td>Address of each BGP peer.</td>
<td></td>
</tr>
<tr>
<td>RIB Summary tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIB Name</td>
<td>Name of the RIB group.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 330: Summary of Key BGP Routing Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Prefixes</td>
<td>Total number of prefixes from the peer, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td>Active Prefixes</td>
<td>Number of prefixes received from the EBGP peers that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td>Suppressed Prefixes</td>
<td>Number of routes received from EBGP peers currently inactive because of damping or other reasons.</td>
<td></td>
</tr>
<tr>
<td>History Prefixes</td>
<td>History of the routes received or suppressed.</td>
<td></td>
</tr>
<tr>
<td>Dumped Prefixes</td>
<td>Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
<td></td>
</tr>
<tr>
<td>Pending Prefixes</td>
<td>Number of pending routes.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Status of the graceful restart process for this routing table: BGP restart is complete, BGP restart in progress, VPN restart in progress, or VPN restart is complete.</td>
<td></td>
</tr>
<tr>
<td>BGP Neighbors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Details</td>
<td>Click this button to view the selected BGP neighbor details.</td>
<td></td>
</tr>
<tr>
<td>Peer Address</td>
<td>Address of the BGP neighbor.</td>
<td></td>
</tr>
<tr>
<td>Autonomous System</td>
<td>AS number of the peer.</td>
<td></td>
</tr>
</tbody>
</table>
Table 330: Summary of Key BGP Routing Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer State</td>
<td>Current state of the BGP session:</td>
<td>Generally, the most common states are <strong>Active</strong>, which indicates a problem establishing the BGP connection, and <strong>Established</strong>, which indicates a successful session setup. The other states are transition states, and BGP sessions normally do not stay in those states for extended periods of time.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—BGP is initiating a TCP connection in an attempt to connect to a peer. If the connection is successful, BGP sends an open message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Connect</strong>—BGP is waiting for the TCP connection to become complete.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Established</strong>—The BGP session has been established, and the peers are exchanging BGP update messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Idle</strong>—This is the first stage of a connection. BGP is waiting for a Start event.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenConfirm</strong>—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenSent</strong>—BGP has sent an open message and is waiting to receive an open message from the peer.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Related Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed Time</td>
<td>Elapsed time since the peering session was last reset.</td>
<td>Configuring BGP Sessions (J-Web Procedure) on page 2557</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Layer 3 Protocols Supported on EX Series Switches on page 2553</td>
</tr>
</tbody>
</table>

**Operational Commands**
clear bgp damping

Syntax

```
clear bgp damping
  \<logical-system (all | logical-system-name)>
  \<prefix>
```

Syntax (EX Series Switch and QFX Series)

```
clear bgp damping
  \<prefix>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear BGP route flap damping information.

Options

- **none**—Clear all BGP route flap damping information.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **prefix**—(Optional) Clear route flap damping information for only the specified destination prefix.

Required Privilege

```
clear
```

Related Documentation

- show policy damping on page 2685
- show route damping on page 3170

List of Sample Output

```
clear bgp damping on page 2652
```

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear bgp damping

user@host> clear bgp damping
```
clear bgp neighbor

Syntax

```
clear bgp neighbor
  <as as-number>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <malformed-route>
  <neighbor>
  <soft | soft-inbound>
  <soft-minimum-igp>
```

Syntax (EX Series Switch and QFX Series)

```
clear bgp neighbor
  <as as-number>
  <instance instance-name>
  <malformed-route>
  <neighbor>
  <soft | soft-inbound>
  <soft-minimum-igp>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

```
malformed-route option introduced in Junos OS Release 13.2.
```

Description

Perform one of the following tasks:

- Change the state of one or more BGP neighbors to **IDLE**. For neighbors in the **ESTABLISHED** state, this command drops the TCP connection to the neighbors and then reestablishes the connection.

- (soft or soft-inbound keyword only) Reapply export policies or import policies, respectively, and send refresh updates to one or more BGP neighbors without changing their state.

Options

- **none**—Change the state of all BGP neighbors to **IDLE**.

- **as as-number**—(Optional) Apply this command only to neighbors in the specified autonomous system (AS).

- **instance instance-name**—(Optional) Apply this command only to neighbors for the specified routing instance.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

- **malformed-route**—(Optional) Remove malformed routes. If a specific neighbor is provided, Junos OS removes malformed routes for that particular neighbor. Otherwise, Junos OS removes malformed routes for all BGP neighbors. To find routes that have malformed attributes, run the **show route hidden** command, and look for routes marked with **MalformedAttr** in the AS path field.
**neighbor**—(Optional) IP address of a BGP peer. Apply this command only to the specified neighbor.

**soft**—(Optional) Reapply any export policies and send refresh updates to neighbors without clearing the state.

**soft-inbound**—(Optional) Reapply any import policies and send refresh updates to neighbors without clearing the state.

**soft-minimum-igp**—(Optional) Provides soft refresh of the outbound state when the interior gateway protocol (IGP) metric is reset.

**Required Privilege Level**

**clear**

**Related Documentation**

- show bgp neighbor on page 2666

**List of Sample Output**

**clear bgp neighbor on page 2654**

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
clear bgp neighbor
```

```
user@host> clear bgp neighbor
```
**clear bgp table**

**Syntax**

```
clear bgp table table-name
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and QFX Series)**

`clear bgp table table-name`

**Release Information**

Command introduced in Junos OS Release 9.0.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Request that BGP refresh routes in a specified routing table.

**Options**

`logical-system (all | logical-system-name)`: (Optional) Perform this operation on all logical systems or on a particular logical system.

`table-name`: Request that BGP refresh routes in the specified table.

**Additional Information**

In some cases, a prefix limit is associated with a routing table for a VPN instance. When this limit is exceeded (for example, because of a network misconfiguration), some routes might not be inserted in the table. Such routes need to be added to the table after the network issue is resolved. Use the `clear bgp table` command to request that BGP refresh routes in a VPN instance table.

**Required Privilege**

`clear`

**List of Sample Output**

- `clear bgp table private.inet.0 on page 2655`
- `clear bgp table inet.6 logical-system all on page 2655`
- `clear bgp table private.inet.6 logical-system ls1 on page 2655`
- `clear bgp table logical-system all inet.0 on page 2655`
- `clear bgp table logical-system ls2 private.inet.0 on page 2656`

**Output Fields**

This command produces no output.

**Sample Output**

```
clear bgp table private.inet.0
    user@host> clear bgp table private.inet.0

clear bgp table inet.6 logical-system all
    user@host> clear bgp table inet.6 logical-system all

clear bgp table private.inet.6 logical-system ls1
    user@host> clear bgp table private.inet.6 logical-system ls1

clear bgp table logical-system all inet.0
    user@host> clear bgp table logical-system all inet.0
```
clear bgp table logical-system ls2 private.inet.0

user@host> clear bgp table logical-system ls2 private.inet.0
show bgp bmp

Syntax: show bgp bmp

Release Information

Description
Display information about the BGP Monitoring Protocol (BMP).

Options
This command has no options.

Required Privilege
view

List of Sample Output: show bgp bmp on page 2657

Output Fields
Table 331 on page 2657 lists the output fields for the show bgp bmp command. Output fields are listed in the approximate order in which they appear.

Table 331: show bgp bmp Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMP station address/port</td>
<td>IP address and port number of the monitoring station to which BGP Monitoring Protocol (BMP) statistics are sent.</td>
</tr>
<tr>
<td>BMP session state</td>
<td>Status of the BMP session: UP or DOWN.</td>
</tr>
<tr>
<td>Memory consumed by BMP</td>
<td>Memory used by the active BMP session.</td>
</tr>
<tr>
<td>Statistics timeout</td>
<td>Amount of time, in seconds, between transmissions of BMP data to the monitoring station.</td>
</tr>
<tr>
<td>Memory limit</td>
<td>Threshold, in bytes, at which the routing device stops collecting BMP data.</td>
</tr>
<tr>
<td>Memory-connect retry timeout</td>
<td>Amount of time, in seconds, after which the routing device attempts to resume a BMP session that was ended after the configured memory threshold was exceeded.</td>
</tr>
</tbody>
</table>

Sample Output

show bgp bmp

user@host> show bgp bmp
BMP station address/port: 172.24.24.157+5454
BMP session state: DOWN
Memory consumed by BMP: 0
Statistics timeout: 15
Memory limit: 10485760
Memory connect retry timeout: 600
### show bgp group

**Syntax**

```
show bgp group
<brief | detail | summary>
<group-name>
<exact-instance instance-name>
<instance instance-name>
<logical-system (all | logical-system-name)>
<rtf>
```

**Syntax (EX Series Switch and QFX Series)**

```
show bgp group
<brief | detail | summary>
<group-name>
<exact-instance instance-name>
<instance instance-name>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- `exact-instance` option introduced in Junos OS Release 11.4.

**Description**

Display information about the configured BGP groups.

**Options**

- `none`—Display group information about all BGP groups.
  - `brief | detail | summary`—(Optional) Display the specified level of output.
  - `group-name`—(Optional) Display group information for the specified group.
  - `exact-instance instance-name`—(Optional) Display information for the specified instance only.
  - `instance instance-name`—(Optional) Display information about BGP groups for all routing instances whose name begins with this string (for example, `cust1`, `cust11`, and `cust111` are all displayed when you run the `show bgp group instance cust1` command). The instance name can be master for the main instance, or any valid configured instance name or its prefix.
  - `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
  - `rtf`—(Optional) Display BGP group route targeting information.

**Required Privilege Level**

- `view`

**List of Sample Output**

- `show bgp group` on page 2663
- `show bgp group brief` on page 2663
- `show bgp group detail` on page 2664
- `show bgp group rtf detail` on page 2665
- `show bgp group summary` on page 2665
Output Fields  Table 332 on page 2660 describes the output fields for the `show bgp group` command. Output fields are listed in the approximate order in which they appear.

**Table 332: show bgp group Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Type or Group</strong></td>
<td>Type of BGP group: Internal or External.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>group-index</strong></td>
<td>Index number for the BGP peer group. The index number differentiates between groups when a single BGP group is split because of different configuration options at the group and peer levels.</td>
<td>rtfdetail</td>
</tr>
<tr>
<td><strong>AS</strong></td>
<td>AS number of the peer. For internal BGP (IBGP), this number is the same as Local AS.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Local AS</strong></td>
<td>AS number of the local routing device.</td>
<td>none</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Name of a specific BGP group.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>Unique index number of a BGP group.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Flags</strong></td>
<td>Flags associated with the BGP group. This field is used by Juniper Networks customer support.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Remove-private options</strong></td>
<td>Options associated with the <code>remove-private</code> statement.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Holdtime</strong></td>
<td>Maximum number of seconds allowed to elapse between successive keepalive or update messages that BGP receives from a peer in the BGP group, after which the connection to the peer is closed and routing devices through that peer become unavailable.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Export policies configured for the BGP group with the <code>export</code> statement.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>MED tracks IGP metric update delay</strong></td>
<td>Time, in seconds, that updates to multiple exit discriminator (MED) are delayed. Also displays the time remaining before the interval is set to expire</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Traffic Statistics Interval</strong></td>
<td>Time between sample periods for labeled-unicast traffic statistics, in seconds.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Total peers</strong></td>
<td>Total number of peers in the group.</td>
<td>brief detail</td>
</tr>
<tr>
<td><strong>Established</strong></td>
<td>Number of peers in the group that are in the established state.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 332: show bgp group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active/Received/Accepted/Damped</strong></td>
<td>Multipurpose field that displays information about BGP peer sessions. The field’s contents depend upon whether a session is established and whether it was established in the main routing device or in a routing instance.</td>
<td>summary</td>
</tr>
<tr>
<td></td>
<td>• If a peer is not established, the field shows the state of the peer session: <strong>Active</strong>, <strong>Connect</strong>, or <strong>Idle</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If a BGP session is established in the main routing device, the field shows the number of active, received, accepted, and damped routes that are received from a neighbor and appear in the inet.0 (main) and inet.2 (multicast) routing tables. For example, 8/10/10/2 and 2/4/4/0 indicate the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 8 active routes, 10 received routes, 10 accepted routes, and 2 damped routes from a BGP peer appear in the inet.0 routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 active routes, 4 received routes, 4 accepted routes, and no damped routes from a BGP peer appear in the inet.2 routing table.</td>
<td></td>
</tr>
<tr>
<td><strong>ip-addresses</strong></td>
<td>List of peers who are members of the group. The address is followed by the peer’s port number.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Route Queue Timer</strong></td>
<td>Number of seconds until queued routes are sent. If this time has already elapsed, this field displays the number of seconds by which the updates are delayed.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Route Queue</strong></td>
<td>Number of prefixes that are queued up for sending to the peers in the group.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>inet.number</strong></td>
<td>Number of active, received, accepted, and damped routes in the routing table. For example, <strong>inet.0: 7/10/9/0</strong> indicates the following:</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• 7 active routes, 10 received routes, 9 accepted routes, and no damped routes from a BGP peer appear in the inet.0 routing table.</td>
<td></td>
</tr>
</tbody>
</table>
## Table 332: show bgp group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table inet.number</strong></td>
<td>Information about the routing table.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• <strong>Received prefixes</strong> — Total number of prefixes from the peer, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active prefixes</strong> — Number of prefixes received from the peer that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Suppressed due to damping</strong> — Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Advertised prefixes</strong> — Number of prefixes advertised to a peer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Received external prefixes</strong> — Total number of prefixes from the external BGP (EBGP) peers, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active external prefixes</strong> — Number of prefixes received from the EBGP peers that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Externals suppressed</strong> — Number of routes received from EBGP peers currently inactive because of damping or other reasons.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Received internal prefixes</strong> — Total number of prefixes from the IBGP peers, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Active internal prefixes</strong> — Number of prefixes received from the IBGP peers that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Internals suppressed</strong> — Number of routes received from IBGP peers currently inactive because of damping or other reasons.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RIB State</strong> — Status of the graceful restart process for this routing table: <strong>BGPrestart is complete</strong>, <strong>BGPrestart in progress</strong>, <strong>VPN restart in progress</strong>, or <strong>VPN restart is complete</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Groups</th>
<th>Total number of groups.</th>
<th>All levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peers</td>
<td>Total number of peers.</td>
<td>All levels</td>
</tr>
<tr>
<td>External</td>
<td>Total number of external peers.</td>
<td>All levels</td>
</tr>
<tr>
<td>Internal</td>
<td>Total number of internal peers.</td>
<td>All levels</td>
</tr>
<tr>
<td>Down peers</td>
<td>Total number of unavailable peers.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flaps</td>
<td>Total number of flaps that occurred.</td>
<td>All levels</td>
</tr>
<tr>
<td>Table</td>
<td>Name of a routing table.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Tot Paths</td>
<td>Total number of routes.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Act Paths</td>
<td>Number of active routes.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
<td>brief, none</td>
</tr>
</tbody>
</table>
Table 332: show bgp group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td>Number of withdrawn routes stored locally to keep track of damping history.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Damp State</td>
<td>Number of active routes with a figure of merit greater than zero, but lower than</td>
<td>brief, none</td>
</tr>
<tr>
<td></td>
<td>the threshold at which suppression occurs.</td>
<td></td>
</tr>
<tr>
<td>Pending</td>
<td>Routes being processed by the BGP import policy.</td>
<td>brief, none</td>
</tr>
<tr>
<td>Group</td>
<td>Group the peer belongs to in the BGP configuration.</td>
<td>detail</td>
</tr>
<tr>
<td>Receive mask</td>
<td>Mask of the received target included in the advertised route.</td>
<td>detail</td>
</tr>
<tr>
<td>Entries</td>
<td>Number of route entries received.</td>
<td>detail</td>
</tr>
<tr>
<td>Target</td>
<td>Route target that is to be passed by route-target filtering. If a route advertised</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>from the provider edge (PE) routing device matches an entry in the route-target filter, the route is passed to the peer.</td>
<td></td>
</tr>
<tr>
<td>Mask</td>
<td>Mask which specifies that the peer receive routes with the given route target.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

**show bgp group**

```
user@host> show bgp group
Groups: 2  Peers: 2    External: 0    Internal: 2    Down peers: 1   Flaps: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0          0          0          0          0          0          0
bgp.l3vpn.0      0          0          0          0          0          0
bgp.rtarget.0    2          0          0          0          0          0
```

**show bgp group brief**

```
user@host> show bgp group brief
Groups: 2  Peers: 2    External: 0    Internal: 2    Down peers: 1   Flaps: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0          0          0          0          0          0          0
bgp.l3vpn.0      0          0          0          0          0          0
```
show bgp group detail

user@host> show bgp group detail
Group Type: Internal    AS: 1                      Local AS: 1
    Name: ibgp            Index: 0                   Flags: <Export Eval>
    Holdtime: 0           Total peers: 3        Established: 0
    22.0.0.2
    22.0.0.8
    22.0.0.5

    Groups: 1  Peers: 3    External: 0    Internal: 3    Down peers: 3   Flaps: 3

    Table bgp.l3vpn.0
    Received prefixes: 0
    Accepted prefixes: 0
    Active prefixes: 0
    Suppressed due to damping: 0
    Received external prefixes: 0
    Active external prefixes: 0
    Externals suppressed: 0
    Received internal prefixes: 0
    Active internal prefixes: 0
    Internals suppressed: 0
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete

    Table bgp.mdt.0
    Received prefixes: 0
    Accepted prefixes: 0
    Active prefixes: 0
    Suppressed due to damping: 0
    Received external prefixes: 0
    Active external prefixes: 0
    Externals suppressed: 0
    Received internal prefixes: 0
    Active internal prefixes: 0
    Internals suppressed: 0
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete

    Table VPN-A.inet.0
    Received prefixes: 0
    Accepted prefixes: 0
    Active prefixes: 0
    Suppressed due to damping: 0
    Received external prefixes: 0
    Active external prefixes: 0
    Externals suppressed: 0
    Received internal prefixes: 0
    Active internal prefixes: 0
    Internals suppressed: 0
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete

    Table VPN-A.mdt.0
    Received prefixes: 0
    Accepted prefixes: 0
    Active prefixes: 0
    Suppressed due to damping: 0
    Received external prefixes: 0
    Active external prefixes: 0
    Externals suppressed: 0
    Received internal prefixes: 0
    Active internal prefixes: 0
    Internals suppressed: 0
    RIB State: BGP restart is complete
    RIB State: VPN restart is complete
show bgp group rtf detail

user@host> show bgp group rtf detail
Group: internal (group-index: 0)
  Table: bgp.rtarget.0
  Entries: 2
  Target          Mask
  100:100/64      00000002
  200:201/64      (Group)

Group: internal (group-index: 1)
  Table: bgp.rtarget.0
  Entries: 1
  Target          Mask
  200:201/64      (Group)

show bgp group summary

user@host> show bgp group summary
Group  Type    Peers  Established  Active/Received/Accepted/Damped
ibgp    Internal 3        0

Groups: 1  Peers: 3  External: 0  Internal: 3  Down peers: 3  Flaps: 3
bgp.13vpn.0 : 0/0/0/0 External: 0/0/0/0 Internal: 0/0/0/0
bgp.mdt.0   : 0/0/0/0 External: 0/0/0/0 Internal: 0/0/0/0
VPN-A.inet.0: 0/0/0/0 External: 0/0/0/0 Internal: 0/0/0/0
VPN-A.mdt.0 : 0/0/0/0 External: 0/0/0/0 Internal: 0/0/0/0
**show bgp neighbor**

**Syntax**
```
show bgp neighbor
<exact-instance instance-name>
<instance instance-name>
<logical-system (all | logical-system-name)>
<neighbor-address>
<orf (detail | neighbor-address)
```

**Syntax (EX Series Switch and QFX Series)**
```
show bgp neighbor
<instance instance-name>
<exact-instance instance-name>
<neighbor-address>
<orf (neighbor-address | detail)
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- orf option introduced in Junos OS Release 9.2.
- exact-instance option introduced in Junos OS Release 11.4.

**Description**
Display information about BGP peers.

**Options**
- **none**—Display information about all BGP peers.
- **exact-instance instance-name**—(Optional) Display information for the specified instance only.
- **instance instance-name**—(Optional) Display information about BGP peers for all routing instances whose name begins with this string (for example, cust1, cust11, and cust111 are all displayed when you run the `show bgp neighbor instance cust1` command).
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **neighbor-address**—(Optional) Display information for only the BGP peer at the specified IP address.
- **orf (detail | neighbor-address)**—(Optional) Display outbound route-filtering information for all BGP peers or only for the BGP peer at the specified IP address. The default is to display brief output. Use the **detail** option to display detailed output.

**Additional Information**
For information about the `local-address`, `nlri`, `hold-time`, and `preference` statements, see the Junos OS Routing Protocols Library for Routing Devices.

**Required Privilege Level**
view

**Related Documentation**
- clear bgp neighbor on page 2653
Output Fields

Table 333 on page 2667 describes the output fields for the `show bgp neighbor` command. Output fields are listed in the approximate order in which they appear.

Table 333: show bgp neighbor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>Address of the BGP neighbor. The address is followed by the neighbor port number.</td>
</tr>
<tr>
<td>AS</td>
<td>AS number of the peer.</td>
</tr>
<tr>
<td>Local</td>
<td>Address of the local routing device. The address is followed by the peer port number.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of peer: <strong>Internal</strong> or <strong>External</strong>.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an Open message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connect</strong>—BGP is waiting for the transport protocol connection to be completed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Established</strong>—The BGP session has been established, and the peers are exchanging update messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Idle</strong>—This is the first stage of a connection. BGP is waiting for a Start event.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenConfirm</strong>—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenSent</strong>—BGP has sent an open message and is waiting to receive an open message from the peer.</td>
</tr>
<tr>
<td>Flags</td>
<td>Internal BGP flags:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Aggregate Label</strong>—BGP has aggregated a set of incoming labels (labels received from the peer) into a single forwarding label.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CleanUp</strong>—The peer session is being shut down.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Delete</strong>—This peer has been deleted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Idled</strong>—This peer has been permanently idled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ImportEval</strong>—At the last commit operation, this peer was identified as needing to reevaluate all received routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Initializing</strong>—The peer session is initializing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SendRtn</strong>—Messages are being sent to the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sync</strong>—This peer is synchronized with the rest of the peer group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TryConnect</strong>—Another attempt is being made to connect to the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unconfigured</strong>—This peer is not configured.</td>
</tr>
<tr>
<td></td>
<td>• <strong>WriteFailed</strong>—An attempt to write to this peer failed.</td>
</tr>
</tbody>
</table>
Table 333: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last state</strong></td>
<td>Previous state of the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—BGP is initiating a transport protocol connection in an attempt to connect to a peer. If the connection is successful, BGP sends an Open message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Connect</strong>—BGP is waiting for the transport protocol connection to be completed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Established</strong>—The BGP session has been established, and the peers are exchanging update messages.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Idle</strong>—This is the first stage of a connection. BGP is waiting for a Start event.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenConfirm</strong>—BGP has acknowledged receipt of an open message from the peer and is waiting to receive a keepalive or notification message.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenSent</strong>—BGP has sent an open message and is waiting to receive an open message from the peer.</td>
</tr>
<tr>
<td><strong>Last event</strong></td>
<td>Last activity that occurred in the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Closed</strong>—The BGP session closed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ConnectRetry</strong>—The transport protocol connection failed, and BGP is trying again to connect.</td>
</tr>
<tr>
<td></td>
<td>• <strong>HoldTime</strong>—The session ended because the hold timer expired.</td>
</tr>
<tr>
<td></td>
<td>• <strong>KeepAlive</strong>—The local routing device sent a BGP keepalive message to the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Open</strong>—The local routing device sent a BGP open message to the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OpenFail</strong>—The local routing device did not receive an acknowledgment of a BGP open message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RecvKeepAlive</strong>—The local routing device received a BGP keepalive message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RecvNotify</strong>—The local routing device received a BGP notification message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RecvOpen</strong>—The local routing device received a BGP open message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RecvUpdate</strong>—The local routing device received a BGP update message from the peer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Start</strong>—The peering session started.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Stop</strong>—The peering session stopped.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TransportError</strong>—A TCP error occurred.</td>
</tr>
<tr>
<td><strong>Last error</strong></td>
<td>Last error that occurred in the BGP session:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cease</strong>—An error occurred, such as a version mismatch, that caused the session to close.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Finite State Machine Error</strong>—In setting up the session, BGP received a message that it did not understand.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hold Time Expired</strong>—The session's hold time expired.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Message Header Error</strong>—The header of a BGP message was malformed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Open Message Error</strong>—A BGP open message contained an error.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—No errors occurred in the BGP session.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Update Message Error</strong>—A BGP update message contained an error.</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>Name of the export policy that is configured on the peer.</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>Name of the import policy that is configured on the peer.</td>
</tr>
</tbody>
</table>
Table 333: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Configured BGP options:</td>
</tr>
<tr>
<td></td>
<td>• AddressFamily—Configured address family: inet or inet-vpn.</td>
</tr>
<tr>
<td></td>
<td>• AuthKeyChain—Authentication key change is enabled.</td>
</tr>
<tr>
<td></td>
<td>• DropPathAttributes—Certain path attributes are configured to be dropped from</td>
</tr>
<tr>
<td></td>
<td>neighbor updates during inbound processing.</td>
</tr>
<tr>
<td></td>
<td>• GracefulRestart—Graceful restart is configured.</td>
</tr>
<tr>
<td></td>
<td>• HoldTime—Hold time configured with the hold-time statement. The hold time is</td>
</tr>
<tr>
<td></td>
<td>three times the interval at which keepalive messages are sent.</td>
</tr>
<tr>
<td></td>
<td>• IgnorePathAttributes—Certain path attributes are configured to be ignored in</td>
</tr>
<tr>
<td></td>
<td>neighbor updates during inbound processing.</td>
</tr>
<tr>
<td></td>
<td>• Local Address—Address configured with the local-address statement.</td>
</tr>
<tr>
<td></td>
<td>• Multihop—Allow BGP connections to external peers that are not on a directly</td>
</tr>
<tr>
<td></td>
<td>connected network.</td>
</tr>
<tr>
<td></td>
<td>• NLRI—Configured MBGP state for the BGP group: multicast, unicast, or both if</td>
</tr>
<tr>
<td></td>
<td>you have configured nlr any.</td>
</tr>
<tr>
<td></td>
<td>• Peer AS—Configured peer autonomous system (AS).</td>
</tr>
<tr>
<td></td>
<td>• Preference—Preference value configured with the preference statement.</td>
</tr>
<tr>
<td></td>
<td>• Refresh—Configured to refresh automatically when the policy changes.</td>
</tr>
<tr>
<td></td>
<td>• Rib-group—Configured routing table group.</td>
</tr>
<tr>
<td>Path-attributes dropped</td>
<td>Path attribute codes that are dropped from neighbor updates.</td>
</tr>
<tr>
<td>Path-attributes ignored</td>
<td>Path attribute codes that are ignored during neighbor updates.</td>
</tr>
<tr>
<td>Authentication key change</td>
<td>(appears only if the authentication-keychain statement has been configured) Name of</td>
</tr>
<tr>
<td></td>
<td>the authentication keychain enabled.</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>(appears only if the authentication-algorithm statement has been configured) Type</td>
</tr>
<tr>
<td></td>
<td>of authentication algorithm enabled: hmac or md5.</td>
</tr>
<tr>
<td>Address families configured</td>
<td>Names of configured address families for the VPN.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Address of the local routing device.</td>
</tr>
<tr>
<td>Remove-private options</td>
<td>Options associated with the remove-private statement.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Hold time configured with the hold-time statement. The hold time is three times</td>
</tr>
<tr>
<td></td>
<td>the interval at which keepalive messages are sent.</td>
</tr>
<tr>
<td>Flags for NLRI</td>
<td>Flags related to labeled-unicast:</td>
</tr>
<tr>
<td>inet-label-unicast</td>
<td>• TrafficStatistics—Collection of statistics for labeled-unicast traffic is</td>
</tr>
<tr>
<td></td>
<td>enabled.</td>
</tr>
</tbody>
</table>
Table 333: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic statistics</td>
<td>Information about labeled-unicast traffic statistics:</td>
</tr>
<tr>
<td>• Options</td>
<td>Options configured for collecting statistics about labeled-unicast traffic.</td>
</tr>
<tr>
<td>• File</td>
<td>Name and location of statistics log files.</td>
</tr>
<tr>
<td>• size</td>
<td>Size of all the log files, in bytes.</td>
</tr>
<tr>
<td>• files</td>
<td>Number of log files.</td>
</tr>
<tr>
<td>Traffic Statistics Interval</td>
<td>Time between sample periods for labeled-unicast traffic statistics, in seconds.</td>
</tr>
<tr>
<td>Preference</td>
<td>Preference value configured with the <code>preference</code> statement.</td>
</tr>
<tr>
<td>Outbound Timer</td>
<td>Time for which the route is available in Junos OS routing table before it is exported to BGP. This field is displayed in the output only if the <code>out-delay</code> parameter is configured to a non-zero value.</td>
</tr>
<tr>
<td>Number of flaps</td>
<td>Number of times the BGP session has gone down and then come back up.</td>
</tr>
<tr>
<td>Peer ID</td>
<td>Router identifier of the peer.</td>
</tr>
<tr>
<td>Group index</td>
<td>Index number for the BGP peer group. The index number differentiates between groups when a single BGP group is split because of different configuration options at the group and peer levels.</td>
</tr>
<tr>
<td>Peer index</td>
<td>Index that is unique within the BGP group to which the peer belongs.</td>
</tr>
<tr>
<td>Local ID</td>
<td>Router identifier of the local routing device.</td>
</tr>
<tr>
<td>Local Interface</td>
<td>Name of the interface on the local routing device.</td>
</tr>
<tr>
<td>Active holdtime</td>
<td>Hold time that the local routing device negotiated with the peer.</td>
</tr>
<tr>
<td>Keepalive interval</td>
<td>Keepalive interval, in seconds.</td>
</tr>
<tr>
<td>BFD</td>
<td>Status of BFD failure detection.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Name of directly connected interface over which direct EBGP peering is established.</td>
</tr>
<tr>
<td>NLRI for restart configured on peer</td>
<td>Names of address families configured for restart.</td>
</tr>
<tr>
<td>NLRI advertised by peer</td>
<td>Address families supported by the peer: unicast or multicast.</td>
</tr>
<tr>
<td>NLRI for this session</td>
<td>Address families being used for this session.</td>
</tr>
<tr>
<td>Peer supports Refresh capability</td>
<td>Remote peer’s ability to send and request full route table readvertisement (route refresh capability). For more information, see RFC 2918, Route Refresh Capability for BGP-4.</td>
</tr>
<tr>
<td>Restart time configured on peer</td>
<td>Configured time allowed for restart on the neighbor.</td>
</tr>
</tbody>
</table>
### Table 333: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stale routes from peer are kept for</td>
<td>When graceful restart is negotiated, the maximum time allowed to hold routes from neighbors after the BGP session has gone down.</td>
</tr>
<tr>
<td>Peer does not support Restarter functionality</td>
<td>Graceful restart restarter-mode is disabled on the peer.</td>
</tr>
<tr>
<td>Peer does not support Receiver functionality</td>
<td>Graceful restart helper-mode is disabled on the peer.</td>
</tr>
<tr>
<td>Restart time requested by this peer</td>
<td>Restart time requested by this neighbor during capability negotiation.</td>
</tr>
<tr>
<td>Restart flag received from the peer</td>
<td>When this field appears, the BGP speaker has restarted (Restarting), and this peer should not wait for the end-of-rib marker from the speaker before advertising routing information to the speaker.</td>
</tr>
<tr>
<td>NLRI that peer supports restart for</td>
<td>Neighbor supports graceful restart for this address family.</td>
</tr>
<tr>
<td>NLRI peer can save forwarding state</td>
<td>Neighbor supporting this address family saves all forwarding states.</td>
</tr>
<tr>
<td>NLRI that peer saved forwarding for</td>
<td>Neighbor saves all forwarding states for this address family.</td>
</tr>
<tr>
<td>NLRI that restart is negotiated for</td>
<td>Router supports graceful restart for this address family.</td>
</tr>
<tr>
<td>NLRI of received end-of-rib markers</td>
<td>Address families for which end-of-routing-table markers are received from the neighbor.</td>
</tr>
<tr>
<td>NLRI of all end-of-rib markers sent</td>
<td>Address families for which end-of-routing-table markers are sent to the neighbor.</td>
</tr>
<tr>
<td>Peer supports 4 byte AS extension (peer-as 1)</td>
<td>Peer understands 4-byte AS numbers in BGP messages. The peer is running Junos OS Release 9.1 or later.</td>
</tr>
<tr>
<td>NLRI(s) for which peer can receive multiple paths</td>
<td>Appears in the command output of the local router if the downstream peer is configured to receive multiple BGP routes to a single destination, instead of only receiving the active route. Possible value is <code>inet-unicast</code>.</td>
</tr>
<tr>
<td>NLRI(s) for which peer can send multiple paths: inet-unicast</td>
<td>Appears in the command output of the local router if the upstream peer is configured to send multiple BGP routes to a single destination, instead of only sending the active route. Possible value is <code>inet-unicast</code>.</td>
</tr>
</tbody>
</table>
Table 333: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table inet.number</strong></td>
<td>Information about the routing table:</td>
</tr>
<tr>
<td>• RIB State —BGP is in the graceful restart process for this routing table: restart is complete or restart in progress.</td>
<td></td>
</tr>
<tr>
<td>• Bit —Number that represents the entry in the routing table for this peer.</td>
<td></td>
</tr>
<tr>
<td>• Send state —State of the BGP group: in sync, not in sync, or not advertising.</td>
<td></td>
</tr>
<tr>
<td>• Active prefixes —Number of prefixes received from the peer that are active in the routing table.</td>
<td></td>
</tr>
<tr>
<td>• Received prefixes —Total number of prefixes from the peer, both active and inactive, that are in the routing table.</td>
<td></td>
</tr>
<tr>
<td>• Accepted prefixes —Total number of prefixes from the peer that have been accepted by a routing policy.</td>
<td></td>
</tr>
<tr>
<td>• Suppressed due to damping —Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
<td></td>
</tr>
<tr>
<td><strong>Last traffic (seconds)</strong></td>
<td>Last time any traffic was received from the peer or sent to the peer, and the last time the local routing device checked.</td>
</tr>
<tr>
<td><strong>Input messages</strong></td>
<td>Messages that BGP has received from the receive socket buffer, showing the total number of messages, number of update messages, number of times a policy is changed and refreshed, and the buffer size in octets. The buffer size is 16 KB.</td>
</tr>
<tr>
<td><strong>Output messages</strong></td>
<td>Messages that BGP has written to the transmit socket buffer, showing the total number of messages, number of update messages, number of times a policy is changed and refreshed, and the buffer size in octets. The buffer size is 16 KB.</td>
</tr>
<tr>
<td><strong>Input dropped path attributes</strong></td>
<td>Information about dropped path attributes:</td>
</tr>
<tr>
<td>• Code —Path attribute code.</td>
<td></td>
</tr>
<tr>
<td>• Count —Path attribute count.</td>
<td></td>
</tr>
<tr>
<td><strong>Input ignored path attributes</strong></td>
<td>Information about ignored path attributes:</td>
</tr>
<tr>
<td>• Code —Path attribute code.</td>
<td></td>
</tr>
<tr>
<td>• Count —Path attribute count.</td>
<td></td>
</tr>
<tr>
<td><strong>Output queue</strong></td>
<td>Number of BGP packets that are queued to be transmitted to a particular neighbor for a particular routing table. Output queue 0 is for unicast NLRIs, and queue 1 is for multicast NLRIs.</td>
</tr>
<tr>
<td><strong>Trace options</strong></td>
<td>Configured tracing of BGP protocol packets and operations.</td>
</tr>
<tr>
<td><strong>Trace file</strong></td>
<td>Name of the file to receive the output of the tracing operation.</td>
</tr>
<tr>
<td><strong>Filter Updates recv</strong></td>
<td>(orf option only) Number of outbound-route filters received for each configured address family.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The counter is cumulative. For example, the counter is increased after the remote peer either resends or clears the outbound route filtering prefix list.</td>
<td></td>
</tr>
</tbody>
</table>
Table 333: show bgp neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate</td>
<td>(orf option only) Number of route updates received with the immediate flag set. The immediate flag indicates that the BGP peer should readvertise the updated routes.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong>: The counter is cumulative. For example, the counter is increased after the remote peer either resends or clears the outbound route filtering prefix list.</td>
</tr>
<tr>
<td>Filter</td>
<td>(orf option only) Type of prefix filter received: prefix-based or extended-community.</td>
</tr>
<tr>
<td>Received filter entries</td>
<td>(orf option only) List of received filters displayed.</td>
</tr>
<tr>
<td>seq</td>
<td>(orf option only) Numerical order assigned to this prefix entry among all the received outbound route filter prefix entries.</td>
</tr>
<tr>
<td>prefix</td>
<td>(orf option only) Address for the prefix entry that matches the filter.</td>
</tr>
<tr>
<td>minlength</td>
<td>(orf option only) Minimum prefix length, in bits, required to match this prefix.</td>
</tr>
<tr>
<td>maxlength</td>
<td>(orf option only) Maximum prefix length, in bits, required to match this prefix.</td>
</tr>
<tr>
<td>match</td>
<td>(orf option only) For this prefix match, whether to permit or deny route updates.</td>
</tr>
</tbody>
</table>

Sample Output

show bgp neighbor

```
user@host > show bgp neighbor
Peer: 10.255.7.250+179 AS 10   Local: 10.255.7.248+63740 AS 10
    Type: Internal    State: Established    Flags: <Sync>
    Last State: OpenConfirm   Last Event: RecvKeepAlive
    Last Error: None
    Export: [ redist_static ]
    Options: <Preference LocalAddress PeerAS Refresh>
    Local Address: 10.255.7.248 Holdtime: 90 Preference: 170 Outbound Timer: 50
    Number of flaps: 0
    Peer ID: 10.255.7.250   Local ID: 10.255.7.248   Active Holdtime: 90
    Keepalive Interval: 30   Group index: 0   Peer index: 0
    BFD: disabled, down
    NLRI for restart configured on peer: inet-unicast
    NLRI advertised by peer: inet-unicast
    NLRI for this session: inet-unicast
    Peer supports Refresh capability (2)
    Stale routes from peer are kept for: 300
    Peer does not support Restarter functionality
    NLRI that restart is negotiated for: inet-unicast
    NLRI of received end-of-rib markers: inet-unicast
    NLRI of all end-of-rib markers sent: inet-unicast
    Peer supports 4 byte AS extension (peer-as 10)
    Peer does not support Addpath
Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes: 1
    Received prefixes: 1
```
Accepted prefixes: 1
Suppressed due to damping: 0
Advertised prefixes: 1
Last traffic (seconds): Received 9  Sent 5  Checked 5
Input messages: Total 36 Updates 2  Refreshes 0  Octets 718
Output messages: Total 37 Updates 1  Refreshes 0  Octets 796
Output Queue[0]: 0

Peer: 10.255.162.214+52193 AS 100 Local: 10.255.167.205+179 AS 100
Type: Internal  State: Established (route reflector client)Flags: <Sync>
Last State: OpenConfirm  Last Event: RecvKeepAlive
Last Error: None
Options: <Preference LocalAddress Cluster AddressFamily Rib-group Refresh>
Address families configured: inet-unicast inet-vpn-unicast route-target
Local Address: 10.255.167.205 Holdtime: 90 Preference: 170
Number of flaps: 0
Peer ID: 10.255.162.214  Local ID: 10.255.167.205  Active Holdtime: 90
Keepalive Interval: 30  Group index: 0  Peer index: 1

show bgp neighbor (CLNS)

user@host> show bgp neighbor
Peer: 10.245.245.1+179 AS 200  Local: 10.245.245.3+3770 AS 100
Type: External  State: Established Flags: <ImportEval Sync>
Last State: OpenConfirm  Last Event: RecvKeepAlive
Last Error: None
Options: <Multihop Preference LocalAddress HoldTime AddressFamily PeerAS Rib-group Refresh>
Address families configured: iso-vpn-unicast
Local Address: 10.245.245.3 Holdtime: 90 Preference: 170
Number of flaps: 0
Peer ID: 10.245.245.1  Local ID: 10.245.245.3  Active Holdtime: 90
Keepalive Interval: 30  Peer index: 0
NLRI advertised by peer: iso-vpn-unicast
NLRI for this session: iso-vpn-unicast
Peer supports Refresh capability (2)
Table bgp.isovpn.0 Bit: 10000
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: in sync
Active prefixes: 3
Received prefixes: 3
Suppressed due to damping: 0
Advertised prefixes: 3
Table aaaa.iso.0
RIB State: BGP restart is complete
RIB State: VPN restart is complete
Send state: not advertising
Active prefixes: 3
Received prefixes: 3
Suppressed due to damping: 0
Last traffic (seconds): Received 6  Sent 5  Checked 5
Input messages: Total 1736  Updates 4  Refreshes 0  Octets 33385
Output messages: Total 1738  Updates 3  Refreshes 0  Octets 33305
Output Queue[0]: 0
Output Queue[1]: 0

show bgp neighbor (Layer 2 VPN)

user@host> show bgp neighbor
Peer: 10.69.103.2  AS 65100 Local: 10.69.103.1  AS 65103
Type: External  State: Active  Flags: <ImportEval>
Last State: Idle     Last Event: Start
Last Error: None    Export: [ BGP-INET-import ]
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS
          Refresh>
Address families configured: inet-unicast
Local Address: 10.69.103.1 Holdtime: 90 Preference: 170
Number of flaps: 0
Peer: 10.69.104.2     AS 65100 Local: 10.69.104.1     AS 65104
Type: External    State: Active    Flags: <ImportEval>
Last State: Idle     Last Event: Start
Last Error: None    Export: [ BGP-L-import ]
Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily PeerAS
          Refresh>
Address families configured: inet-labeled-unicast
Local Address: 10.69.104.1 Holdtime: 90 Preference: 170
Number of flaps: 0
Type: Internal    State: Established    Flags: <ImportEval>
Last State: OpenConfirm   Last Event: RecvKeepAlive
Last Error: None    Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily
                       Rib-group Refresh>
Address families configured: inet-vpn-unicast l2vpn
Number of flaps: 0
Keepalive Interval: 30
NLRI for restart configured on peer: inet-vpn-unicast l2vpn
NLRI advertised by peer: inet-vpn-unicast l2vpn
NLRI for this session: inet-vpn-unicast l2vpn
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
Restart time requested by this peer: 120
NLRI that peer supports restart for: inet-vpn-unicast l2vpn
NLRI peer can save forwarding state: inet-vpn-unicast l2vpn
NLRI that peer saved forwarding for: inet-vpn-unicast l2vpn
NLRI that restart is negotiated for: inet-vpn-unicast l2vpn
NLRI of received end-of-rib markers: inet-vpn-unicast l2vpn
Table bgp.l3vpn.0 Bit: 10000
RIB State: BGP restart in progress
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:    10
Received prefixes: 10
Suppressed due to damping: 0
Table bgp.l2vpn.0 Bit: 20000
RIB State: BGP restart in progress
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:    1
Received prefixes: 1
Suppressed due to damping: 0
Table BGP-INET.inet.0 Bit: 30000
RIB State: BGP restart in progress
RIB State: VPN restart in progress
Send state: in sync
Active prefixes:    2
Received prefixes: 2
show bgp neighbor (Layer 3 VPN)

user@host> show bgp neighbor

Peer: 4.4.4.4+179     AS 10045 Local: 5.5.5.5+1214    AS 10045
Type: Internal    State: Established    Flags: <ImportEval>
show bgp neighbor neighbor-address

user@host> show bgp neighbor 192.168.1.111
Peer: 10.255.245.12+179 AS 35  Local: 10.255.245.13+2884 AS 35
  Type: Internal  State: Established (route reflector client)Flags: <Sync>
  Last State: OpenConfirm  Last Event: RecvKeepAlive
  Last Error: None
  Export: [ match-all ] Import: [ match-all ]
  Options: <Preference LocalAddress HoldTime GracefulRestart AddressFamily Rib-group Refresh>
  Address families configured: inet-vpn-unicast inet-labeled-unicast
  Local Address: 5.5.5.5 Holdtime: 90 Preference: 170
  Flags for NLRI inet-labeled-unicast: TrafficStatistics
Traffic Statistics: Options: all File: /var/log/bstat.log
size 131072 files 10
Traffic Statistics Interval: 60
Number of flaps: 0
Peer ID: 192.168.1.110  Local ID: 192.168.1.111  Active Holdtime: 90
Keepalive Interval: 30
NLRI for restart configured on peer: inet-vpn-unicast
NLRI advertised by peer: inet-vpn-unicast
NLRI for this session: inet-vpn-unicast
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
Restart time requested by this peer: 120
NLRI that peer supports restart for: inet-vpn-unicast
NLRI peer can save forwarding state: inet-vpn-unicast
NLRI that peer saved forwarding for: inet-vpn-unicast
NLRI that restart is negotiated for: inet-vpn-unicast
NLRI of received end-of-rib markers: inet-vpn-unicast
NLRI of all end-of-rib markers sent: inet-vpn-unicast
Table bgp.l3vpn.0 Bit: 10000
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: in sync
  Active prefixes: 2
  Received prefixes: 2
  Suppressed due to damping: 0
Table vpn-green.inet.0 Bit: 20001
  RIB State: BGP restart is complete
  RIB State: VPN restart is complete
  Send state: in sync
  Active prefixes: 2
  Received prefixes: 2
  Suppressed due to damping: 0
Last traffic (seconds): Received 15  Sent 20  Checked 20
Input messages: Total 40  Updates 2  Refreshes 0  Octets 856
Output messages: Total 44  Updates 2  Refreshes 0  Octets 1066
Output Queue[0]: 0
Output Queue[1]: 0
Trace options: detail packets
Trace file: /var/log/bgpr.log size 131072 files 10
Flags for NLRI inet-labeled-unicast: AggregateLabel
   Number of flaps: 0
   Peer ID: 10.255.245.12   Local ID: 10.255.245.13   Active Holdtime: 90
   Keepalive Interval: 30
   BFD: disabled
NLRI advertised by peer: inet-unicast inet-labeled-unicast
NLRI for this session: inet-unicast inet-labeled-unicast
Peer supports Refresh capability (2)
Restart time configured on the peer: 300
Stale routes from peer are kept for: 60
Restart time requested by this peer: 300
NLRI that peer supports restart for: inet-unicast inet6-unicast
NLRI that restart is negotiated for: inet-unicast inet6-unicast
NLRI of received end-of-rib markers: inet-unicast inet6-unicast
NLRI of all end-of-rib markers sent: inet-unicast inet6-unicast
Table inet.0 Bit: 10000
   RIB State: restart is complete
   Send state: in sync
   Active prefixes: 4
   Received prefixes: 6
   Suppressed due to damping: 0
Table inet6.0 Bit: 20000
   RIB State: restart is complete
   Send state: in sync
   Active prefixes: 0
   Received prefixes: 2
   Suppressed due to damping: 0
Last traffic (seconds): Received 3    Sent 3    Checked 3
Input messages: Total 9      Updates 6       Refreshes 0     Octets 403
Output messages: Total 7      Updates 3       Refreshes 0     Octets 365
Output Queue[0]: 0
Output Queue[1]: 0
Trace options: detail packets
Trace file: /var/log/bgpgr size 131072 files 10

show bgp neighbor neighbor-address

user@host> show bgp neighbor 192.168.4.222
Peer: 192.168.4.222+4902 AS 65501 Local: 192.168.4.221+179 AS 65500
   Type: External    State: Established    Flags: <Sync>
   Last State: OpenConfirm   Last Event: RecvKeepAlive
   Last Error: Cease
   Export: [ export-policy ] Import: [ import-policy ]
   Options: <Preference HoldTime AddressFamily PeerAS PrefixLimit Refresh>
Address families configured: inet-unicast inet-multicast
   Holdtime: 60000 Preference: 170
   Number of flaps: 4
   Last flap event: RecvUpdate
   Error: 'Cease' Sent: 5 Recv: 0
   Peer ID: 10.255.245.6   Local ID: 10.255.245.5   Active Holdtime: 60000
   Keepalive Interval: 20000   Peer index: 0
   BFD: disabled, down
Local Interface: fxp0.0
NLRI advertised by peer: inet-unicast inet-multicast
NLRI for this session: inet-unicast inet-multicast
Peer supports Refresh capability (2)
Table inet.0 Bit: 10000
   RIB State: BGP restart is complete
   Send state: in sync
   Active prefixes: 8
   Received prefixes: 10
show bgp neighbor orf neighbor-address detail

user@host > show bgp neighbor orf 192.168.165.56 detail
Peer: 192.168.165.56+179 Type: External
  Group: ext1

inet-unicast
  Filter updates recv: 1 Immediate: 1
  Filter: prefix-based receive
     Received filter entries:
       seq 1: prefix 2.2.2.2/32: minlen 32: maxlen 32: match deny:

inet6-unicast
  Filter updates recv: 0 Immediate: 1
  Filter: prefix-based receive
     Received filter entries:
       *:*
show bgp summary

Syntax

show bgp summary
<exact-instance instance-name>
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and QFX Series)

show bgp summary
<exact-instance instance-name>
<instance instance-name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
exact-instance option introduced in Junos OS Release 11.4.

Description

Display BGP summary information.

Options

none—Display BGP summary information for all routing instances.

exact-instance instance-name—(Optional) Display information for the specified instance only.

instance instance-name—(Optional) Display information for all routing instances whose name begins with this string (for example, cust1, cust11, and cust111 are all displayed when you run the show bgp summary instance cust1 command). The instance name can be master for the main instance, or any valid configured instance name or its prefix.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

List of Sample Output

show bgp summary (When a Peer Is Not Established) on page 2683
show bgp summary (When a Peer Is Established) on page 2683
show bgp summary (CLNS) on page 2683
show bgp summary (Layer 2 VPN) on page 2683
show bgp summary (Layer 3 VPN) on page 2684

Output Fields

Table 334 on page 2680 describes the output fields for the show bgp summary command. Output fields are listed in the approximate order in which they appear.

Table 334: show bgp summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Number of BGP groups.</td>
</tr>
<tr>
<td>Peers</td>
<td>Number of BGP peers.</td>
</tr>
</tbody>
</table>
Table 334: show bgp summary Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down peers</td>
<td>Number of down BGP peers.</td>
</tr>
<tr>
<td>Table</td>
<td>Name of routing table.</td>
</tr>
<tr>
<td>Tot Paths</td>
<td>Total number of paths.</td>
</tr>
<tr>
<td>Act Paths</td>
<td>Number of active routes.</td>
</tr>
<tr>
<td>Suppressed</td>
<td>Number of routes currently inactive because of damping or other reasons. These routes do not appear in the forwarding table and are not exported by routing protocols.</td>
</tr>
<tr>
<td>History</td>
<td>Number of withdrawn routes stored locally to keep track of damping history.</td>
</tr>
<tr>
<td>Damp State</td>
<td>Number of routes with a figure of merit greater than zero, but still active because the value has not reached the threshold at which suppression occurs.</td>
</tr>
<tr>
<td>Pending</td>
<td>Routes in process by BGP import policy.</td>
</tr>
<tr>
<td>Peer</td>
<td>Address of each BGP peer. Each peer has one line of output.</td>
</tr>
<tr>
<td>AS</td>
<td>Peer's AS number.</td>
</tr>
<tr>
<td>InPkt</td>
<td>Number of packets received from the peer.</td>
</tr>
<tr>
<td>OutPkt</td>
<td>Number of packets sent to the peer.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Number of BGP packets that are queued to be transmitted to a particular neighbor. It normally is 0 because the queue usually is emptied quickly.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Number of times the BGP session has gone down and then come back up.</td>
</tr>
<tr>
<td>Last Up/Down</td>
<td>Last time since the neighbor transitioned to or from the established state.</td>
</tr>
</tbody>
</table>
Table 334: show bgp summary Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| State/#Active/Received/Accepted/Damped | Multipurpose field that displays information about BGP peer sessions. The field’s contents depend upon whether a session is established and whether it was established on the main routing device or in a routing instance.  
  - If a peer is not established, the field shows the state of the peer session: **Active**, **Connect**, or **Idle**.  
    In general, the Idle state is the first stage of a connection. BGP is waiting for a Start event. A session can be idle for other reasons as well. The reason that a session is idle is sometimes displayed. For example: **Idle (Removal in progress)** or **Idle (LicenseFailure)**.  
  - If a BGP session is established on the main routing device, the field shows the number of active, received, accepted, and damped routes that are received from a neighbor and appear in the `inet.0` (main) and `inet.2` (multicast) routing tables. For example, **8/10/10/2 and 2/4/4/0** indicate the following:  
    - 8 active routes, 10 received routes, 10 accepted routes, and 2 damped routes from a BGP peer appear in the `inet.0` routing table.  
    - 2 active routes, 4 received routes, 4 accepted routes, and no damped routes from a BGP peer appear in the `inet.2` routing table.  
  - If a BGP session is established in a routing instance, the field indicates the established (**Establ**) state, identifies the specific routing table that receives BGP updates, and shows the number of active, received, and damped routes that are received from a neighbor. For example, **Establ VPN-AB.inet.0:2/4/0** indicates the following:  
    - The BGP session is established.  
    - Routes are received in the `VPN-AB.inet.0` routing table.  
    - The local routing device has two active routes, four received routes, and no damped routes from a BGP peer.  
When a BGP session is established, the peers are exchanging update messages.
Sample Output

show bgp summary (When a Peer Is Not Established)

user@host> show bgp summary
Table | Tot Paths | Act Paths | Suppressed | History | Damp | State | Pending
inet.0 | 6 | 4 | 0 | 0 | 0 | 0 | 0
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
10.0.0.3 | 65002 | 86 | 90 | 0 | 2 | 42:54 | 0/0/0
10.0.0.4 | 65002 | 90 | 91 | 0 | 1 | 42:54 | 0/2/0
10.0.0.6 | 65002 | 87 | 90 | 0 | 3 | 3 Active
10.1.12.1 | 65001 | 89 | 89 | 0 | 1 | 42:54 | 4/4/0

show bgp summary (When a Peer Is Established)

user@host> show bgp summary
Table | Tot Paths | Act Paths | Suppressed | History | Damp | State | Pending
inet.0 | 6 | 4 | 0 | 0 | 0 | 0 | 0
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
10.0.0.2 | 65002 | 88675 | 88652 | 0 | 2 | 42:38 | 2/4/0
10.0.0.3 | 65002 | 54528 | 54532 | 0 | 1 | 2w4d22h | 0/0/0
10.0.0.4 | 65002 | 51597 | 51584 | 0 | 0 | 2w3d22h | 2/2/0

show bgp summary (CLNS)

user@host> show bgp summary
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
10.245.245.1 | 200 | 1735 | 1737 | 0 | 14:26:12 | Establ
gbgp.isovpn.0: 3/3/0
aaaa.iso.0: 3/3/0

show bgp summary (Layer 2 VPN)

user@host> show bgp summary
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
10.255.245.35 | 65299 | 72 | 74 | 0 | 19:00 | Establ
gbgp.l2vpn.0: 1/1/0
frame-vpn.l2vpn.0: 1/1/0
show bgp summary (Layer 3 VPN)

```
user@host> show bgp summary
Groups: 2 Peers: 2 Down peers: 0
Table | Tot Paths | Act Paths | Suppressed | History | Damp | State | Pending
bgp.l3vpn.0 | 2 | 2 | 0 | 0 | 0 | 0 | 0
Peer | AS | InPkt | OutPkt | OutQ | Flaps | Last Up/Dwn
State | #Active/Received/Damped...
10.39.1.5 | 2 | 21 | 22 | 0 | 0 | 6:26 Establ
VPN-AB.inet.0: 1/1/0
10.255.71.15 | 1 | 19 | 21 | 0 | 0 | 6:17 Establ
bgp.l3vpn.0: 2/2/0
VPN-A.inet.0: 1/1/0
VPN-AB.inet.0: 2/2/0
VPN-B.inet.0: 1/1/0
```
**show policy damping**

**Syntax**

```
show policy damping
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and QFX Series)**

```
show policy damping
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display information about BGP route flap damping parameters.

**Options**

- `none`—Display information about BGP route flap damping parameters.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**

In the output from this command, figure-of-merit values correlate with the probability of future instability of a routing device. Routes with higher figure-of-merit values are suppressed for longer periods of time. The figure-of-merit value decays exponentially over time. A figure-of-merit value of zero is assigned to each new route. The value is increased each time the route is withdrawn or readvertised, or when one of its path attributes changes.

**Required Privilege Level**

- `view`

**Related Documentation**

- “Configuring BGP Flap Damping Parameters” in the *Routing Policy Feature Guide for Routing Devices*
- `clear bgp damping` on page 2652
- `show route damping` on page 3170

**List of Sample Output**

- `show policy damping` on page 2686

**Output Fields**

Table 335 on page 2685 describes the output fields for the `show policy damping` command. Output fields are listed in the approximate order in which they appear.

**Table 335: show policy damping Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Halflife</td>
<td>Decay half-life, in minutes. The value represents the period during which the accumulated figure-of-merit value is reduced by half if the route remains stable. If a route has flapped, but then becomes stable, the figure-of-merit value for the route decays exponentially. For example, for a route with a figure-of-merit value of 1500, if no incidents occur, its figure-of-merit value is reduced to 750 after 15 minutes and to 375 after another 15 minutes.</td>
</tr>
</tbody>
</table>
### Table 335: show policy damping Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reuse merit</td>
<td>Figure-of-merit value below which a suppressed route can be used again. A suppressed route becomes reusable when its figure-of-merit value decays to a value below a reuse threshold, and the route once again is considered usable and can be installed in the forwarding table and exported from the routing table.</td>
</tr>
<tr>
<td>Suppress/cutoff merit</td>
<td>Figure-of-merit value above which a route is suppressed for use or inclusion in advertisements. When a route's figure-of-merit value reaches a particular level, called the cutoff or suppression threshold, the route is suppressed. When a route is suppressed, the routing table no longer installs the route into the forwarding table and no longer exports this route to any of the routing protocols.</td>
</tr>
<tr>
<td>Maximum suppress time</td>
<td>Maximum hold-down time, in minutes. The value represents the maximum time that a route can be suppressed no matter how unstable it has been before this period of stability.</td>
</tr>
<tr>
<td>Computed values</td>
<td>• <strong>Merit ceiling</strong>—Maximum merit that a flapping route can collect.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Maximum decay</strong>—Maximum decay half-life, in minutes.</td>
</tr>
</tbody>
</table>

### Sample Output

show policy damping

```bash
user@host> show policy damping
Default damping information:
  Halflife: 15 minutes
  Reuse merit: 750 Suppress/cutoff merit: 3000
  Maximum suppress time: 60 minutes
  Computed values:
    Merit ceiling: 12110
    Maximum decay: 6193
Damping information for "standard-damping":
  Halflife: 10 minutes
  Reuse merit: 4000 Suppress/cutoff merit: 8000
  Maximum suppress time: 30 minutes
  Computed values:
    Merit ceiling: 32120
    Maximum decay: 12453
```
PART 17

IS-IS

- Overview on page 2689
- Configuration on page 2693
- Administration on page 2751
CHAPTER 51

Overview

- Layer 3 Protocols on page 2689

Layer 3 Protocols

- Layer 3 Protocols Supported on EX Series Switches on page 2689
- Layer 3 Protocols Not Supported on EX Series Switches on page 2690

Layer 3 Protocols Supported on EX Series Switches

EX Series switches support the Junos OS Layer 3 features and configuration statements listed in Table 326 on page 2553:

Table 336: Supported Junos OS Layer 3 Protocol Statements and Features

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>BFD</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>ICMP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>IGMPv1, v2, and v3</td>
<td>Fully supported.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>MLD</td>
<td>Fully supported (MLD versions 1 and 2).</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>MPLS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS MPLS Applications Configuration Guide</td>
</tr>
<tr>
<td>OSPFv1, v2 and v3</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
</tbody>
</table>
### Table 336: Supported Junos OS Layer 3 Protocol Statements and Features (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td>Fully supported on EX3200, EX3300, EX4200, EX6200, and EX8200 switches.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>PPM</td>
<td>Supported. See “EX Series Switch Software Features Overview” on page 27 for specific platform information.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIPv2</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>SNMP</td>
<td>Fully supported.</td>
<td>Junos OS Network Management Configuration Guide</td>
</tr>
<tr>
<td>VRRP</td>
<td>Fully supported.</td>
<td>See “Understanding VRRP on EX Series Switches” on page 2220. See also Junos OS High Availability Guide.</td>
</tr>
</tbody>
</table>

#### Related Documentation
- Layer 3 Protocols Not Supported on EX Series Switches on page 2554
- EX Series Switch Software Features Overview on page 27

### Layer 3 Protocols Not Supported on EX Series Switches

EX Series switches do not support the Junos OS Layer 3 protocols and features listed in Table 327 on page 2554:

#### Table 337: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVMRP</td>
<td>• dvmrp and subordinate statements</td>
</tr>
<tr>
<td>Flow aggregation (cflowd)</td>
<td>• cflow and subordinate statements</td>
</tr>
<tr>
<td>IPSec</td>
<td>• [edit services] statements related to IPSec</td>
</tr>
<tr>
<td>IS-IS:</td>
<td>• cns-routing statement</td>
</tr>
<tr>
<td></td>
<td>• ipv6-multicast statement</td>
</tr>
<tr>
<td></td>
<td>• lsp-interval statement</td>
</tr>
<tr>
<td></td>
<td>• label-switched-path statement</td>
</tr>
<tr>
<td></td>
<td>• lsp-lifetime statement</td>
</tr>
<tr>
<td></td>
<td>• te-metric statement</td>
</tr>
<tr>
<td>Logical routers</td>
<td>• logical-routers and subordinate statements</td>
</tr>
</tbody>
</table>
Table 337: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS:</td>
<td>• ldp and all subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td>• Fast Reroute (FRR)</td>
<td></td>
</tr>
<tr>
<td>• Label Distribution Protocol (LDP) (except on EX8200 switches)</td>
<td></td>
</tr>
<tr>
<td>• Layer 3 VPNs (except on EX8200 switches)</td>
<td></td>
</tr>
<tr>
<td>• Multiprotocol BGP (MP-BGP) for VPN-IPv4 family</td>
<td></td>
</tr>
<tr>
<td>• Pseudowire emulation (PWE3)</td>
<td></td>
</tr>
<tr>
<td>• Routing policy statements related to Layer 3 VPNs and MPLS (except on EX8200 switches)</td>
<td></td>
</tr>
<tr>
<td>• Virtual Private LAN Service (VPLS)</td>
<td></td>
</tr>
<tr>
<td>Network Address Translation (NAT)</td>
<td>• nat and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• Policy statements related to NAT</td>
</tr>
<tr>
<td>OSPF</td>
<td>• demand-circuit statement</td>
</tr>
<tr>
<td></td>
<td>• label-switched-path and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• neighbor statement within an OSPF area</td>
</tr>
<tr>
<td></td>
<td>• peer-interface and subordinate statements within an OSPF area</td>
</tr>
<tr>
<td></td>
<td>• sham-link statement</td>
</tr>
<tr>
<td></td>
<td>• te-metric statement</td>
</tr>
<tr>
<td>PIM SM</td>
<td>• Not supported on EX2200 switches</td>
</tr>
<tr>
<td>PIM SSM</td>
<td>• Not supported on EX2200 switches</td>
</tr>
<tr>
<td>PIM DM</td>
<td>• Not supported on EX2200 or EX4500 switches</td>
</tr>
<tr>
<td>PIM:</td>
<td>• inet6 family (EX2200 and EX4500 switches)</td>
</tr>
<tr>
<td>• IPv6</td>
<td></td>
</tr>
<tr>
<td>PPM</td>
<td>• Not supported on EX2200 and EX3300 switches</td>
</tr>
<tr>
<td>Routing instances:</td>
<td>• l2vpn and subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td>• Routing instance forwarding</td>
<td>• ldp and subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• vpls and subordinate statements</td>
</tr>
<tr>
<td>Routed VLAN interfaces (RVIs)</td>
<td>• family mpls statement</td>
</tr>
</tbody>
</table>
Table 337: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP and SDP</td>
<td>• sap and all subordinate statements</td>
</tr>
<tr>
<td>General routing options in the routing-options hierarchy:</td>
<td>• auto-export and subordinate statements</td>
</tr>
<tr>
<td>• MPLS and label-switched-paths</td>
<td>• dynamic-tunnels and subordinate statements</td>
</tr>
<tr>
<td>• lsp-next-hop and subordinate statements</td>
<td>• multicast and subordinate statements</td>
</tr>
<tr>
<td>• p2mp-lsp-next-hop and subordinate statements</td>
<td>• route-distinguisher-id statement (except on EX8200 switches)</td>
</tr>
<tr>
<td>Traffic sampling and forwarding in the forwarding-options hierarchy</td>
<td>• accounting and subordinate statements</td>
</tr>
<tr>
<td>• family mpls and family multiservice under hash-key hierarchy</td>
<td>• family inet output hierarchy:</td>
</tr>
<tr>
<td>• cflowd statement</td>
<td>• export-format-cflowd-version-5 statement</td>
</tr>
<tr>
<td>• flow-active-timeout statement</td>
<td>• flow-export-destination statement</td>
</tr>
<tr>
<td>• flow-inactive-timeout statement</td>
<td>• interface statement</td>
</tr>
<tr>
<td>• port-mirroring statement (On EX Series switches, port mirroring is implemented using the analyzer statement.)</td>
<td>• sampling and subordinate statements</td>
</tr>
</tbody>
</table>

Related Documentation

- Layer 3 Protocols Supported on EX Series Switches on page 2553
- EX Series Switch Software Features Overview on page 27
CHAPTER 52

Configuration

- Configuration Statements on page 2694
Configuration Statements

authentication-key (Protocols IS-IS)

Syntax:  
```
authentication-key key;
```

Hierarchy Level:  
```
[edit logical-systems logical-system-name protocols isis level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
[edit protocols isis level level-number],
[edit routing-instances routing-instance-name protocols isis level level-number]
```

Release Information:  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description:  
Authentication key (password). Neighboring routing devices use the password to verify  
the authenticity of packets sent from this interface. For the key to work, you also must  
include the `authentication-type` statement.

All routing devices must use the same password. If you are using the Junos OS IS-IS  
software with another implementation of IS-IS, the other implementation must be  
configured to use the same password for the domain, the area, and all interfaces adjacent  
to the Juniper Networks routing device.

Default:  
If you do not include this statement and the `authentication-type` statement, IS-IS  
authentication is disabled.

Options:  
```
key—Authentication password. The password can be up to 1024 characters long.  
Characters can include any ASCII strings. If you include spaces, enclose all characters  
in quotation marks (" ").
```

**CAUTION:** A simple password for authentication is truncated if it exceeds  
254 characters.

Required Privilege:  
```
routing—to view this statement in the configuration.  
routing-control—to add this statement to the configuration.
```

Related Documentation:  
```
• Example: Configuring Hitless Authentication Key Rollover for IS-IS
```
**authentication-type (Protocols IS-IS)**

**Syntax**

```
authentication-type authentication;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
[edit protocols isis level level-number],
[edit routing-instances routing-instance-name protocols isis level level-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Enable authentication and specify the authentication scheme for IS-IS. If you enable authentication, you must specify a password by including the `authentication-key` statement.

**Default**

If you do not include this statement and the `authentication-key` statement, IS-IS authentication is disabled.

**Options**

`authentication`—Authentication scheme:

- `md5`—Use HMAC authentication in combination with MD5. HMAC-MD5 authentication is defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

- `simple`—Use a simple password for authentication. The password is included in the transmitted packet, making this method of authentication relatively insecure. We recommend that you *not* use this authentication method.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*
- `authentication-key` on page 2694
- `no-authentication-check` on page 2727
bfd-liveness-detection (Protocols IS-IS)

**Syntax**

```
bfd-liveness-detection {
  authentication {
    algorithm algorithm-name;
    key-chain key-chain-name;
    loose-check;
  }
  detection-time {
    threshold milliseconds;
  }
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  version (1 | automatic);
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
detection-time threshold and transmit-interval threshold options added in Junos OS Release 8.2.
Support for logical systems introduced in Junos OS Release 8.3.
no-adaptation statement introduced in Junos OS Release 9.0.
authentication algorithm, authentication key-chain, and authentication loose-check options introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure bidirectional failure detection timers and authentication.

**Options**

- **authentication algorithm algorithm-name**—Configure the algorithm used to authenticate the specified BFD session: simple-password, keyed-md5, keyed-sha-1, meticulous-keyed-md5, meticulous-keyed-sha-1.

- **authentication key-chain key-chain-name**—Associate a security key with the specified BFD session using the name of the security keychain. The name you specify must match one of the keychains configured in the authentication-key-chains key-chain statement at the [edit security] hierarchy level.

- **authentication loose-check**—(Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication might not be configured at both ends of the BFD session.
**detection-time threshold milliseconds**—Configure a threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

**minimum-interval milliseconds**—Configure the minimum interval after which the local routing device transmits a hello packet and then expects to receive a reply from the neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the `transmit-interval minimum-interval` and `minimum-receive-interval` statements.

**Range:** 1 through 255,000

**minimum-receive-interval milliseconds**—Configure the minimum interval after which the local routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum receive interval using the `minimum-interval` statement.

**Range:** 1 through 255,000

**multiplier number**—Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.

**Range:** 1 through 255

**Default:** 3

**no-adaptation**—Specify that BFD sessions not adapt to changing network conditions. We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

**transmit-interval threshold milliseconds**—Configure the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent. The interval threshold must be greater than the minimum transmit interval.

**Range:** 0 through 4,294,967,295 \( (2^{32} - 1) \)

**transmit-interval minimum-interval milliseconds**—Configure a minimum interval after which the local routing device transmits hello packets to a neighbor. Optionally, instead of using this statement, you can configure the minimum transmit interval using the `minimum-interval` statement.

**Range:** 1 through 255,000

**version**—Configure the BFD version to detect: 1 (BFD version 1) or automatic (autodetect the BFD version)

**Default:** automatic
**checksum (Protocols IS-IS)**

**Syntax**
```
checksum;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Enable checksums for packets on this interface.

Junos OS supports IS-IS checksums as documented in RFC 3358, *Optional Checksums in Intermediate System to Intermediate System (ISIS)*.

The checksum cannot be enabled with MD5 hello authentication on the same interface.

**Required Privilege**
```
route—To view this statement in the configuration.
route-control—To add this statement to the configuration.
```

**Related Documentation**
- Example: *Enabling Packet Checksums on IS-IS Interfaces*
csnp-interval

Syntax

csnp-interval (seconds | disable);

Hierarchy Level

[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]

Release Information

Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Configure the interval between complete sequence number PDUs (CSNPs) on a LAN interface.

If the routing device is the designated router on a LAN, IS-IS sends CSN packets every 10 seconds. If the routing device is on a point-to-point interface, it sends CSN packets every 5 seconds. To protect against link-state PDU flooding, we recommend modifying the default interval.

To modify the CSNP interval, include the csnp-interval statement.

To configure the interface not to send any CSNPs, specify the disable option.

Default

By default, IS-IS sends CSNPs periodically. If the routing device is the designated router on a LAN, IS-IS sends CSNPs every 10 seconds. If the routing device is on a point-to-point interface, it sends CSNPs every 5 seconds.

Options

disable—Do not send CSNPs on this interface.

seconds—Number of seconds between the sending of CSNPs.

Range: 1 through 65,535 seconds
Default: 10 seconds on LAN broadcast links. 5 seconds on point-to-point links.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring the Transmission Frequency for CSNP Packets on IS-IS Interfaces
disable (Protocols IS-IS)

Syntax disable;

Hierarchy Level

- [edit logical-systems logical-system-name protocols isis],
- [edit logical-systems logical-system-name protocols isis interface interface-name],
- [edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
- [edit logical-systems logical-system-name protocols isis traffic-engineering],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis traffic-engineering],
- [edit protocols isis],
- [edit protocols isis interface interface-name],
- [edit protocols isis interface interface-name level level-number],
- [edit protocols isis traffic-engineering],
- [edit routing-instances routing-instance-name protocols isis],
- [edit routing-instances routing-instance-name protocols isis interface interface-name],
- [edit routing-instances routing-instance-name protocols isis interface interface-name level level-number],
- [edit routing-instances routing-instance-name protocols isis traffic-engineering]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Disable IS-IS on the routing device, on an interface, or on a level.

At the [edit protocols isis traffic-engineering] hierarchy level, disable IS-IS support for traffic engineering.

Enabling IS-IS on an interface (by including the interface statement at the [edit protocols isis] or the [edit routing-instances routing-instance-name protocols isis] hierarchy level), disabling it (by including the disable statement), and not actually having IS-IS run on an interface (by including the passive statement) are mutually exclusive states.

Default

IS-IS is enabled for Level 1 and Level 2 routers on all interfaces on which family iso is enabled.

IS-IS support for traffic engineering is enabled.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Multi-Level IS-IS
- IS-IS Overview
### export (Protocols IS-IS)

**Syntax**

```
export [ policy-names ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols isis],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
- [edit protocols isis],
- [edit routing-instances routing-instance-name protocols isis]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Apply one or more policies to routes being exported from the routing table into IS-IS.

All routing protocols store the routes that they learn in the routing table. The routing table uses this collected route information to determine the active routes to destinations. The routing table then installs the active routes into its forwarding table and exports them into the routing protocols. It is these exported routes that the protocols advertise.

For each protocol, you control which routes the protocol stores in the routing table and which routes the routing table exports into the protocol from the routing table by defining a *routing policy* for that protocol.

**NOTE:** For IS-IS, you cannot apply routing policies that affect how routes are imported into the routing table; doing so with a link-state protocol can easily lead to an inconsistent topology database.

**Options**

- **policy-names**—Name of one or more policies.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Redistributing OSPF Routes into IS-IS*
- *Example: Configuring an IS-IS Default Route Policy on Logical Systems*
external-preference (Protocols IS-IS)

Syntax

```
external-preference preference;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols isis level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
[edit protocols isis level level-number],
[edit routing-instances routing-instance-name protocols isis level level-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Configure the preference of external routes.

Options

```
preference—Preference value.
```

Range: 0 through 4,294,967,295 (2^{32} – 1)

Default: 15 (for Level 1 internal routes), 18 (for Level 2 internal routes), 160 (for Level 1 external routes), 165 (for Level 2 external routes)

Required Privilege

Level routing—To view this statement in the configuration.

Level routing-control—To add this statement to the configuration.

Related Documentation

- Route Preferences Overview
- Example: Redistributing OSPF Routes into IS-IS
- Example: Redistributing BGP Routes with a Specific Community Tag into IS-IS
- preference on page 2740
graceful-restart (Protocols IS-IS)

Syntax  graceful-restart {
  disable;
  helper-disable;
  restart-duration seconds;
}

Hierarchy Level  [edit logical-systems logical-system-name protocols isis],
                 [edit protocols isis]

Release Information  Statement introduced before Junos OS Release 7.4.
                      Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure graceful restart parameters for IS-IS.

Graceful restart allows a routing device to restart with minimal effects to the network,
and is enabled for all routing protocols at the [edit routing-options] hierarchy level. When
graceful restart is enabled, the restarting routing device is not removed from the network
topology during the restart period. The adjacencies are reestablished after restart is
complete.

On LAN interfaces where IS-IS is configured on a transit router that serves as the
designated router (DR), a graceful restart causes:

- The ingress router of the label-switched path (LSP), which passes through the DR, to
  break the LSP.
- The ingress router to re-signal the LSP.

Options  disable—Disable graceful restart for IS-IS.

  helper-disable—Disable graceful restart helper capability. Helper mode is enabled by
default.

  restart-duration seconds—Time period for the restart to last, in seconds.
  Range: 30 through 300 seconds
  Default: 30 seconds

Required Privilege Level  routing—To view this statement in the configuration.
                          routing-control—To add this statement to the configuration.

Related Documentation  • Configuring Routing Protocols Graceful Restart
**hello-authentication-key**

**Syntax**
```
hello-authentication-key password;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols isis interface interface-name level number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level number],
[edit protocols isis interface interface-name level number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level number]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Configure an authentication key (password) for hello packets. Neighboring routing devices use the password to verify the authenticity of packets sent from an interface. For the key to work, you also must include the `hello-authentication-type` statement.

**Default**
By default, hello authentication is not configured on an interface. However, if IS-IS authentication is configured, the hello packets are authenticated using the IS-IS authentication type and password.

**Options**
- `password`—Authentication password. The password can be up to 255 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (" ").

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- authentication-key on page 2694
- authentication-type on page 2695
- hello-authentication-type on page 2705
**Syntax**
```
hello-authentication-type (md5 | simple);
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols isis interface interface-name level number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level number],
[edit protocols isis interface interface-name level number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level number]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Enable authentication on an interface for hello packets. If you enable authentication on hello packets, you must specify a password by including the `hello-authentication-key` statement.

You can configure authentication for a given IS-IS level on an interface. On a point-to-point link, if you enable hello authentication for both IS-IS levels, the password configured for Level 1 is used for both levels.

**CAUTION:** If no authentication is configured for Level 1 on a point-to-point link with both levels enabled, the hello packets are sent without any password, regardless of the Level 2 authentication configurations.

**Default**
By default, hello authentication is not configured on an interface. However, if IS-IS authentication is configured, the hello packets are authenticated using the IS-IS authentication type and password.

**Options**
- `md5`—Specifies Message Digest 5 as the packet verification type.
- `simple`—Specifies simple authentication as the packet verification type.

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- `authentication-key` on page 2694
- `authentication-type` on page 2695
- `hello-authentication-key` on page 2704
**hello-interval (Protocols IS-IS)**

**Syntax**

```
hello-interval seconds;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
[edit protocols isis interface interface-name level level-number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Modify the frequency with which the routing device sends hello packets out of an interface, in seconds.

Routing devices send hello packets at a fixed interval on all interfaces to establish and maintain neighbor relationships. This interval is advertised in the hello interval field in the hello packet.

You can send out hello packets in subsecond intervals. To send out hello packets every 333 milliseconds, set the `hello-interval` value to 1.

**Options**

- `seconds`—Frequency of transmission for hello packets.
  - **Range:** 1 through 20,000 seconds
  - **Default:** 3 seconds (for designated intermediate system [DIS] routers), 9 seconds (for non-DIS routers)

**Required Privilege**

- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

**Related Documentation**

- `hold-time`
**hello-padding**

**Syntax**

```
hello-padding (adaptive | disable | loose | strict);
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure padding on hello packets to accommodate asymmetrical maximum transfer units (MTUs) from different hosts.

This helps to prevent a premature adjacency Up state when one routing device's MTU does not meet the requirements to establish the adjacency.

As an OSI Layer 2 protocol, IS-IS does not support data fragmentation. Therefore, maximum packet sizes must be established and supported between two routers. During adjacency establishment, the IS-IS protocol makes sure that the link supports a packet size of 1492 bytes by padding outgoing hello packets up to the maximum packet size of 1492 bytes.

This is the default behavior of the Junos OS IS-IS implementation. However, Junos OS provides an option to disable hello padding that can override this behavior.

There are four types of hello padding:

- **Adaptive padding**—On point-to-point connections, the hello packets are padded from the initial detection of a new neighbor until the neighbor verifies the adjacency as Up in the adjacency state type, length, and value (TLV) tuple. If the neighbor does not support the adjacency state TLV, then padding continues. On LAN connections, padding starts from the initial detection of a new neighbor until there is at least one active adjacency on the interface. Adaptive padding has more overhead than loose padding and is able to detect MTU asymmetry from one side of the connection. This one-sided detection can result in generation of extra link-state PDUs that are flooded throughout the network. Specify the **adaptive** option to configure enough padding to establish an adjacency to neighbors.

- **Disabled padding**—Padding is disabled on all types of interfaces for all adjacency states. Specify the **disable** option to accommodate interfaces that support less than the default packet size of 1492 bytes.

- **Loose padding** (the default)—The hello packet is padded from the initial detection of a new neighbor until the adjacency transitions to the Up state. Loose padding might not be able to detect certain situations such as asymmetrical MTUs between the routing devices. Specify the **loose** option to configure enough padding to initialize an adjacency to neighbors.
• Strict padding—Padding is done on all interface types and for all adjacency states, and is continuous. Strict padding has the most overhead. The advantage is that strict padding detects MTU issues on both sides of a link. Specify the strict option to configure padding to allow all adjacency states with neighbors.

Options

- adaptive—Configure padding until the neighbor adjacency is established and active.
- disable—Disable padding on all types of interfaces for all adjacency states.
- loose—Configure padding until the state of the adjacency is initialized.
- strict—Configure padding for all adjacency states.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring IS-IS
**hold-time (Protocols IS-IS)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>hold-time seconds;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit logical-systems logical-system-name protocols isis interface interface-name level level-number], [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number], [edit protocols isis interface interface-name level level-number], [edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]</td>
</tr>
<tr>
<td>Description</td>
<td>Set the length of time a neighbor considers this router to be operative (up) after receiving a hello packet. If the neighbor does not receive another hello packet within the specified time, it marks this routing device as inoperative (down). The hold time itself is advertised in the hello packets. The hold time specifies how long a neighbor should consider this routing device to be operative without receiving another hello packet. If the neighbor does not receive a hello packet from this routing device within the hold time, it marks the routing device as being unavailable.</td>
</tr>
<tr>
<td>Options</td>
<td>seconds—Hold-time value, in seconds. Range: 3 through 65,535 seconds, or 1 to send out hello packets every 333 milliseconds Default: 9 seconds (for designated intermediate system [DIS] routers), 27 seconds (for non-DIS routers; three times the default hello interval)</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>routing—to view this statement in the configuration. routing-control—to add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• Example: Configuring IS-IS • hello-interval on page 2706</td>
</tr>
</tbody>
</table>
### ignore-attached-bit

**Syntax**

```plaintext
ignore-attached-bit;
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Ignore the attached bit on IS-IS Level 1 routers. Configuring this statement enables the routing device to ignore the attached bit on incoming Level 1 link-state PDUs. If the attached bit is ignored, no default route, which points to the routing device which has set the attached bit, is installed.

There might be times, such as during a denial-of-service (DoS) attack, that you do not want a Level 1 router to be able to forward traffic based on a default route.

To prevent a routing device from being able to reach interarea destinations, you can prevent the routing device from installing the default route without affecting the status of its IS-IS adjacencies. The `ignore-attached-bit` statement is used to tell the routing device to ignore the presence of the attached bit in Level 1 link-state PDUs, which blocks the installation of the IS-IS default route.

**Default**

The `ignore-attached-bit` statement is disabled by default.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>routing-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- [Juniper Networks](https://www.juniper.net)
interface (Protocols IS-IS)

Syntax

interface (all | interface-name) {
  disable;
  bfd-liveness-detection {
    authentication {
      algorithm algorithm-name;
      key-chain key-chain-name;
      loose-check;
    }
    detection-time {
      threshold milliseconds;
    }
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    transmit-interval {
      threshold milliseconds;
      minimum-interval milliseconds;
    }
    multiplier number;
  }
  checksum;
  csnp-interval (seconds | disable);
  hello-padding (adaptive | loose | strict);
  ldp-synchronization {
    disable;
    hold-time seconds;
  }
  lsp-interval milliseconds;
  mesh-group (value | blocked);
  no-adjacency-hold-down;
  no-ipv4-multicast;
  no-ipv6-multicast;
  no-ipv6-unicast;
  no-unicast-topology;
  passive;
  point-to-point;
  level level-number {
    disable;
    hello-authentication-key key;
    hello-authentication-key-chain key-chain-name;
    hello-authentication-type authentication;
    hello-interval seconds;
    hold-time seconds;
    ipv4-multicast-metric metric;
    ipv6-multicast-metric metric;
    ipv6-unicast-metric metric;
    metric metric;
    passive;
    priority number;
    te-metric metric;
  }
}
Hierarchy Level

[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Configure interface-specific IS-IS properties. To configure more than one interface, include the interface statement multiple times.

Enabling IS-IS on an interface (by including the interface statement at the [edit protocols isis] or the [edit routing-instances routing-instance-name protocols isis] hierarchy level), disabling it (by including the disable statement), and not actually having IS-IS run on an interface (by including the passive statement) are mutually exclusive states.

Options
all—Have Junos OS create IS-IS interfaces automatically. If you include this option, disable IS-IS on the management interface (fxp0).

interface-name—Name of an interface. Specify the full interface name, including the physical and logical address components.

The remaining statements are explained separately.

Required Privilege
level routing—To view this statement in the configuration.
level routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring IS-IS
• Example: Configuring Multi-Level IS-IS
**ipv4-multicast**

**Syntax**

`ipv4-multicast;`

**Hierarchy Level**

[edit logical-systems logical-system-name protocols isis topologies],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis topologies],
[edit routing-instances routing-instance-name protocols isis topologies]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure alternate IPv4 multicast topologies.

**NOTE:** The IS-IS interface metrics for the IPv4 topology can be configured independently of the IPv6 metrics. You can also selectively disable interfaces from participating in the IPv6 topology while continuing to participate in the IPv4 topology. This lets you exercise control over the paths that unicast data takes through a network.

**Default**

Multicast topologies are disabled.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring IS-IS Multicast Topology
ipv4-multicast-metric

Syntax
ipv4-multicast-metric metric;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
[edit protocols isis interface interface-name level level-number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Specify the multicast topology metric value for the level.

Options
metric—Metric value.

Range: 0 through 16,777,215

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring IS-IS Multicast Topology

ipv6-multicast

Syntax
ipv6-multicast;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis topologies],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis topologies],
[edit protocols isis topologies],
[edit routing-instances routing-instance-name protocols isis topologies]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Configure alternate IPv6 multicast topologies.

Default
Multicast topologies are disabled.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring IS-IS Multicast Topology
ipv6-multicast-metric

Syntax
ipv6-multicast-metric metric;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
[edit protocols isis interface interface-name level level-number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Specify the IPv6 alternate multicast topology metric value for the level.

Options
metric—Metric value.
Range: 0 through 16,777,215

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring IS-IS Multicast Topology
## ipv6-unicast

**Syntax**
```
ipv6-unicast;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols isis topologies],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis topologies],
[edit protocols isis topologies],
[edit routing-instances routing-instance-name protocols isis topologies]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure alternate IPv6 unicast topologies.

This statement causes IS-IS to calculate an alternate IPv6 unicast topology, in addition to the normal IPv4 unicast topology, and add the corresponding routes to inet6.0.

---

**NOTE:** The IS-IS interface metrics for the IPv4 topology can be configured independently of the IPv6 metrics. You can also selectively disable interfaces from participating in the IPv6 topology while continuing to participate in the IPv4 topology. This lets you exercise control over the paths that unicast data takes through a network.

---

**Default**
IPv6 unicast topologies are disabled.

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring IS-IS IPv4 and IPv6 Unicast Topologies*
ipv6-unicast-metric

Syntax
ipv6-unicast-metric metric;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
[edit protocols isis interface interface-name level level-number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Specify the IPv6 unicast topology metric value for the level. The IS-IS interface metrics for the IPv4 topology can be configured independently of the IPv6 metrics.

Options
metric—Metric value.
Range: 0 through 16,777,215

Required Privilege
level routing—To view this statement in the configuration.
level routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring IS-IS IPv4 and IPv6 Unicast Topologies
### isis

**Syntax**  
isis [...]

**Hierarchy Level**  
[edit logical-systems logical-system-name protocols],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols],  
[edit protocols],  
[edit routing-instances routing-instance-name protocols]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**  
Enable IS-IS routing on the routing device or for a routing instance.

The `isis` statement is the one statement you must include in the configuration to run IS-IS on the routing device or in a routing instance.

**Default**  
IS-IS is disabled on the routing device.

**Required Privilege**  
- routing—To view this statement in the configuration.  
- routing-control—To add this statement to the configuration.

**Related Documentation**  
- Example: Configuring IS-IS  
- Example: Configuring Multi-Level IS-IS
level (Global IS-IS)

Syntax  
level level-number {
    authentication-key key;
    authentication-key-chain (Protocols IS-IS) key-chain-name;
    authentication-type type;
    external-preference preference;
    no-csnp-authentication;
    no-hello-authentication;
    no-psnp-authentication;
    preference preference;
    wide-metrics-only;
}

Hierarchy Level  
[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description  
Configure the global-level properties.

You can administratively divide a single AS into smaller groups called areas. You configure each routing device interface to be in an area. Any interface can be in any area. The area address applies to the entire routing device. You cannot specify one interface to be in one area and another interface in a different area. To route between areas, you must have two adjacent Level 2 routers that communicate with each other.

Level 1 routers can only route within their IS-IS area. To send traffic outside their area, Level 1 routers must send packets to the nearest intra-area Level 2 router. A routing device can be a Level 1 router, a Level 2 router, or both. You specify the router level on a per-interface basis, and a routing device becomes adjacent to other routing devices on the same level on that link only.

You can configure one Level 1 routing process and one Level 2 routing process on each interface, and you can configure the two levels differently.

Options  
level-number—IS-IS level number.
Values: 1 or 2

The remaining statements are explained separately.

Required Privilege  
Level  
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation  
• Example: Configuring IS-IS
• Example: Configuring Multi-Level IS-IS
**link-protection (Protocols IS-IS)**

**Syntax**

```plaintext
link-protection;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols isis interface interface-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name]`
- `[edit protocols isis interface interface-name]`
- `[edit routing-instances routing-instance-name protocols isis interface interface-name]`

**Release Information**

- Statement introduced in Junos OS Release 9.5.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Enable link protection on the specified IS-IS interface. Junos OS creates a backup loop-free alternate path to the primary next hop for all destination routes that traverse the protected interface.

**Required Privilege**

- **Level** routing—To view this statement in the configuration.
- **Level** routing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring Link and Node Protection for IS-IS Routes*
- node-link-protection on page 2734

---

**loose-authentication-check**

**Syntax**

```plaintext
loose-authentication-check;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols isis]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis]`
- `[edit protocols isis]`
- `[edit routing-instances routing-instance-name protocols isis]`

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Allow the use of MD5 authentication without requiring network-wide deployment.

**Required Privilege**

- **Level** routing—To view this statement in the configuration.
- **Level** routing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*
**lsp-interval**

**Syntax**

```
lsp-interval milliseconds;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure the link-state PDU interval time.

By default, the routing device sends one link-state PDU packet out an interface every 100 milliseconds. To disable the transmission of all link-state PDUs, set the interval to 0.

Link-state PDU throttling by use of the `lsp-interval` statement controls the flooding pace to neighboring routing devices in order to not overload them.

Also, consider that control traffic (such as link-state PDUs and related packets) might delay user traffic (information packets) because control traffic always has precedence in terms of scheduling on the routing device interface cards. Unfortunately, the control traffic transmission rate is not decreased on low-bandwidth interfaces, such as DS-0 or fractional T1 and E1 interface. Line control traffic stays the same. On a low-bandwidth circuit that is transmitting 30 full-MTU-sized packets, there is not much bandwidth left over for other types of packets.

**Default**

By default, the routing device sends one link-state PDU out an interface every 100 milliseconds.

**Options**

`milliseconds`—Number of milliseconds between the sending of link-state PDUs. Specifying a value of 0 blocks all link-state PDU transmission.

**Range:** 0 through 1000 milliseconds

**Default:** 100 milliseconds

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring the Transmission Frequency for Link-State PDUs on IS-IS Interfaces
**lsp-lifetime**

**Syntax**

```plaintext
lsp-lifetime seconds;
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Specify how long a link-state PDU originating from the routing device should persist in the network. The routing device sends link-state PDUs often enough so that the link-state PDU lifetime never expires.

Because link-state PDUs have a maximum lifetime, they need to be refreshed. Refreshing means that a routing device needs to re-originate its link-state PDUs periodically. The re-origination interval must be less than the link-state PDU’s lifetime. For example, if the link-state PDU is valid for 1200 seconds, the routing device needs to refresh the link-state PDU in less than 1200 seconds to avoid removal of the link-state PDU from the link-state database by other routing devices. The recommended maximum link-state PDU origination interval is the lifetime minus 300 seconds. So, in a default environment this would be 900 seconds. In Junos OS, the refresh interval is derived from the lifetime and is equal to the lifetime minus 317 seconds. You can change the lifetime to a higher value to reduce the number of refreshes in the network. (You would rarely want to increase the number of refreshes.) Often these periodic link-state PDU refreshes are referred to as refresh noise, and network administrators want to reduce this noise as much as possible.

The `show isis overview` command displays the link-state PDU lifetime.

**Default**

By default, link-state PDUs are maintained in network databases for 1200 seconds (20 minutes) before being considered invalid. This length of time, called the **LSP lifetime**, normally is sufficient to guarantee that link-state PDUs never expire.

**Options**

- `seconds`—link-state PDU lifetime, in seconds.
  - **Range:** 350 through 65,535 seconds
  - **Default:** 1200 seconds

**Required Privilege Level**

- **Routing**—To view this statement in the configuration.
- **Routing-Control**—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring the Transmission Frequency for Link-State PDUs on IS-IS Interfaces](http://www.juniper.net/us/en/training/certification/JNCIP_studyguide.pdf)
max-areas

**Syntax**

max-areas number;

**Hierarchy Level**

[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis]
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]

**Release Information**

Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Modify the maximum number of IS-IS areas advertised.

This value is included in the Maximum Address Area field of the IS-IS common PDU header included in all outgoing PDUs.

The maximum number of areas you can advertise is restricted to 36 to ensure that the IIH PDUs have enough space to include other type, length, and value (TLV) fields, such as the Authentication and IPv4 and IPv6 Interface Address TLVs.

**Options**

*number*—Maximum number of areas to include in the IS-IS hello (IIH) PDUs and link-state PDUs.

**Range**: 3 through 36

**Default**: 3

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

* Example: Configuring Multi-Level IS-IS
**mesh-group (Protocols IS-IS)**

**Syntax**

```plaintext
mesh-group (blocked | value);
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols isis interface interface-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name]`
- `[edit protocols isis interface interface-name]`
- `[edit routing-instances routing-instance-name protocols isis interface interface-name]`

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure an interface to be part of a mesh group, which is a set of fully connected nodes.

A *mesh group* is a set of routing devices that are fully connected. That is, they have a fully meshed topology. When link-state PDUs are being flooded throughout an area, each router within a mesh group receives only a single copy of a link-state PDU instead of receiving one copy from each neighbor, thus minimizing the overhead associated with the flooding of link-state PDUs.

To create a mesh group and designate that an interface be part of the group, assign a mesh-group number to all the routing device interfaces in the group. To prevent an interface in the mesh group from flooding link-state PDUs, configure blocking on that interface.

**Options**

- **blocked**—Configure the interface so that it does not flood link-state PDUs.

- **value**—Number that identifies the mesh group.

  **Range:** 1 through 4,294,967,295 ($2^{32} - 1$; 32 bits are allocated to identify a mesh group)

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring Mesh Groups of IS-IS Interfaces*
**metric (Protocols IS-IS)**

**Syntax**

```
metric metric;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
[edit protocols isis interface interface-name level level-number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Specify the metric value for the level.

All IS-IS routes have a cost, which is a routing metric that is used in the IS-IS link-state calculation. The cost is an arbitrary, dimensionless integer that can be from 1 through 63, or from 1 through 16,777,215 \((2^{24} – 1)\) if you are using wide metrics.

Similar to other routing protocols, IS-IS provides a way of exporting routes from the routing table into the IS-IS network. When a route is exported into the IS-IS network without a specified metric, IS-IS uses default metric values for the route, depending on the protocol that was used to learn the route.

Table 338 on page 2725 depicts IS-IS route export metric default values.

### Table 338: Default Metric Values for Routes Exported into IS-IS

<table>
<thead>
<tr>
<th>Protocol Used for Learning the Route</th>
<th>Default Metric Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>10</td>
</tr>
<tr>
<td>Static</td>
<td>Same as reported by the protocol used for exporting the route</td>
</tr>
<tr>
<td>Aggregate</td>
<td>10</td>
</tr>
<tr>
<td>Generate</td>
<td>10</td>
</tr>
<tr>
<td>RIP</td>
<td>Same as reported by the protocol used for exporting the route</td>
</tr>
<tr>
<td>OSPF</td>
<td>Same as reported by the protocol used for exporting the route</td>
</tr>
<tr>
<td>BGP</td>
<td>10</td>
</tr>
</tbody>
</table>

The default metric values behavior can be customized by using routing policies.

**Options**

- **metric**—Metric value.
- **Range:** 1 through 63, or 1 through 16,777,215 (if you have configured wide metrics)
Default: 10 (for all interfaces except lo0), 0 (for the lo0 interface)

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Enabling Wide IS-IS Metrics for Traffic Engineering
• te-metric
• wide-metrics-only on page 2750

no-adjacency-holddown

Syntax no-adjacency-holddown;

Hierarchy Level [edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]

Release Information Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description Disable the hold-down timer for IS-IS adjacencies.

A hold-down timer delays the advertising of adjacencies by waiting until a time period has elapsed before labeling adjacencies in the up state. You can disable this hold-down timer, which labels adjacencies up faster. However, disabling the hold-down timer creates more frequent link-state PDU updates and SPF computation.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation • hold-time on page 2709
no-authentication-check

Syntax
no-authentication-check;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Generate authenticated packets and check the authentication on received packets, but
do not reject packets that cannot be authenticated.

Required Privilege
Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• csnp-interval on page 2699
• hello-authentication-type on page 2705

no-csnp-authentication

Syntax
no-csnp-authentication;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
[edit protocols isis level level-number],
[edit routing-instances routing-instance-name protocols isis level level-number]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Suppress authentication check on complete sequence number PDU (CSNP) packets.

Required Privilege
Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• csnp-interval on page 2699
no-eligible-backup (Protocols IS-IS)

Syntax

```plaintext
no-eligible-backup;
```

Hierarchy Level

```plaintext
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Exclude the specified interface as a backup interface for IS-IS interfaces on which link protection or node-link protection is enabled.

Required Privilege

- Level routing—To view this statement in the configuration.
- Level routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Link and Node Protection for IS-IS Routes
- link-protection on page 2720
- node-link-protection on page 2734

no-hello-authentication

Syntax

```plaintext
no-hello-authentication;
```

Hierarchy Level

```plaintext
[edit logical-systems logical-system-name protocols isis level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
[edit protocols isis level level-number],
[edit routing-instances routing-instance-name protocols isis level level-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Suppress authentication check on complete sequence number hello packets.

Required Privilege

- Level routing—To view this statement in the configuration.
- Level routing-control—To add this statement to the configuration.

Related Documentation

- hello-authentication-type on page 2705
no-ipv4-multicast

Syntax

\[
\text{no-ipv4-multicast;}
\]

Hierarchy Level

[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Exclude an interface from IPv4 multicast topologies.

Default

Multicast topologies are disabled.

Required Privilege

Level: routing—to view this statement in the configuration.
Level: routing-control—to add this statement to the configuration.

Related Documentation

* Example: Configuring IS-IS Multicast Topology
no-ipv4-routing

Syntax  
no-ipv4-routing;

Hierarchy Level  
[edit logical-systems logical-system-name protocols isis],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],  
[edit protocols isis],  
[edit routing-instances routing-instance-name protocols isis]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description  
Disable IP version 4 (IPv4) routing.

Disabling IPv4 routing has the following results:

- The routing device does not advertise the network layer protocol identifier (NLPID) for IPv4 in the Junos OS link-state PDU fragment zero.
- The routing device does not advertise any IPv4 prefixes in Junos OS link-state PDUs.
- The routing device does not advertise the NLPID for IPv4 in Junos OS hello packets.
- The routing device does not advertise any IPv4 addresses in Junos OS hello packets.
- The routing device does not calculate any IPv4 routes.

NOTE: Note: Even when no-ipv4-routing is configured, an IS-IS traceoptions log can list rejected IPv4 addresses. When a configuration is committed, IS-IS schedules a scan of the routing table to determine whether any routes need to be exported into the IS-IS link state database. The implicit default export policy action is to reject everything. IPv4 addresses from the routing table are examined for export, rejected by the default policy, and the rejections are logged.

Required Privilege Level  
- routing—To view this statement in the configuration.  
- routing-control—To add this statement to the configuration.

Related Documentation  
- Example: Configuring IS-IS IPv4 and IPv6 Unicast Topologies
no-ipv6-multicast

Syntax

no-ipv6-multicast;

Hierarchy Level

[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Exclude an interface from the IPv6 multicast topologies.

Default

Multicast topologies are disabled.

Required Privilege

Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring IS-IS Multicast Topology
**no-ipv6-routing**

**Syntax**
```
no-ipv6-routing;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Disable IP version 6 (IPv6) routing.

Disabling IPv6 routing has the following results:

- The routing device does not advertise the network layer protocol identifier (NLPID) for IPv6 in the Junos OS link-state PDU fragment zero.
- The routing device does not advertise any IPv6 prefixes in Junos OS link-state PDUs.
- The routing device does not advertise the NLPID for IPv6 in Junos OS hello packets.
- The routing device does not advertise any IPv6 addresses in Junos OS hello packets.
- The routing device does not calculate any IPv6 routes.

**Required Privilege**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring IS-IS IPv4 and IPv6 Unicast Topologies
**no-ipv6-unicast**

**Syntax**

```
no-ipv6-unicast;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Exclude an interface from the IPv6 unicast topologies. This enables you to exercise control over the paths that unicast data takes through a network.

**Default**

IPv6 unicast topologies are disabled.

**Required Privilege**

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring IS-IS IPv4 and IPv6 Unicast Topologies

---

**no-psnp-authentication**

**Syntax**

```
no-psnp-authentication;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols isis level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
[edit protocols isis level level-number],
[edit routing-instances routing-instance-name protocols isis level level-number]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Suppress authentication check on partial sequence number PDU (PSNP) packets.

**Required Privilege**

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring IS-IS Authentication
no-unicast-topology

Syntax
no-unicast-topology;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]

Release Information
Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Exclude an interface from the IPv4 unicast topologies.

Default
IPv4 unicast topologies are disabled.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring IS-IS Multicast Topology

node-link-protection (Protocols IS-IS)

Syntax
node-link-protection;

Hierarchy Level
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-routers logical-router-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name]

Release Information
Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Enable node-link protection on the specified IS-IS interface. Junos OS creates an alternate loop-free path to the primary next hop for all destination routes that traverse a protected interface. This alternate path avoids the primary next-hop routing device altogether and establishes a path through a different routing device.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Link and Node Protection for IS-IS Routes
• link-protection on page 2720
overload (Protocols IS-IS)

**Syntax**

```plaintext
overload {
    advertise-high-metrics;
    allow-route-leaking;
    timeout seconds;
}
```

**Hierarchy Level**

- `edit logical-systems logical-system-name protocols isis`
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis`
- `edit protocols isis`
- `edit routing-instances routing-instance-name protocols isis`

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure the local routing device so that it appears to be overloaded. This statement causes the routing device to continue participating in IS-IS routing, but prevents it from being used for transit traffic. Traffic destined to immediately attached subnets continues to transit the routing device.

You can also advertise maximum link metrics in network layer reachability information (NLRI) instead of setting the overload bit.

You configure or disable overload mode in IS-IS with or without a timeout. Without a timeout, overload mode is set until it is explicitly deleted from the configuration. With a timeout, overload mode is set if the time elapsed since the IS-IS instance started is less than the specified timeout.

A timer is started for the difference between the timeout and the time elapsed since the instance started. If the time elapsed after the IS-IS instance is enabled is less than the specified timeout, overload mode is set. When the timer expires, overload mode is cleared. In overload mode, the routing device IS-IS advertisements are originated with the overload bit set. This causes the transit traffic to take paths around the routing device. However, the overloaded routing device's own links are still accessible.

The value of the overload bit depends on these three scenarios:

1. When the overload bit has already been set to a given value and the routing process is restarted: Link-state PDUs are regenerated with the overload bit cleared.
2. When the overload bit is reset to a lesser value while the routing process is running: Link-state PDUs are regenerated with the overload bit cleared.
3. When the overload bit is reset to a greater value while the routing process is running: Link-state PDUs are regenerated with the overload bit set to the difference between the old and new value.

In overload mode, the routing device advertisement is originated with all the transit routing device links (except stub) set to a metric of 0xFFFF. The stub routing device links are
advertised with the actual cost of the interfaces corresponding to the stub. This causes the transit traffic to avoid the overloaded routing device and take paths around the routing device.

To understand the reason for setting the overload bit, consider that BGP converges slowly. It is not very good at detecting that a neighbor is down because it has slow-paced keepalive timers. Once the BGP neighbor is determined to be down, it can take up to 2 minutes for a BGP router to declare the neighbor down. IS-IS is much quicker. IS-IS only takes 10-30 seconds to detect absent peers. It is the slowness of BGP, more precisely the slowness of internal BGP (IBGP), that necessitates the use of the overload bit. IS-IS and BGP routing are mutually dependent on each other. If both do not converge at the same time, traffic is dropped without notification (black holed).

You might want to configure the routing device so that it appears to be overloaded when you are restarting routing on the device. Setting the overload bit for a fixed amount of time right after a restart of the routing protocol process (rpd) ensures that the router does not receive transit traffic while the routing protocols (especially IBGP) are still converging.

Setting the overload bit is useful when performing hardware or software maintenance work on a routing device. After the maintenance work, clear the overload bit to carry on forwarding transit traffic. Manual clearing of the overload bit is not always possible. What is needed is an automated way of clearing the overload bit after some amount of time. Most networks use a time value of 300 seconds. This 5-minute value provides a good balance, allowing time to bring up even large internal IBGP meshes, while still relatively quick.

Another appropriate application for setting for the overload bit is on dedicated devices such as BGP route reflectors, which are intentionally not meant to carry any transit traffic. In this case, you would not use the timer.

You can verify that the overload bit is set by running the `show isis database` command.
**Options**  
**advertise-high-metrics**—Advertise maximum link metrics in NLRIs instead of setting the overload bit.

The **advertise-high-metric** setting is only valid while the routing device is in overload mode. When **advertise-high-metric** is configured, IS-IS does not set the overload bit. Rather, it sets the metric to 63 or 16,777,214, depending whether wide metrics are enabled. This allows the overloaded routing device to be used for transit as a last resort.

An L1-L2 router in overload mode stops leaking route information between L1 and L2 levels and clears its attached bit. This is also true when **advertise-high-metrics** is configured.

**allow-route-leaking**—Enable leaking of route information into the network even if the overload bit is set.

---

**NOTE:** The **allow-route-leaking** option does not work if the routing device is in dynamic overload mode. Dynamic overload can occur if the device has exceeded its resource limits, such as the prefix limit.

---

**timeout seconds**—Number of seconds at which the overloading is reset.  
**Range:** 60 through 1800 seconds  
**Default:** 0 seconds

---

**Required Privilege**  
**Level**  
route—To view this statement in the configuration.  
route-control—To add this statement to the configuration.

---

**Related Documentation**  
• Example: Configuring IS-IS
passive (Protocols IS-IS)

**Syntax**
```
passive;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols isis interface interface-name],
[edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
[edit protocols isis interface interface-name],
[edit protocols isis interface interface-name level level-number],
[edit routing-instances routing-instance-name protocols isis interface interface-name],
[edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Advertise the direct interface addresses on an interface or into a level on the interface without actually running IS-IS on that interface or level.

This statement effectively prevents IS-IS from running on the interface. To enable IS-IS on an interface, include the ```interface``` statement at the [edit protocols isis] or the [edit routing-instances routing-instance-name protocols isis] hierarchy level. To disable it, include the ```disable``` statement at those hierarchy levels. The three states—enabling, disabling, or not running IS-IS on an interface—are mutually exclusive.

---

**NOTE:** Configuring IS-IS on a loopback interface automatically renders it as a passive interface, irrespective of whether the passive statement was used in the configuration of the interface.

If neither passive mode nor the ```family iso``` option is configured on the IS-IS interface, then the routing device treats the interface as not being operational, and no direct IPv4/IPv6 routes are exported into IS-IS. (You configure the ```family iso``` option at the [edit interfaces interface-name unit logical-unit-number] hierarchy level.)

**Default**
By default, IS-IS must be configured on an interface or a level for direct interface addresses to be advertised into that level.

**Required Privilege Level**
- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

**Related Documentation**
- Example: Configuring Multi-Level IS-IS
- ```disable```
point-to-point

**Syntax**  
point-to-point;

**Hierarchy Level**  
[edit logical-systems logical-system-name protocols isis interface interface-name],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name],  
[edit protocols isis interface interface-name],  
[edit routing-instances routing-instance-name protocols isis interface interface-name]

**Release Information**  
Statement introduced before Junos OS Release 7.4,  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**  
Configure an IS-IS interface to behave like a point-to-point connection.

You can use the **point-to-point** statement to configure a LAN interface to act like a point-to-point interface for IS-IS. You do not need an unnumbered LAN interface, and it has no effect if configured on an interface that is already point-to-point.

The **point-to-point** statement affects only IS-IS protocol procedures on that interface. All other protocols continue to treat the interface as a LAN interface. Only two IS-IS routing devices can be connected to the LAN interface, and both must be configured as point-to-point.

**Required Privilege Level**  
- routing—To view this statement in the configuration.  
- routing-control—To add this statement to the configuration.

**Related Documentation**  
- **IS-IS Overview**  
- **Understanding IS-IS Designated Routers**  
- **Example: Configuring Synchronization Between IS-IS and LDP**
**preference (Protocols IS-IS)**

**Syntax**

`preference preference;`

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols isis level level-number]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number]`
- `[edit protocols isis level level-number]`
- `[edit routing-instances routing-instance-name protocols isis level level-number]`

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure the preference of internal routes.

Route preferences (also known as administrative distances) are used to select which route is installed in the forwarding table when several protocols calculate routes to the same destination. The route with the lowest preference value is selected.

To change the preference values, include the `preference` statement (for internal routes) or the `external-preference` statement.

**Options**

- `preference`—Preference value.
  - **Range:** 0 through 4,294,967,295 (2^{32} – 1)
  - **Default:** 15 (for Level 1 internal routes), 18 (for Level 2 internal routes), 160 (for Level 1 external routes), 165 (for Level 2 external routes)

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Route Preferences Overview
- Example: Redistributing OSPF Routes into IS-IS
- Example: Redistributing BGP Routes with a Specific Community Tag into IS-IS
- `external-preference` on page 2702
prefix-export-limit (Protocols IS-IS)

**Syntax**
```
prefix-export-limit number;
```

**Hierarchy Level**
- [edit logical-systems logical-system-name protocols isis level level-number],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
- [edit protocols isis level level-number],
- [edit routing-instances routing-instance-name protocols isis level level-number]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Configure a limit to the number of prefixes exported into IS-IS.

By default, there is no limit to the number of prefixes that can be exported into IS-IS. To configure a limit to the number of prefixes that can be exported into IS-IS, include the `prefix-export-limit` statement. The `prefix-export-limit` statement protects the rest of the network from a malicious policy by applying a threshold filter for exported routes.

The number of prefixes depends on the size of your network. Good design advice is to set it to double the total number of IS-IS Level 1 and Level 2 routing devices in your network.

If the number of prefixes exported into IS-IS exceeds the configured limit, the overload bit is set and the overload state is reached. When other routers detect that this bit is set, they do not use this routing device for transit traffic, but they do use it for packets destined to the overloaded routing device's directly connected networks and IP prefixes. The overload state can be cleared by using the `clear isis overload` command.

The `show isis overview` command displays the prefix export limit when it is configured.

**Options**
- **number**—Prefix limit.
  - **Range:** 0 through 4,294,967,295 (2^{32} – 1)
  - **Default:** None

**Required Privilege**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Redistributing BGP Routes with a Specific Community Tag into IS-IS
- Example: Redistributing OSPF Routes into IS-IS
priority (Protocols IS-IS)

Syntax

```
priority number;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols isis interface interface-name level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis interface interface-name level level-number],
[edit protocols isis interface interface-name level level-number],
[edit routing-instances routing-instance-name protocols isis interface interface-name level level-number]
```

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Configure the interface’s priority for becoming the designated router. The interface with the highest priority value becomes that level’s designated router.

The priority value is meaningful only on a multiaccess network. It has no meaning on a point-to-point interface.

A routing device advertises its priority to become a designated router in its hello packets. On all multiaccess networks, IS-IS uses the advertised priorities to elect a designated router for the network. This routing device is responsible for sending network link-state advertisements, which describe all the routing devices attached to the network. These advertisements are flooded throughout a single area.

A routing device’s priority for becoming the designated router is indicated by an arbitrary number from 0 through 127. Routing devices with a higher value are more likely to become the designated router.

Options

- **number**—Priority value.
  - Range: 0 through 127
  - Default: 64

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring IS-IS Designated Routers
**reference-bandwidth (Protocols IS-IS)**

**Syntax**
```
reference-bandwidth reference-bandwidth;
```

**Hierarchy Level**
- `[edit logical-systems logical-system-name protocols isis]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis]`
- `[edit protocols isis]`
- `[edit routing-instances routing-instance-name protocols isis]`

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Optimize routing based on bandwidth by setting the reference bandwidth used in calculating the default interface cost.

All IS-IS interfaces have a cost, which is a routing metric that is used in the IS-IS link-state calculation. Routes with lower total path metrics are preferred over those with higher path metrics. When there are several equal-cost routes to a destination, traffic is distributed equally among them.

The cost of a route is described by a single dimensionless metric that is determined using the following formula:

\[
\text{cost} = \frac{\text{reference-bandwidth}}{\text{bandwidth}}
\]

For example, if you set the reference bandwidth to 1 Gbps (that is, `reference-bandwidth` is set to 1,000,000,000), a 100-Mbps interface has a routing metric of 10.

All IS-IS interfaces have a cost, which is a routing metric that is used in the IS-IS link-state calculation. Routes with lower total path metrics are preferred over those with higher path metrics.

**Options**
- `reference-bandwidth`—Reference bandwidth value in bits per second.

  **Range:** 9600 through 1,000,000,000,000 bps
  **Default:** None

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring IS-IS
rib-group (Protocols IS-IS)

Syntax

```
rib-group {
    inet group-name;
    inet6 group-name;
}
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols isis],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
- [edit protocols isis],
- [edit routing-instances routing-instance-name protocols isis]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Install routes learned from IS-IS routing instances into routing tables in the IS-IS routing table group. You can install IPv4 routes or IPv6 routes.

Support for IPv6 routing table groups in IS-IS enables IPv6 routes that are learned from IS-IS routing instances to be installed into other routing tables defined in an IS-IS routing table group.

Options

- **group-name**—Name of the routing table group.
- **inet**—Install IPv4 IS-IS routes.
- **inet6**—Install IPv6 IS-IS routes.

Required Privilege Level

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

Related Documentation

- Example: Exporting Specific Routes from One Routing Table Into Another Routing Table
- Example: Importing Direct and Static Routes Into a Routing Instance
- Understanding Multiprotocol BGP
### spf-options (Protocols IS-IS)

**Syntax**

```json
spf-options {
    delay milliseconds;
    holddown milliseconds;
    rapid-runs number;
}
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols isis],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
- [edit protocols isis],
- [edit routing-instances routing-instance-name protocols isis]

**Release Information**

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure options for running the shortest-path-first (SPF) algorithm.

Running the SPF algorithm is usually the beginning of a series of larger system-wide events. For example, the SPF algorithm can lead to interior gateway protocol (IGP) prefix changes, which then lead to BGP nexthop resolution changes. Consider what happens if there are rapid link changes in the network. The local routing device can become overwhelmed. This is why it sometimes makes sense to throttle the scheduling of the SPF algorithm.

You can configure the following SPF options:

- The delay in the time between the detection of a topology change and when the SPF algorithm actually runs.
- The maximum number of times that the SPF algorithm can run in succession before the hold-down timer begins.
- The time to hold down, or wait, before running another SPF calculation after the SPF algorithm has run in succession the configured maximum number of times.

If the network stabilizes during the hold-down period and the SPF algorithm does not need to run again, the system reverts to the configured values for the `delay` and `rapid-runs` statements.

**Options**

- `delay milliseconds`—Time interval between the detection of a topology change and when the SPF algorithm runs.
  
  **Range:** 50 through 1000 milliseconds
  
  **Default:** 200 milliseconds

- `holddown milliseconds`—Time interval to hold down, or wait before a subsequent SPF algorithm runs after the SPF algorithm has run in succession the configured maximum number of times in succession.
  
  **Range:** 2000 through 10,000 milliseconds
  
  **Default:** 5000 milliseconds
rapid-runs number—Maximum number of times the SPF algorithm can run in succession. After the maximum is reached, the holddown interval begins.

Range: 1 through 5
Default: 3

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring Link and Node Protection for IS-IS Routes

**topologies (Protocols IS-IS)**

Syntax
topologies {
ipv4-multicast;
ipv6-multicast;
ipv6-unicast;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols isis],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
[edit protocols isis],
[edit routing-instances routing-instance-name protocols isis]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Configure alternate IS-IS topologies.

The remaining statements are explained separately.

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring IS-IS IPv4 and IPv6 Unicast Topologies
- Example: Configuring IS-IS Multicast Topology
**traceoptions (Protocols IS-IS)**

**Syntax**

```
traceoptions {
    file name <size size> <files number> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols isis],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis],
- [edit protocols isis],
- [edit routing-instances routing-instance-name protocols isis]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure IS-IS protocol-level tracing options. To specify more than one tracing operation, include multiple `flag` statements.

**NOTE:** The `traceoptions` statement is not supported on QFabric systems.

**Default**

The default IS-IS protocol-level tracing options are those inherited from the routing protocols `traceoptions` statement included at the `[edit routing-options]` hierarchy level.

**Options**

- `disable`—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as `all`.

- `file name`—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks (" "). All files are placed in the directory `/var/log`. We recommend that you place IS-IS tracing output in the file `isis-log`.

- `files number`—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

  **Range:** 2 through 1000 files

  **Default:** 10 files

- `flag flag`—Tracing operation to perform. To specify more than one flag, include multiple `flag` statements.

**IS-IS Protocol-Specific Tracing Flags**
- **csn**—Complete sequence number PDU (CSNP) packets
- **error**—Errored IS-IS packets
- **graceful-restart**—Graceful restart operation
- **hello**—Hello packets
- **ldp-synchronization**—Synchronization between IS-IS and LDP
- **lsp**—Link-state PDUs
- **lsp-generation**—Link-state PDU generation packets
- **packets**—All IS-IS protocol packets
- **psn**—Partial sequence number PDU (PSNP) packets
- **spf**—Shortest-path-first calculations

**Global Tracing Flags**

- **all**—All tracing operations
- **general**—A combination of the **normal** and **route** trace operations
- **normal**—All normal operations, including adjacency changes

**Default:** If you do not specify this option, only unusual or abnormal operations are traced.

- **policy**—Policy operations and actions
- **route**—Routing table changes
- **state**—State transitions
- **task**—Routing protocol task processing
- **timer**—Routing protocol timer processing

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Provide detailed trace information.
- **receive**—Trace the packets being received.
- **send**—Trace the packets being transmitted.

**no-world-readable**—(Optional) Prevent any user from reading the log file.
size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When the *trace-file* again reaches its maximum size, *trace-file.0* is renamed *trace-file.1* and *trace-file* is renamed *trace-file.0*. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. Note that if you specify a maximum file size, you also must specify a maximum number of trace files with the files option.

Syntax:  xk to specify KB, xm to specify MB, or xg to specify GB

Range:  10 KB through the maximum file size supported on your system

Default:  128 KB

world-readable—(Optional) Allow any user to read the log file.

Required Privilege Level

- routing and trace—To view this statement in the configuration.
- routing-control and trace-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring the Transmission Frequency for CSNPs on IS-IS Interfaces
- Example: Configuring the Transmission Frequency for Link-State PDU on IS-IS Interfaces
- Example: Enabling Packet Checksums on IS-IS Interfaces
### wide-metrics-only

**Syntax**

wide-metrics-only;

**Hierarchy Level**

[edit logical-systems logical-system-name protocols isis level level-number],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols isis level level-number],
[edit protocols isis level level-number],
[edit routing-instances routing-instance-name protocols isis level level-number]

**Release Information**

Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure IS-IS to generate metric values greater than 63 on a per IS-IS level basis.

Normally, IS-IS metrics can have values up to 63, and IS-IS generates two type, length, and value (TLV) tuples, one for an IS-IS adjacency and the second for an IP prefix. To allow IS-IS to support traffic engineering, a second pair of TLVs has been added to IS-IS, one for IP prefixes and the second for IS-IS adjacency and traffic engineering information. With these TLVs, IS-IS metrics can have values up to 16,777,215 ($2^{24} - 1$).

To configure IS-IS to generate only the new pair of TLVs and thus to allow the wider range of metric values, include the `wide-metrics-only` statement.

**Default**

By default, Junos OS supports the sending and receiving of wide metrics. Junos OS allows a maximum metric value of 63 and generates both pairs of TLVs.

**Required Privilege**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Enabling Wide IS-IS Metrics for Traffic Engineering
- `te-metric`
CHAPTER 53

Administration

- Operational Commands on page 2751

Operational Commands
**clear isis adjacency**

**Syntax**

```
clear isis adjacency
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>
<neighbor>
```

**Syntax (EX Series Switches and QFX Series)**

```
clear isis adjacency
<instance instance-name>
<interface interface-name>
<neighbor>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Remove entries from the IS-IS adjacency database.

**Options**

- **none**—Remove all entries from the adjacency database.
  - **instance instance-name**—(Optional) Clear all adjacencies for the specified routing instance only.
  - **interface interface-name**—(Optional) Clear all adjacencies for the specified interface only.
  - **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
  - **neighbor**—(Optional) Clear adjacencies for the specified neighbor only.

**Required Privilege Level**

- **clear**

**Related Documentation**

- show isis adjacency on page 2760

**List of Sample Output**

**clear isis adjacency on page 2752**

**Output Fields**

See show isis adjacency for an explanation of output fields.

**Sample Output**

The following sample output displays IS-IS adjacency database information before and after the **clear isis adjacency** command is entered:

```
user@host> show isis adjacency
IS-IS adjacency database:
Interface    System    L State Hold (secs) SNPA
so-1/0/0.0    karakul    3 Up                26
so-1/1/3.0    1921.6800.5080 3 Up 23
```
so-5/0/0.0  1921.6800.5080  3 Up  19

user@host> clear isis adjacency karakul

user@host> show isis adjacency
IS-IS adjacency database:
Interface   System       L State      Hold (secs)     SNPA
so-1/0/0.0   karakul     3 Initializing 26
so-1/1/3.0   1921.6800.5080 3 Up  24
so-5/0/0.0   1921.6800.5080 3 Up  21
clear isis database

Syntax

```
clear isis database
<entries>
<instance instance-name>
<logical-system (all | logical-system-name)>
<purge>
```

Syntax (EX Series Switches and QFX Series)

```
clear isis database
<entries>
<instance instance-name>
<purge>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`purge` option introduced in Junos OS Release 9.0.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Remove the entries from the IS-IS link-state database, which contains prefixes and topology information. You can also use `purge` with any of the options to initiate a network-wide purge of link-state PDUs rather than the local deletion of entries from the IS-IS link-state database.

**CAUTION:** In a production network, the `purge` command option might cause short-term network-wide traffic disruptions.

Options

- **none**—Remove all entries from the IS-IS link-state database for all routing instances.
- **entries**—(Optional) Name of the database entry.
- **instance instance-name**—(Optional) Clear all entries for the specified routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **purge**—(Optional) Discard all entries in the IS-IS link-state database.

Required Privilege Level
clear

Related Documentation

- show isis database on page 2774

List of Sample Output

clear isis database on page 2755

Output Fields

See show isis database for an explanation of output fields.
Sample Output

clear isis database

The following sample output displays IS-IS link-state database information before and after the clear isis database command is entered:

```
user@host> show isis database
IS-IS level 1 link-state database:
LSP ID                  Sequence Checksum Lifetime (secs)
crater.00-00                0x12   0x84dd            1139
1 LSPs
IS-IS level 2 link-state database:
LSP ID                  Sequence Checksum Lifetime (secs)
crater.00-00                0x19   0xe92c            1134
badlands.00-00              0x16   0x1454             985
carlsbad.00-00              0x33   0x220b            1015
ranier.00-00                0x2e   0xfc31            1007
1921.6800.5066.00-00        0x11   0x7313             566
1921.6800.5067.00-00        0x14   0xd9d4             939
6 LSPs

user@host> clear isis database

user@host> show isis database
IS-IS level 1 link-state database:
LSP ID                  Sequence Checksum Lifetime (secs)

IS-IS level 2 link-state database:
LSP ID                  Sequence Checksum Lifetime (secs)
```
clear isis overload

Syntax

```plaintext
clear isis overload
<instance instance-name>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches and QFX Series)

```plaintext
clear isis overload
<instance instance-name>
```

Release Information

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Reset the IS-IS dynamic overload bit. This command can appear to not work, continuing to display overload after execution. The bit is reset only if the root cause is corrected by configuration remotely or locally.

When other routers detect that the overload bit is set, they do not use this routing device for transit traffic, but they do use it for packets destined to the overloaded routing device’s directly connected networks and IP prefixes.

Options

- `none`—Reset the IS-IS dynamic overload bit.
- `instance instance-name`—(Optional) Reset the IS-IS dynamic overload bit for the specified routing instance.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

- `clear`

Related Documentation

- `show isis database` on page 2774

List of Sample Output

- `clear isis overload` on page 2756

Output Fields

See `show isis database` for an explanation of output fields.

Sample Output

The following sample output displays IS-IS database information before and after the `clear isis overload` command is entered:

```
user@host> show isis database
IS-IS level 1 link-state database:
LSP ID Sequence Checksum Lifetime Attributes
pro3-c.00-00 0x4 0x10db 1185 L1 L2 Overload
 1 LSPs
```
### IS-IS level 2 link-state database:

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>pro3-c.00-00</td>
<td>0x5</td>
<td>0x429f</td>
<td>1185</td>
<td>L1 L2 Overload</td>
</tr>
<tr>
<td>pro2-a.00-00</td>
<td>0x91e</td>
<td>0x2589</td>
<td>874</td>
<td>L1 L2</td>
</tr>
<tr>
<td>pro2-a.02-00</td>
<td>0x1</td>
<td>0xcbc</td>
<td>874</td>
<td>L1 L2</td>
</tr>
</tbody>
</table>

3 LSPs

---

```
user@host> clear isis overload

user@host> show isis database
```

### IS-IS level 1 link-state database:

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>pro3-c.00-00</td>
<td>0xa</td>
<td>0x429e</td>
<td>1183</td>
<td>L1 L2</td>
</tr>
</tbody>
</table>

1 LSPs

### IS-IS level 2 link-state database:

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>pro3-c.00-00</td>
<td>0xc</td>
<td>0x9c39</td>
<td>1183</td>
<td>L1 L2</td>
</tr>
<tr>
<td>pro2-a.00-00</td>
<td>0x91e</td>
<td>0x2589</td>
<td>783</td>
<td>L1 L2</td>
</tr>
<tr>
<td>pro2-a.02-00</td>
<td>0x1</td>
<td>0xcbc</td>
<td>783</td>
<td>L1 L2</td>
</tr>
</tbody>
</table>

3 LSPs
**clear isis statistics**

**Syntax**
```
clear isis statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and QFX Series)**
```
clear isis statistics
<instance instance-name>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Set statistics about IS-IS traffic to zero.

**Options**
- **none**—Set IS-IS traffic statistics to zero for all routing instances.
- **instance instance-name**—(Optional) Set IS-IS traffic statistics to zero for the specified routing instance only.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
```
view
```

**Related Documentation**
- [show isis statistics on page 2798](#)

**List of Sample Output**
```
clear isis statistics on page 2758
```

**Output Fields**
See [show isis statistics](#) for an explanation of output fields.

**Sample Output**
```
clear isis statistics
```

The following sample output displays IS-IS statistics before and after the `clear isis statistics` command is entered:

```
user@host> show isis statistics
IS-IS statistics for merino:

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Rexmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>12793</td>
<td>12793</td>
<td>0</td>
<td>8666</td>
<td>719</td>
</tr>
<tr>
<td>IIH</td>
<td>116751</td>
<td>116751</td>
<td>0</td>
<td>118834</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>203956</td>
<td>203956</td>
<td>0</td>
<td>204080</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>7356</td>
<td>7350</td>
<td>6</td>
<td>8635</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>340856</td>
<td>340850</td>
<td>6</td>
<td>340215</td>
<td>719</td>
</tr>
</tbody>
</table>

Total packets received: 340856 Sent: 340934

SNP queue length: 0 Drops: 0
LSP queue length: 0 Drops: 0

SPF runs: 1064
Fragments rebuilt: 1087
LSP regenerations: 436
Purges initiated: 0

user@host> clear isis statistics

user@host> show isis statistics
IS-IS statistics for merino:

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Rexmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IIH</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

Total packets received: 5 Sent: 7

SNP queue length: 0 Drops: 0
LSP queue length: 0 Drops: 0

SPF runs: 0
Fragments rebuilt: 0
LSP regenerations: 0
Purges initiated: 0
show isis adjacency

Syntax

show isis adjacency
<system-id>
<brief | detail | extensive>
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)

show isis adjacency
<system-id>
<brief | detail | extensive>
<instance instance-name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Display information about IS-IS neighbors.

Options

none—Display standard information about IS-IS neighbors for all routing instances.

system-id—(Optional) Display information about IS-IS neighbors for the specified intermediate system.

brief | detail | extensive—(Optional) Display standard information about IS-IS neighbors with the specified level of output.

instance instance-name—(Optional) Display information about IS-IS neighbors for the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Display information about IS-IS neighbors for all logical systems or for a particular logical system.

Required Privilege Level

view

Related Documentation

• clear isis adjacency on page 2752

List of Sample Output

show isis adjacency on page 2762
show isis adjacency brief on page 2762
show isis adjacency detail on page 2763
show isis adjacency extensive on page 2763

Output Fields

Table 339 on page 2760 describes the output fields for the show isis adjacency command. Output fields are listed in the approximate order in which they appear.

Table 339: show isis adjacency Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 339: show isis adjacency Output Fields  (*continued*)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System identifier (<strong>sysid</strong>), displayed as a name, if possible.</td>
<td>brief</td>
</tr>
<tr>
<td>L or Level</td>
<td>Level:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3—Level 1 and Level 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An exclamation point (!) preceding the level number indicates that the adjacency is missing an IP address.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>State of the adjacency: <strong>Up, Down, New, One-way, Initializing, or Rejected.</strong></td>
<td>All levels</td>
</tr>
<tr>
<td>Hold (secs)</td>
<td>Remaining hold time of the adjacency.</td>
<td>brief</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address of the next hop).</td>
<td>brief</td>
</tr>
<tr>
<td>Expires in</td>
<td>How long until the adjacency expires, in seconds.</td>
<td>detail</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority to become the designated intermediate system.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Up/Down transitions</td>
<td>Count of adjacency status changes from <strong>Up</strong> to <strong>Down</strong> or from <strong>Down</strong> to <strong>Up</strong></td>
<td>detail</td>
</tr>
<tr>
<td>Last transition</td>
<td>Time of the last <strong>Up/Down</strong> transition.</td>
<td>detail</td>
</tr>
<tr>
<td>Circuit type</td>
<td>Bit mask of levels on this interface: 1=Level 1 router; 2=Level 2 router; 3=both Level 1 and Level 2 router.</td>
<td>detail</td>
</tr>
<tr>
<td>Speaks</td>
<td>Protocols supported by this neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address of the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Topologies</td>
<td>Supported topologies.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Restart capable</td>
<td>Whether a neighbor is capable of graceful restart: <strong>Yes</strong> or <strong>No</strong>.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Adjacency advertisement: Advertise</td>
<td>This routing device has signaled to advertise this interface to its neighbors in their link-state PDUs.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Adjacency advertisement: Suppress</td>
<td>This neighbor has signaled not to advertise the interface in the routing device’s outbound link-state PDUs.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>IP addresses</td>
<td>IP address of this neighbor.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 339: show isis adjacency Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition log</td>
<td>List of recent transitions, including:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• When—Time at which an IS-IS adjacency transition occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—Current state of the IS-IS adjacency (up, down, or rejected).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Up—Adjacency is up and operational.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—Adjacency is down and not available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rejected—Adjacency has been rejected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Event—Type of transition that occurred.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Seenself—Possible routing loop has been detected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface down—IS-IS interface has gone down and is no longer available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Error—Adjacency error.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down reason—Reason that an IS-IS adjacency is down:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3-Way Handshake Failed—Connection establishment failed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Address Mismatch—Address mismatch caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Aged Out—Link expired.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISO Area Mismatch—IS-IS area mismatch caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bad Hello—Unacceptable hello message caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• BFD Session Down—Bidirectional failure detection caused link failure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface Disabled—IS-IS interface is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface Down—IS-IS interface is unavailable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface Level Disabled—IS-IS level is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Level Changed—IS-IS level has changed on the adjacency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Level Mismatch—Levels on adjacency are not compatible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MPLS LSP Down—Label-switched path (LSP) is unavailable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MT Topology Changed—IS-IS topology has changed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MT Topology Mismatch—IS-IS topology is mismatched.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Remote System ID Changed—Adjacency peer system ID changed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Protocol Shutdown—IS-IS protocol is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CLI Command—Adjacency brought down by user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unknown—Unknown.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show isis adjacency

```
user@host> show isis adjacency
Interface     System    L State   Hold (secs)   SNPA
at-2/3/0.0    ranier    3 Up       23            
```

show isis adjacency brief

The output for the `show isis adjacency brief` command is identical to that for the `show isis adjacency` command. For sample output, see `show isis adjacency on page 2762`. 
show isis adjacency detail

user@host> show isis adjacency detail
ranier
  Interface: at-2/3/0.0, Level: 3, State: Up, Expires in 21 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 00:01:09 ago
  Circuit type: 3, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes
  IP addresses: 11.1.1.2

show isis adjacency extensive

user@host> show isis adjacency extensive
ranier
  Interface: at-2/3/0.0, Level: 3, State: Up, Expires in 22 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 00:01:16 ago
  Circuit type: 3, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes
  IP addresses: 11.1.1.2
  Transition log:
<table>
<thead>
<tr>
<th>When</th>
<th>State</th>
<th>Event</th>
<th>Down reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wed Nov 8 21:24:25</td>
<td>Up</td>
<td>Seenself</td>
<td></td>
</tr>
</tbody>
</table>
**show isis authentication**

**Syntax**
```
show isis authentication
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and QFX Series)**
```
show isis authentication
<instance instance-name>
```

**Release Information**
Command introduced in Junos OS Release 7.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Support for hitless authentication key rollover introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Display information about IS-IS authentication.

**Options**
- `none`—Display information about IS-IS authentication.
- `instance instance-name`—(Optional) Display IS-IS authentication for the specified routing instance.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view

**List of Sample Output**
- show isis authentication on page 2765
- show isis authentication (With Hitless Authentication Key Rollover Configured) on page 2765

**Output Fields**
Table 340 on page 2764 describes the output fields for the `show isis authentication` command. Output fields are listed in the approximate order in which they appear.

**Table 340: show isis authentication Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface name.</td>
</tr>
<tr>
<td>Level</td>
<td>IS-IS level.</td>
</tr>
<tr>
<td>IIH Auth</td>
<td>IS-IS Hello (IIH) packet authentication type. Displays the name of the active keychain if hitless authentication key rollover is configured.</td>
</tr>
<tr>
<td>CSN Auth</td>
<td>Complete sequence number authentication type.</td>
</tr>
<tr>
<td>PSN Auth</td>
<td>Partial sequence number authentication type.</td>
</tr>
</tbody>
</table>
Table 340: show isis authentication Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1 LSP Authentication</td>
<td>Layer 1 link-state PDU authentication type.</td>
</tr>
<tr>
<td>L2 LSP Authentication</td>
<td>Layer 2 link-state PDU authentication type.</td>
</tr>
</tbody>
</table>

Sample Output

show isis authentication

```
user@host> show isis authentication
Interface          Level IIH Auth  CSN Auth  PSN Auth
at-2/3/0.0          1     Simple    Simple    Simple
                    2     MD5       MD5       MD5

L1 LSP Authentication: Simple
L2 LSP Authentication: MD5
```

show isis authentication (With Hitless Authentication Key Rollover Configured)

```
user@host> show isis authentication
Interface          Level IIH Auth  CSN Auth  PSN Auth
so-0/1/3.0          2     hakrhello MD5       MD5

L2 LSP Authentication: MD5
```
**show isis backup coverage**

Syntax

```
show isis backup coverage
<instance instance-name>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches and QFX Series)

```
show isis backup coverage
<instance instance-name>
```

Release Information

Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Display information about the level of backup coverage available.

Options

- **none**—Display information about the level of backup coverage available for all the nodes and prefixes in the network.

- **instance instance-name**—(Optional) Display information about the level of backup coverage for a specific IS-IS routing instance.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

View

Related Documentation

- Example: Configuring Link and Node Protection for IS-IS Routes
- show isis backup label-switched-path on page 2768

List of Sample Output

**show isis backup coverage** on page 2767

Output Fields

Table 341 on page 2766 lists the output fields for the **show isis backup coverage** command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>Type of topology or address family: IPv4 Unicast or IPv6 Unicast.</td>
</tr>
<tr>
<td>Level</td>
<td>IS-IS level:</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1</td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2</td>
</tr>
<tr>
<td>Node</td>
<td>By topology, the percentage of all routes configured on the node that are protected through backup coverage.</td>
</tr>
</tbody>
</table>
### Table 341: show isis backup coverage Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>Percentage of IPv4 unicast routes that are protected through backup coverage.</td>
</tr>
<tr>
<td>IPv6</td>
<td>Percentage of IPv6 unicast routes that are protected through backup coverage.</td>
</tr>
<tr>
<td>CLNS</td>
<td>Percentage of Connectionless Network Service (CLNS) routes that are protected through backup coverage.</td>
</tr>
</tbody>
</table>

### Sample Output

**show isis backup coverage**

```
user@host> show isis backup coverage
Backup Coverage:
Topology    Level  Node  IPv4    IPv6    CLNS
IPV4 Unicast 2 28.57%  22.22%   0.00%   0.00%
IPV6 Unicast 2  0.00%   0.00%   0.00%   0.00%
```
**show isis backup label-switched-path**

**Syntax**

```
show isis backup label-switched-path
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and QFX Series)**

```
show isis backup label-switched-path
```

**Release Information**

- Command introduced in Junos OS Release 9.5.
- Command introduced in Junos OS Release 9.5 for EX Series switches.
- Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Display information about MPLS label-switched-paths (LSPs) designated as backup routes for IS-IS routes.

**Options**

- **none**—Display information about MPLS LSPs designated as backup routes for IS-IS routes.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

- **Level**
  - view

**Related Documentation**

- Example: Configuring Link and Node Protection for IS-IS Routes
- `show isis backup coverage` on page 2766

**List of Sample Output**

```
show isis backup label-switched-path on page 2769
```

**Output Fields**

Table 342 on page 2768 lists the output fields for the `show isis backup label-switched-path` command. Output fields are listed in the approximate order in which they appear.

**Table 342: show isis backup label-switched-path Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup MPLS LSPs</td>
<td>List of MPLS LSPs designated as backup paths for IS-IS routes.</td>
</tr>
<tr>
<td>Egress</td>
<td>IP address of the egress routing device for the LSP.</td>
</tr>
<tr>
<td>Status</td>
<td>State of the LSP:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Up</strong>—The routing device can detect RSVP hello messages from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—The routing device has received one of the following indications:</td>
</tr>
<tr>
<td></td>
<td>• Communication failure from the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• Communication from IGP that the neighbor is unavailable.</td>
</tr>
<tr>
<td></td>
<td>• Change in the sequence numbers in the RSVP hello messages sent by the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Deleted</strong>—LSP is no longer available as a backup path.</td>
</tr>
</tbody>
</table>
Table 342: show isis backup label-switched-path Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last change</td>
<td>Time elapsed since the neighbor state changed either from up to down or from down to up. The format is hh:mm:ss.</td>
</tr>
<tr>
<td>TE-metric</td>
<td>Configured traffic engineering metric.</td>
</tr>
<tr>
<td>Metric</td>
<td>Configured metric.</td>
</tr>
</tbody>
</table>

Sample Output

show isis backup label-switched-path

user@host> show isis backup label-switched-path
Backup MPLS LSPs:
  f-to-g, Egress: 192.168.1.4, Status: up, Last change: 06:12:03
    TE-metric: 9, Metric: 0
**show isis backup spf results**

**Syntax**

```
show isis backup spf results
<instance instance-name>
<level (1 | 2)>
<logical-system (all | logical-system-name)>
<no-coverage>
<topology (ipv4-unicast | ipv6-multicast | ipv6-unicast | unicast)>
```

**Syntax (EX Series Switches)**

```
show isis backup spf results
<instance instance-name>
<level (1 | 2)>
<no-coverage>
<topology (ipv4-unicast | unicast)>
```

**Release Information**

Command introduced in Junos OS Release 9.5.

**Description**

Display information about IS-IS shortest-path-first (SPF) calculations for backup paths.

**Options**

- `none`—Display information about IS-IS SPF calculations for all backup paths for all destination nodes.
- `instance instance-name`—(Optional) Display SPF calculations for backup paths for the specified routing instance.
- `level (1 | 2)`—(Optional) Display SPF calculations for the backup paths for the specified IS-IS level.
- `logical-system logical-system-name`—(Optional) Display SPF calculations for the backup paths for all logical systems or on a particular logical system.
- `no-coverage`—(Optional) Display SPF calculations only for destinations that do not have backup coverage.
- `topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)`—(Optional) Display SPF calculations for backup paths for the specified topology only.

**Required Privilege**

- **Level**
  - `view`

**Related Documentation**

- *Example: Configuring Link and Node Protection for IS-IS Routes*
- `show isis backup coverage on page 2766`

**List of Sample Output**

- `show isis backup spf results on page 2771`
- `show isis backup spf results no-coverage on page 2772`

**Output Fields**

Table 343 on page 2771 lists the output fields for the `show isis backup spf results` command. Output fields are listed in the approximate order in which they appear.
Table 343: show isis backup spf results Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node-name</td>
<td>Name of the destination node.</td>
</tr>
<tr>
<td>Address</td>
<td>Address of the destination node.</td>
</tr>
<tr>
<td>Primary next-hop</td>
<td>Interface and name of the node of the primary next hop to reach the destination.</td>
</tr>
<tr>
<td>Root</td>
<td>Name of the next-hop neighbor.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric to the node.</td>
</tr>
<tr>
<td>Eligible</td>
<td>Indicates that the next-hop neighbor has been designated as a backup path to the destination node.</td>
</tr>
<tr>
<td>Backup next-hop</td>
<td>Name of the interface of the backup next hop.</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address of the next hop).</td>
</tr>
<tr>
<td>LSP</td>
<td>Name of the MPLS label-switched path (LSP) designated as a backup path.</td>
</tr>
<tr>
<td>Not eligible</td>
<td>Indicates that the next-hop neighbor cannot function as a backup path to the destination.</td>
</tr>
<tr>
<td>Reason</td>
<td>Describes why the next-hop neighbor is designated as Not eligible as a backup path.</td>
</tr>
</tbody>
</table>

Sample Output

show isis backup spf results

user@host> show isis backup spf results
IS-IS level 1 SPF results:
pro-bng3-k.00
  Primary next-hop: fe-1/3/3.0, IPV4, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
  Primary next-hop: fe-1/3/3.0, IPV6, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
    Root: pro-bng3-k, Root Metric: 10, Metric: 0, Root Preference: 0x0
    Not eligible, IPV4, Reason: Primary next-hop link fate sharing
    Not eligible, IPV6, Reason: Primary next-hop link fate sharing
  Root: pro-bng3-i, Root Metric: 10, Metric: 20, Root Preference: 0x0
    track-item: pro-bng3-k.00-00
    track-item: pro-bng3-j.00-00
    Not eligible, IPV4, Reason: Path loops
    Not eligible, IPV6, Reason: Path loops
pro-bng3-i.00
  Primary next-hop: fe-0/1/2.0, IPV4, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
  Primary next-hop: fe-0/1/2.0, IPV6, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
    Root: pro-bng3-i, Root Metric: 10, Metric: 0, Root Preference: 0x0
    Not eligible, IPV4, Reason: Primary next-hop link fate sharing
    Not eligible, IPV6, Reason: Primary next-hop link fate sharing
    Root: pro-bng3-k, Root Metric: 10, Metric: 20, Root Preference: 0x0
track-item: pro-bng3-j.00-00
track-item: pro-bng3-i.00-00
Not eligible, IPV4, Reason: Path loops
Not eligible, IPV6, Reason: Path loops

2 nodes

IS-IS level 2 SPF results:
pro-bng3-k.00
Primary next-hop: fe-1/3/3.0, IPV4, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
Primary next-hop: fe-1/3/3.0, IPV6, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
Root: pro-bng3-k, Root Metric: 10, Metric: 0, Root Preference: 0x0
Not eligible, IPV4, Reason: Primary next-hop link fate sharing
Not eligible, IPV6, Reason: Primary next-hop link fate sharing
Root: pro-bng3-i, Root Metric: 10, Metric: 20, Root Preference: 0x0
track-item: pro-bng3-k.00-00
track-item: pro-bng3-j.00-00
Not eligible, IPV4, Reason: Path loops
Not eligible, IPV6, Reason: Path loops

pro-bng3-i.00
Primary next-hop: fe-0/1/2.0, IPV4, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
Primary next-hop: fe-0/1/2.0, IPV6, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
Root: pro-bng3-i, Root Metric: 10, Metric: 0, Root Preference: 0x0
Not eligible, IPV4, Reason: Primary next-hop link fate sharing
Not eligible, IPV6, Reason: Primary next-hop link fate sharing
Root: pro-bng3-k, Root Metric: 10, Metric: 20, Root Preference: 0x0
track-item: pro-bng3-j.00-00
track-item: pro-bng3-i.00-00
Not eligible, IPV4, Reason: Path loops
Not eligible, IPV6, Reason: Path loops

2 nodes

show isis backup spf results no-coverage

user@host> show isis backup spf results no-coverage

IS-IS level 1 SPF results:
pro-bng3-k.00
Primary next-hop: fe-1/3/3.0, IPV4, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
Primary next-hop: fe-1/3/3.0, IPV6, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
Root: pro-bng3-k, Root Metric: 10, Metric: 0, Root Preference: 0x0
Root: pro-bng3-i, Root Metric: 10, Metric: 20, Root Preference: 0x0
track-item: pro-bng3-k.00-00
track-item: pro-bng3-j.00-00

pro-bng3-i.00
Primary next-hop: fe-0/1/2.0, IPV4, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
Primary next-hop: fe-0/1/2.0, IPV6, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
Root: pro-bng3-i, Root Metric: 10, Metric: 0, Root Preference: 0x0
Root: pro-bng3-k, Root Metric: 10, Metric: 20, Root Preference: 0x0
track-item: pro-bng3-j.00-00
track-item: pro-bng3-i.00-00

2 nodes

IS-IS level 2 SPF results:
pro-bng3-k.00
Primary next-hop: fe-1/3/3.0, IPV4, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
Primary next-hop: fe-1/3/3.0, IPV6, pro-bng3-k, SNPA: b0:c6:9a:2c:f0:de
Root: pro-bng3-k, Root Metric: 10, Metric: 0, Root Preference: 0x0
Root: pro-bng3-i, Root Metric: 10, Metric: 20, Root Preference: 0x0
track-item: pro-bng3-k.00-00
track-item: pro-bng3-j.00-00

pro-bng3-i.00
Primary next-hop: fe-0/1/2.0, IPV4, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
Primary next-hop: fe-0/1/2.0, IPV6, pro-bng3-i, SNPA: b0:c6:9a:2a:f4:21
   Root: pro-bng3-i, Root Metric: 10, Metric: 0, Root Preference: 0x0
   Root: pro-bng3-k, Root Metric: 10, Metric: 20, Root Preference: 0x0
       track-item: pro-bng3-j.00-00
       track-item: pro-bng3-i.00-00
2 nodes
show isis database

**Syntax**
```plaintext
show isis database
<system-id>
<brief | detail | extensive>
<instance instance-name>
<level (1 | 2)>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and QFX Series)**
```plaintext
show isis database
<system-id>
<brief | detail | extensive>
<level (1 | 2)>
<instance instance-name>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Display the entries in the IS-IS link-state database, which contains data about PDU packets.

**Options**
- **none**—Display standard information about IS-IS link-state database entries for all routing instances.
- **system id**—(Optional) Display IS-IS link-state database entries for the specified intermediate system.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **instance instance-name**—(Optional) Display IS-IS link-state database entries for the specified routing instance.
- **level (1 | 2)**—(Optional) Display IS-IS link-state database entries for the specified IS-IS level.
- **logical-system (all | logical-system-name)**—(Optional) Display standard information about IS-IS link-state database entries for all logical systems or for a particular logical system.

**Required Privilege Level**
- view

**Related Documentation**
- clear isis database on page 2754

**List of Sample Output**
- show isis database on page 2776
- show isis database brief on page 2777
- show isis database detail on page 2777
- show isis database extensive on page 2777
Output Fields

Table 344 on page 2775 describes the output fields for the `show isis database` command. Output fields are listed in the approximate order in which they appear. Fields that contain internal IS-IS information useful only in troubleshooting obscure problems are not described in the table. For more details about these fields, contact your customer support representative.

**Table 344: show isis database Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Name of the interface on which the link-state PDU has been received; always IS-IS for this command.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
| level         | Level of intermediate system:  
• 1—Intermediate system routes within an area; when the destination is outside an area, it routes toward a Level 2 system.  
• 2—Intermediate system routes between areas and toward other ASs. | All levels      |
| LSP ID        | Link-state PDU identifier.                                                        | All levels      |
| Sequence      | Sequence number of the link-state PDU.                                            | All levels      |
| Checksum      | Checksum value of the link-state PDU.                                             | All levels      |
| Lifetime (secs) | Remaining lifetime of the link-state PDU, in seconds.                           | All levels      |
| Attributes    | Attributes of the specified database: L1, L2, Overload, or Attached (L1 only).    | none brief      |
| # LSPs        | Total number of link-state PDUs in the specified link-state database.            | none brief      |
| IP prefix     | Prefix advertised by this link-state PDU.                                         | detail extensive|
| IS neighbor   | IS-IS neighbor of the advertising system.                                         | detail extensive|
| ES neighbor   | (J Series routers only) An ES-IS neighbor of the advertising system.              | detail extensive|
| IP prefix     | IPv4 prefix advertised by this link-state PDU.                                    | detail extensive|
| V6 prefix     | IPv6 prefix advertised by this link-state PDU.                                    | detail extensive|
| Metric        | Metric of the prefix or neighbor.                                                | detail extensive|
| Header        |  
• LSP ID—Link state PDU identifier of the header.  
• Length—Header length.  
• Allocated Length—Amount of length available for the header.  
• Router ID—Address of the local routing device.  
• Remaining Lifetime—Remaining lifetime of the link-state PDU, in seconds. | extensive        |
Table 344: show isis database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet</td>
<td>• LSP ID—The identifier for the link-state PDU.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Length—Packet length.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lifetime—Remaining lifetime, in seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Checksum—The checksum of the link-state PDU.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sequence—The sequence number of the link-state PDU. Every time the link-state</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDU is updated, this number increments.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Attributes—Packet attributes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• NLPID—Network layer protocol identifier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fixed length—Specifies the set length for the packet.</td>
<td></td>
</tr>
</tbody>
</table>

| TLVs       | • Area Address—Area addresses that the routing device can reach.                  | extensive       |
|            | • Speaks—Supported routing protocols.                                             |                 |
|            | • IP router id—ID of the routing device (usually the IP address).                 |                 |
|            | • IP address—IPv4 address.                                                        |                 |
|            | • Hostname—Assigned name of the routing device.                                   |                 |
|            | • IP prefix—IP prefix of the routing device.                                       |                 |
|            | • Metric—IS-IS metric that measures the cost of the adjacency between the         |                 |
|            |   originating routing device and the advertised routing device.                   |                 |
|            | • IP extended prefix—Extended IP prefix of the routing device.                    |                 |
|            | • IS neighbor—Directly attached neighbor’s name and metric.                       |                 |
|            | • IS extended neighbor—Directly attached neighbor’s name, metric, and IP address. |                 |

Sample Output

show isis database

```plaintext
user@host> show isis database
IS-IS level 1 link-state database:
LSP ID                      Sequence Checksum Lifetime Attributes
kobuk.00-00                      0x3   0x3167     1057 L1 L2
camaro.00-00                     0x5   0x770e     1091 L1 L2
ranier.00-00                     0x4   0xaa95     1091 L1 L2
glacier.00-00                    0x4   0x206f     1089 L1 L2
glacier.02-00                    0x1   0xd141     1089 L1 L2
badlands.00-00                   0x3   0x87a2     1093 L1 L2
  6 LSPs

IS-IS level 2 link-state database:
LSP ID                      Sequence Checksum Lifetime Attributes
kobuk.00-00                      0x6   0x8d6b     1096 L1 L2
camaro.00-00                     0x9   0x877b     1101 L1 L2
ranier.00-00                     0x8   0x855d     1103 L1 L2
glacier.00-00                    0x7   0xf892     1098 L1 L2
glacier.02-00                    0x1   0xd141     1089 L1 L2
badlands.00-00                   0x6   0x562      1105 L1 L2
  6 LSPs
```

Copyright © 2013, Juniper Networks, Inc.
**show isis database brief**

The output for the `show isis database brief` command is identical to that for the `show isis database` command. For sample output, see `show isis database on page 2776`.

**show isis database detail**

```
user@host> show isis database logical-system CE3 sisira.00-00 detail

IS-IS level 1 link-state database:

sisira.00-00 Sequence: 0x11, Checksum: 0x10fc, Lifetime: 975 secs
  IS neighbor: hemantha-CE3.02          Metric:       10
  ES neighbor: 0015.0015.0015           Metric:       10 Down
  ES neighbor: 0025.0025.0025           Metric:       10 Down
  ES neighbor: 0030.0030.0030           Metric:       10 Down
  ES neighbor: 0040.0040.0040           Metric:       10 Down
  ES neighbor: sisira                    Metric:        0
  IP prefix: 1.0.0.0/24                 Metric:       10 External Down
  IP prefix: 3.0.0.0/24                 Metric:       10 External Down
  IP prefix: 4.0.0.0/24                 Metric:       10 External Down
  IP prefix: 5.0.0.0/24                 Metric:       10 Internal Up
  IP prefix: 15.15.15.15/32             Metric:       10 External Down
  IP prefix: 25.25.25.25/32             Metric:       10 External Down
  IP prefix: 30.30.30.30/32             Metric:       10 External Down
  IP prefix: 40.40.40.40/32             Metric:       10 External Down
  IP prefix: 60.60.60.60/32             Metric:        0 Internal Up

IS-IS level 2 link-state database:

sisira.00-00 Sequence: 0x13, Checksum: 0x69ac, Lifetime: 993 secs
  IS neighbor: hemantha-CE3.02          Metric:       10
  IP prefix: 1.0.0.0/24                 Metric:       10 External Down
  IP prefix: 3.0.0.0/24                 Metric:       10 External Down
  IP prefix: 4.0.0.0/24                 Metric:       10 External Down
  IP prefix: 5.0.0.0/24                 Metric:       10 Internal Up
  IP prefix: 15.15.15.15/32             Metric:       10 External Down
  IP prefix: 25.25.25.25/32             Metric:       10 External Down
  IP prefix: 30.30.30.30/32             Metric:       10 External Down
  IP prefix: 40.40.40.40/32             Metric:       10 External Down
  IP prefix: 50.50.50.50/32             Metric:       10 Internal Up
  IP prefix: 60.60.60.60/32             Metric:        0 Internal Up
  ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0015.0015.0015/152
    Metric:       10 External Down
  ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0025.0025.0025/152
    Metric:       10 External Down
  ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0030.0030.0030/152
    Metric:       10 External Down
  ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0040.0040.0040/152
    Metric:       10 External Down
  ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0060.0060.0060/152
    Metric:        0 Internal Up
```

**show isis database extensive**

```
user@host> show isis database logical-system CE3 sisira.00-00 extensive

IS-IS level 1 link-state database:

sisira.00-00 Sequence: 0x11, Checksum: 0x10fc, Lifetime: 970 secs
```
<table>
<thead>
<tr>
<th>IS neighbor: hemantha-CE3.02</th>
<th>Metric: 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-way fragment: hemantha-CE3.02-00, Two-way first fragment: hemantha-CE3.02-00</td>
<td></td>
</tr>
<tr>
<td>ES neighbor: 0015.0015.0015</td>
<td>Metric: 10 Down</td>
</tr>
<tr>
<td>ES neighbor: 0025.0025.0025</td>
<td>Metric: 10 Down</td>
</tr>
<tr>
<td>ES neighbor: 0030.0030.0030</td>
<td>Metric: 10 Down</td>
</tr>
<tr>
<td>ES neighbor: 0040.0040.0040</td>
<td>Metric: 10 Down</td>
</tr>
<tr>
<td>ES neighbor: sisira</td>
<td>Metric: 0</td>
</tr>
<tr>
<td>IP prefix: 1.0.0.0/24</td>
<td>Metric: 10 External Down</td>
</tr>
<tr>
<td>IP prefix: 3.0.0.0/24</td>
<td>Metric: 10 External Down</td>
</tr>
<tr>
<td>IP prefix: 4.0.0.0/24</td>
<td>Metric: 10 External Down</td>
</tr>
<tr>
<td>IP prefix: 5.0.0.0/24</td>
<td>Metric: 10 Internal Up</td>
</tr>
<tr>
<td>IP prefix: 15.15.15.15/32</td>
<td>Metric: 10 External Down</td>
</tr>
<tr>
<td>IP prefix: 25.25.25.25/32</td>
<td>Metric: 10 External Down</td>
</tr>
<tr>
<td>IP prefix: 30.30.30.30/32</td>
<td>Metric: 10 External Down</td>
</tr>
<tr>
<td>IP prefix: 40.40.40.40/32</td>
<td>Metric: 10 External Down</td>
</tr>
<tr>
<td>IP prefix: 60.60.60.60/32</td>
<td>Metric: 0 Internal Up</td>
</tr>
</tbody>
</table>

Header: LSP ID: sisira.00-00, Length: 336 bytes
Allocated length: 336 bytes, Router ID: 0.0.0.0
Remaining lifetime: 970 secs, Level: 1, Interface: 333
Estimated free bytes: 144, Actual free bytes: 0
Aging timer expires in: 970 secs
Protocols: IP, IPv6, CLNS

Packet: LSP ID: sisira.00-00, Length: 336 bytes, Lifetime : 1198 secs
Checksum: 0x10fc, Sequence: 0x11, Attributes: 0xb L1 L2 Attached
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 18, Packet version: 1, Max area: 0

TLVs:
Area address: 60.0006.80ff.f800.0000.0108.0001 (13)
Speaks: IP
Speaks: IPv6
Speaks: CLNP
Hostname: sisira
ES neighbor TLV: Internal, Metric: default 0, Up
ES: sisira
IS neighbor: hemantha-CE3.02, Internal, Metric: default 10
IS neighbor: hemantha-CE3.02, Metric: default 10
ES neighbor TLV: External, Metric: default 10, Down
ES: 0040.0040.0040
ES neighbor TLV: External, Metric: default 10, Down
ES: 0025.0025.0025
ES neighbor TLV: External, Metric: default 10, Down
ES: 0015.0015.0015
ES neighbor TLV: External, Metric: default 10, Down
ES: 0030.0030.0030
IP external prefix: 3.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 4.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 15.15.15.15/32, Internal, Metric: default 10, Down
IP external prefix: 25.25.25.25/32, Internal, Metric: default 10, Down
IP external prefix: 30.30.30.30/32, Internal, Metric: default 10, Down
IP external prefix: 40.40.40.40/32 metric 10 down
IP extended prefix: 3.0.0.0/24 metric 10 down
IP extended prefix: 4.0.0.0/24 metric 10 down
IP extended prefix: 15.15.15.15/32 metric 10 down
IP extended prefix: 25.25.25.25 metric 10 down
IP extended prefix: 30.30.30.30 metric 10 down
IP extended prefix: 40.40.40.40 metric 10 down
IP extended prefix: 15.15.15.15/32 metric 10 down
IP extended prefix: 25.25.25.25 metric 10 down
IP extended prefix: 30.30.30.30/32 metric 10 down
IP prefix: 60.60.60.60/32, Internal, Metric: default 0, Up
IP prefix: 5.0.0.0/24, Internal, Metric: default 10, Up
IP extended prefix: 60.60.60.60/32 metric 0 up
IP extended prefix: 5.0.0.0/24 metric 10 up
No queued transmissions

IS-IS level 2 link-state database:

sisira.00-00 Sequence: 0x13, Checksum: 0x69ac, Lifetime: 988 secs
IS neighbor: hemantha-CE3.02 Metric: 10
Two-way fragment: hemantha-CE3.02-00, Two-way first fragment:
hemantha-CE3.02-00

IP prefix: 1.0.0.0/24 Metric: 10 External Down
IP prefix: 3.0.0.0/24 Metric: 10 External Down
IP prefix: 4.0.0.0/24 Metric: 10 External Down
IP prefix: 5.0.0.0/24 Metric: 10 Internal Up
IP prefix: 15.15.15.15/32 Metric: 10 External Down
IP prefix: 25.25.25.25/32 Metric: 10 External Down
IP prefix: 30.30.30.30/32 Metric: 10 External Down
IP prefix: 40.40.40.40/32 Metric: 10 External Down
IP prefix: 50.50.50.50/32 Metric: 10 Internal Up
IP prefix: 60.60.60.60/32 Metric: 0 Internal Up
ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0015.0015.0015/152 Metric: 10 External Down
ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0025.0025.0025/152 Metric: 10 External Down
ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0030.0030.0030/152 Metric: 10 External Down
ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0040.0040.0040/152 Metric: 10 External Down
ISO prefix: 60.0006.80ff.f800.0000.0108.0001.0060.0060.0060/152 Metric: 0 Internal Up

Header: LSP ID: sisira.00-00, Length: 427 bytes
Allocated length: 427 bytes, Router ID: 0.0.0.0
Remaining lifetime: 988 secs, Level: 2, Interface: 333
Estimated free bytes: 130, Actual free bytes: 0
Aging timer expires in: 988 secs
Protocols: IP, IPv6, CLNS

Packet: LSP ID: sisira.00-00, Length: 427 bytes, Lifetime: 1198 secs
Checksum: 0x69ac, Sequence: 0x13, Attributes: 0x3 L1 L2
NLPID: 0x83, Fixed length: 27 bytes, Version: 1, Sysid length: 0 bytes
Packet type: 20, Packet version: 1, Max area: 0

TLVs:
Area address: 60.0006.80ff.f800.0000.0108.0001 (13)
Speaks: IP
Speaks: IPV6
Speaks: CLNP
Hostname: sisira
IS neighbor: hemantha-CE3.02, Internal, Metric: default 10
IS extended neighbor: hemantha-CE3.02, Metric: default 10
IP external prefix: 3.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 4.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 15.15.15.15/32, Internal, Metric: default 10, Down
IP external prefix: 25.25.25.25/32, Internal, Metric: default 10, Down
IP external prefix: 1.0.0.0/24, Internal, Metric: default 10, Down
IP external prefix: 30.30.30.30/32, Internal, Metric: default 10, Down
IP extended prefix: 3.0.0.0/24 metric 10 down
IP extended prefix: 4.0.0.0/24 metric 10 down
IP extended prefix: 25.25.25.25/32 metric 10 down
IP extended prefix: 15.15.15.15/32 metric 10 down
IP extended prefix: 1.0.0.0/24 metric 10 down
IP extended prefix: 30.30.30.30/32 metric 10 down
ISO prefix-neighbor TLV: Internal, Metric: default 0, Up
  Prefix : 60.0006.80ff.f800.0000.0108.0001.0060.0060.0060/152
ISO prefix-neighbor TLV: External, Metric: default 10, Down
  Prefix : 60.0006.80ff.f800.0000.0108.0001.0040.0040.0040/152
ISO prefix-neighbor TLV: External, Metric: default 10, Down
  Prefix : 60.0006.80ff.f800.0000.0108.0001.0025.0025.0025/152
ISO prefix-neighbor TLV: External, Metric: default 10, Down
  Prefix : 60.0006.80ff.f800.0000.0108.0001.0015.0015.0015/152
ISO prefix-neighbor TLV: External, Metric: default 10, Down
  Prefix : 60.0006.80ff.f800.0000.0108.0001.0030.0030.0030/152
IP prefix: 60.60.60.60/32, Internal, Metric: default 0, Up
IP prefix: 5.0.0.0/24, Internal, Metric: default 10, Up
IP prefix: 50.50.50.50/32, Internal, Metric: default 10, Up
IP extended prefix: 60.60.60.60/32 metric 0 up
IP extended prefix: 5.0.0.0/24 metric 10 up
IP extended prefix: 50.50.50.50/32 metric 10 up
No queued transmissions
show isis hostname

**Syntax**

show isis hostname
<logical-system (all | logical-system-name)>

**Syntax (EX Series Switches and QFX Series)**

show isis hostname

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Display IS-IS hostname database information.

**Options**

- **none**—Display IS-IS hostname database information.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

- **Level**
- **view**

**List of Sample Output**

*show isis hostname on page 2781*

**Output Fields**

Table 345 on page 2781 describes the output fields for the `show isis hostname` command. Output fields are listed in the approximate order in which they appear.

**Table 345: show isis hostname Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System id</td>
<td>System identifier mapped to the hostname.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname mapped to the system identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of mapping between system identifier and hostname.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Dynamic</strong>—Hostname mapping determined as described in RFC 2763, <em>Dynamic Hostname Exchange Mechanism for IS-IS</em>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Static</strong>—Hostname mapping configured by user.</td>
</tr>
</tbody>
</table>

**Sample Output**

*show isis hostname*

```
user@host> show isis hostname
IS-IS hostname database:  
System Id          Hostname   Type
1921.6800.4201    isis1      Dynamic
1921.6800.4202    isis2      Static
1921.6800.4203    isis3      Dynamic
```
show isis interface

Syntax

show isis interface
<brief | detail | extensive>
@interface-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)

show isis interface
<brief | detail | extensive>
@interface-name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Display status information about IS-IS-enabled interfaces.

NOTE: If the configured metric for an IS-IS level is above 63, and the wide-metrics-only statement is not configured, the show isis interface detail command and the show isis interface extensive command display 63 as the metric value for that level. Configure the wide-metrics-only statement to generate metric values greater than 63 on a per IS-IS level basis.

The show isis interface command displays the configured metric value for an IS-IS level irrespective of whether is configured or not.

Options

none—Display standard information about all IS-IS-enabled interfaces.

brief | detail | extensive—(Optional) Display the specified level of output.

@interface-name—(Optional) Display information about the specified interface only.

loglogical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

Related Documentation

• Example: Enabling Wide IS-IS Metrics for Traffic Engineering

List of Sample Output

show isis interface on page 2784
show isis interface brief on page 2784
show isis interface detail on page 2785
show isis interface extensive on page 2785
show isis interface extensive (With LDP) on page 2785

Output Fields

Table 346 on page 2783 describes the output fields for the show isis interface command. Output fields are listed in the approximate order in which they appear.
**Table 346: show isis interface Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>Name of the interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Designated router</td>
<td>Routing device selected by other routers that is responsible for sending link-state</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>advertisements that describe the network. Used only on broadcast networks.</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>Interface index assigned by the Junos OS kernel.</td>
<td>detail</td>
</tr>
<tr>
<td>State</td>
<td>Internal implementation information.</td>
<td>detail</td>
</tr>
<tr>
<td>Circuit id</td>
<td>Circuit identifier.</td>
<td>detail</td>
</tr>
<tr>
<td>Circuit type</td>
<td>Circuit type:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3—Level 1 and Level 2</td>
<td></td>
</tr>
<tr>
<td>LSP interval</td>
<td>Interval between link-state PDUs sent from the interface.</td>
<td>detail</td>
</tr>
<tr>
<td>CSNP interval</td>
<td>Interval between complete sequence number PDUs sent from the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Sysid</td>
<td>System identifier.</td>
<td>detail</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the adjacency is made.</td>
<td>none brief</td>
</tr>
<tr>
<td>Lor Level</td>
<td>Level:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2 only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3—Level 1 and Level 2</td>
<td></td>
</tr>
<tr>
<td>CirID</td>
<td>Circuit identifier.</td>
<td>none brief</td>
</tr>
<tr>
<td>Level 1 DR</td>
<td>Level 1 designated intermediate system.</td>
<td>none brief</td>
</tr>
<tr>
<td>Level 2 DR</td>
<td>Level 2 designated intermediate system.</td>
<td>none brief</td>
</tr>
<tr>
<td>L1/L2 Metric</td>
<td>Interface's metric for Level 1 and Level 2. If there is no information, the metric</td>
<td>none brief</td>
</tr>
<tr>
<td></td>
<td>is 0.</td>
<td></td>
</tr>
<tr>
<td>Adjacency</td>
<td>This routing device has signaled to advertise this interface to its neighbors in</td>
<td>detail extensive</td>
</tr>
<tr>
<td>advertisement:</td>
<td>their label-switched paths (LSPs).</td>
<td></td>
</tr>
<tr>
<td>Advertise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjacency</td>
<td>This neighbor has signaled not to advertise this interface in the routing device's</td>
<td>detail extensive</td>
</tr>
<tr>
<td>advertisement:</td>
<td>outbound LSPs.</td>
<td></td>
</tr>
<tr>
<td>Suppress</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjacencies</td>
<td>Number of adjacencies established on this interface.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 346: show isis interface Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Priority value for this interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric value for this interface.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello(s) / Hello Interval</td>
<td>Interface’s hello interval.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Hold(s) / Hold Time</td>
<td>Interface’s hold time.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Designated Router</td>
<td>Router responsible for sending network link-state advertisements, which describe all the routing devices attached to the network.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello padding</td>
<td>Type of hello padding:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Adaptive—On point-to-point connections, the hello packets are padded from the initial detection of a new neighbor until the neighbor verifies the adjacency as Up in the adjacency state TLV. If the neighbor does not support the adjacency state TLV, then padding continues. On LAN connections, padding starts from the initial detection of a new neighbor until there is at least one active adjacency on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Loose—(Default) The hello packet is padded from the initial detection of a new neighbor until the adjacency transitions to the Up state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strict—Padding is performed on all interface types and for all adjacency states, and is continuous.</td>
<td></td>
</tr>
<tr>
<td>LDP sync state</td>
<td>Current LDP synchronization state: in sync, in holddown, or not supported.</td>
<td>extensive</td>
</tr>
<tr>
<td>reason</td>
<td>Reason for being in the LDP sync state.</td>
<td>extensive</td>
</tr>
<tr>
<td>config holdtime</td>
<td>Configured value of the hold timer.</td>
<td>extensive</td>
</tr>
<tr>
<td>remaining</td>
<td>If the state is not in sync and the hold time is not infinity, then this field displays the remaining hold time in seconds.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

show isis interface

```bash
user@host> show isis interface
IS-IS interface database:
<table>
<thead>
<tr>
<th>Interface</th>
<th>L CirID</th>
<th>Level 1 DR</th>
<th>Level 2 DR</th>
<th>L1/L2 Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-2/3/0.0</td>
<td>3</td>
<td>0x1 Point to Point</td>
<td>Point to Point</td>
<td>10/10</td>
</tr>
<tr>
<td>lo0.0</td>
<td>0</td>
<td>0x1 Passive</td>
<td>Passive</td>
<td>0/0</td>
</tr>
</tbody>
</table>
```

show isis interface brief

The output for the show isis interface brief command is identical to that for the show isis interface command. For sample output, see show isis interface on page 2784.
show isis interface detail

user@host> show isis interface detail
IS-IS interface database:
at-2/3/0.0
  Index: 66, State: 0x6, Circuit id: 0x1, Circuit type: 3
  LSP interval: 100 ms, CSNP interval: 5 s
  Level Adjacencies Priority Metric Hello (s) Hold (s) Designated Router
   1       1       64     10     9.000       27
   2       1       64     10     9.000       27
lo0.0
  Index: 64, State: 0x6, Circuit id: 0x1, Circuit type: 0
  LSP interval: 100 ms, CSNP interval: disabled
  Level Adjacencies Priority Metric Hello (s) Hold (s) Designated Router
   1      0       64      0 Passive
   2      0       64      0 Passive

show isis interface extensive

user@host> show isis interface extensive
IS-IS interface database:
at-2/3/0.0
  Index: 66, State: 0x6, Circuit id: 0x1, Circuit type: 3
  LSP interval: 100 ms, CSNP interval: 5 s, Loose Hello padding
  Level 1
    Adjacencies: 1, Priority: 64, Metric: 10
    Hello Interval: 9.000 s, Hold Time: 27 s
  Level 2
    Adjacencies: 1, Priority: 64, Metric: 10
    Hello Interval: 9.000 s, Hold Time: 27 s
lo0.0
  Index: 64, State: 0x6, Circuit id: 0x1, Circuit type: 0
  LSP interval: 100 ms, CSNP interval: disabled, Loose Hello padding
  Level 1
    Adjacencies: 0, Priority: 64, Metric: 0
    Passive
  Level 2
    Adjacencies: 0, Priority: 64, Metric: 0
    Passive

show isis interface extensive (With LDP)

user@host> show isis interface extensive
IS-IS interface database:
so-1/1/2.0
  Index: 114, State: 0x6, Circuit id: 0x1, Circuit type: 2
  LSP interval: 100 ms, CSNP interval: 20 s, Loose Hello padding
  Adjacency advertisement: Advertise
  LDP sync state: in sync, for: 00:01:28, reason: LDP up during config
  config holdtime: 20 seconds
  Level 2
    Adjacencies: 1, Priority: 64, Metric: 11
    Hello Interval: 9.000 s, Hold Time: 27 s
    IPV4 MulticastMetric: 10
    IPV6 UnicastMetric: 10
show isis overview

Syntax

show isis overview
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)

show isis overview
<instance instance-name>

Release Information

Command introduced in Junos OS Release 8.5.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Display IS-IS overview information.

Options

none—Display standard overview information about IS-IS for all routing instances.
instance instance-name—(Optional) Display overview information for the specified routing instance.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

List of Sample Output

show isis overview on page 2788

Output Fields

Table 347 on page 2786 lists the output fields for the show isis overview command. Output fields are listed in the approximate order in which they appear.

Table 347: show isis overview Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>IS-IS routing instance.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Router ID of the routing device.</td>
</tr>
<tr>
<td>Adjacency holddown</td>
<td>Adjacency holddown capability: enabled or disabled.</td>
</tr>
<tr>
<td>Maximum Areas</td>
<td>Maximum number of IS-IS areas advertised by the routing device.</td>
</tr>
<tr>
<td>LSP life time</td>
<td>Lifetime of the link-state PDU, in seconds.</td>
</tr>
<tr>
<td>Attached bit evaluation</td>
<td>Attached bit capability: enabled or disabled.</td>
</tr>
<tr>
<td>SPF delay</td>
<td>Delay before performing consecutive shortest-path-first (SPF) calculations.</td>
</tr>
<tr>
<td>SPF holddown</td>
<td>Delay before performing additional SPF calculations after the maximum number of consecutive SPF calculations is reached.</td>
</tr>
</tbody>
</table>
### Table 347: show isis overview Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF rapid runs</td>
<td>Maximum number of SPF calculations that can be performed in succession before the holddown timer begins.</td>
</tr>
<tr>
<td>Overload bit at startup</td>
<td>Overload bit capability is enabled.</td>
</tr>
<tr>
<td>is set</td>
<td></td>
</tr>
<tr>
<td>Overload high metrics</td>
<td>Overload high metrics capability: enabled or disabled.</td>
</tr>
<tr>
<td>Overload timeout</td>
<td>Time period after which overload is reset and the time that remains before the timer is set to expire.</td>
</tr>
<tr>
<td>Traffic engineering</td>
<td>Traffic engineering capability: enabled or disabled.</td>
</tr>
<tr>
<td>Restart</td>
<td>Graceful restart capability: enabled or disabled.</td>
</tr>
<tr>
<td>Restart duration</td>
<td>Time period for complete reacquisition of IS-IS neighbors.</td>
</tr>
<tr>
<td>Helper mode</td>
<td>Graceful restart helper capability: enabled or disabled.</td>
</tr>
<tr>
<td>Level</td>
<td>IS-IS level:</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1 information</td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2 information</td>
</tr>
<tr>
<td>IPv4 is enabled</td>
<td>IP Protocol version 4 capability is enabled.</td>
</tr>
<tr>
<td>IPv6 is enabled</td>
<td>IP Protocol version 6 capability is enabled.</td>
</tr>
<tr>
<td>CLNS is enabled</td>
<td>(J Series routers only) OSI CLNP capability is enabled.</td>
</tr>
<tr>
<td>Internal route</td>
<td>Preference value of internal routes.</td>
</tr>
<tr>
<td>preference</td>
<td></td>
</tr>
<tr>
<td>External route</td>
<td>Preference value of external routes.</td>
</tr>
<tr>
<td>preference</td>
<td></td>
</tr>
<tr>
<td>Prefix export limit</td>
<td>Number of prefixes allowed to be exported, as configured by the prefix-export-limit statement.</td>
</tr>
<tr>
<td>Prefix export count</td>
<td>Number of prefixes exported.</td>
</tr>
<tr>
<td>Wide area metrics are</td>
<td>Wide area metrics capability is enabled.</td>
</tr>
<tr>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>Narrow metrics are</td>
<td>Narrow metrics capability is enabled.</td>
</tr>
<tr>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>
Sample Output

show isis overview

user@host> show isis overview
Instance: master
   Router ID: 10.255.107.183
   Adjacency holddown: disabled
   Maximum Areas: 3
   LSP life time: 1200
   Attached bit evaluation: enabled
   SPF delay: 200 msec, SPF holddown: 5000 msec, SPF rapid runs: 3
   IPv4 is enabled, IPv6 is enabled
   Traffic engineering: enabled
   Restart: Disabled
      Helper mode: Enabled
   Level 1
      Internal route preference: 15
      External route preference: 160
      Wide metrics are enabled, Narrow metrics are enabled
   Level 2
      Internal route preference: 18
      External route preference: 165
      Prefix export limit: 5, Prefix export count: 5
      Wide metrics are enabled
show isis route

Syntax

```xml
show isis route
<destination>
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>
```

Syntax (EX Series Switches and QFX Series)

```xml
show isis route
<destination>
<inet | inet6>
<instance instance-name>
<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Display the routes in the IS-IS routing table.

Options

```
none—Display all routes in the IS-IS routing table for all supported address families for all routing instances.

destination—(Optional) Destination address for the route.

inet | inet6—(Optional) Display inet (IPv4) or inet6 (IPv6) routes, respectively.

instance instance-name—(Optional) Display routes for the specified routing instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)—(Optional) Display routes for the specified topology only, or use unicast to display information, if available, for both IPv4 and IPv6 unicast topologies.
```

Required Privilege Level

```
view
```

List of Sample Output

```
show isis route logical-system on page 2790
show isis route (CLNS) on page 2790
show isis route on page 2791
```

Output Fields

Table 348 on page 2789 describes the output fields for the `show isis route` command. Output fields are listed in the approximate order in which they appear.

**Table 348: show isis route Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current version</td>
<td>Number of the current version of the IS-IS routing table.</td>
</tr>
</tbody>
</table>
Table 348: show isis route Output Fields  (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>Version of Level 1 SPF that was run.</td>
</tr>
<tr>
<td>L2</td>
<td>Version of Level 2 SPF that was run.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Destination of the route.</td>
</tr>
<tr>
<td>L</td>
<td>IS-IS level:</td>
</tr>
<tr>
<td></td>
<td>• 1—Level 1 only</td>
</tr>
<tr>
<td></td>
<td>• 2—Level 2 only</td>
</tr>
<tr>
<td></td>
<td>• 3—Level 1 and Level 2</td>
</tr>
<tr>
<td>Version</td>
<td>Version of SPF that generated the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric value associated with the route.</td>
</tr>
<tr>
<td>Type</td>
<td>Metric type: int (internal) or ext (external).</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface to the next hop.</td>
</tr>
<tr>
<td>Via</td>
<td>System identifier of the next hop, displayed as a name if possible.</td>
</tr>
<tr>
<td>ISO Routes</td>
<td>ISO routing table entries.</td>
</tr>
<tr>
<td>snpa</td>
<td>MAC address.</td>
</tr>
</tbody>
</table>

Sample Output

show isis route logical-system

```
user@host> show isis route logical-system ls1
IS-IS routing table                  Current version: L1: 8 L2: 11
Prefix          L Version Metric Type Interface  Via
10.9.7.0/30      2     11     20 int  gr-0/2/0.0  h
10.9.201.1/32    2     11     60 int  gr-0/2/0.0  h
```

show isis route (CLNS)

```
user@host> show isis route
IS-IS routing table                  Current version: L1: 10 L2: 8
IPv4/IPv6 Routes
Prefix          L Version Metric Type Interface  Via
0.0.0.0/0       1     10     10 int  fe-0/0/1.0  ISIS.0
ISIS Routes
Prefix          L Version Metric Type Interface  Via  snpa
0/0             1     10     10 int  fe-0/0/1.0  isis.0 0:12:0:34:0:56
47.0005.80ff.f800.0000.0108.0001/104
```
### show isis route

```
show isis route

IS-IS routing table Current version: L1: 4 L2: 13
IPv4/IPv6 Routes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>L</th>
<th>Version</th>
<th>Metric</th>
<th>Type</th>
<th>Interface</th>
<th>NH</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.71.52/32</td>
<td>2</td>
<td>13</td>
<td>10</td>
<td>int</td>
<td>ae0.0</td>
<td>IPV4</td>
<td>camaro</td>
</tr>
<tr>
<td>10.255.71.238/32</td>
<td>2</td>
<td>13</td>
<td>20</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV4</td>
<td>olympic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>as0.0</td>
<td></td>
<td>glacier</td>
</tr>
<tr>
<td>10.255.71.239/32</td>
<td>2</td>
<td>13</td>
<td>20</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV4</td>
<td>olympic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ae0.0</td>
<td></td>
<td>camaro</td>
</tr>
<tr>
<td>10.255.71.242/32</td>
<td>2</td>
<td>13</td>
<td>10</td>
<td>int</td>
<td>as0.0</td>
<td>IPV4</td>
<td>glacier</td>
</tr>
<tr>
<td>10.255.71.243/32</td>
<td>2</td>
<td>13</td>
<td>10</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV4</td>
<td>olympic</td>
</tr>
<tr>
<td>12.13.0.0/30</td>
<td>2</td>
<td>13</td>
<td>20</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV4</td>
<td>olympic</td>
</tr>
<tr>
<td>12.15.0.0/30</td>
<td>2</td>
<td>13</td>
<td>20</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV4</td>
<td>olympic</td>
</tr>
<tr>
<td>13.15.0.0/30</td>
<td>2</td>
<td>13</td>
<td>30</td>
<td>int</td>
<td>ae0.0</td>
<td>IPV4</td>
<td>camaro</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>so-0/0/0.0</td>
<td>IPV4</td>
<td>olympic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>as0.0</td>
<td>IPV4</td>
<td>glacier</td>
</tr>
<tr>
<td>13.16.0.0/30</td>
<td>2</td>
<td>13</td>
<td>25</td>
<td>int</td>
<td>as0.0</td>
<td>IPV4</td>
<td>glacier</td>
</tr>
<tr>
<td>14.15.0.0/30</td>
<td>2</td>
<td>13</td>
<td>20</td>
<td>int</td>
<td>ae0.0</td>
<td>IPV4</td>
<td>camaro</td>
</tr>
<tr>
<td>192.2.1.0/30</td>
<td>2</td>
<td>13</td>
<td>30</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV4</td>
<td>olympic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>as0.0</td>
<td>IPV4</td>
<td>glacier</td>
</tr>
<tr>
<td>leee::/64</td>
<td>2</td>
<td>13</td>
<td>30</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV6</td>
<td>olympic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>as0.0</td>
<td>IPV6</td>
<td>glacier</td>
</tr>
<tr>
<td>abcdd::10:255:71:52/128</td>
<td>2</td>
<td>13</td>
<td>10</td>
<td>int</td>
<td>ae0.0</td>
<td>IPV6</td>
<td>camaro</td>
</tr>
<tr>
<td>abcdd::10:255:71:238/128</td>
<td>2</td>
<td>13</td>
<td>20</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV6</td>
<td>olympic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>as0.0</td>
<td>IPV6</td>
<td>glacier</td>
</tr>
<tr>
<td>abcdd::10:255:71:239/128</td>
<td>2</td>
<td>13</td>
<td>20</td>
<td>int</td>
<td>so-0/0/0.0</td>
<td>IPV6</td>
<td>olympic</td>
</tr>
</tbody>
</table>
```
ae0.0 IPV6 camaro
abcd::10:255:71:242/128 2 13 10 int as0.0 IPV6 glacier
abcd::10:255:71:243/128 2 13 10 int so-6/0/0.0 IPV6 olympic
**show isis spf**

**Syntax**

`show isis spf (brief | log | results)`

- `<instance instance-name>`
- `<level (1 | 2)>`
- `<logical-system (all | logical-system-name)>`
- `<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>`

**Syntax (EX Series Switches)**

`show isis spf (brief | log | results)`

- `<instance instance-name>`
- `<level (1 | 2)>`
- `<topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)>`

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display information about IS-IS shortest-path-first (SPF) calculations.

**Options**

- `brief`—Display an overview of SPF calculations.
- `instance instance instance-name`—(Optional) Display SPF calculations for the specified routing instance.
- `level (1 | 2)`—(Optional) Display SPF calculations for the specified IS-IS level.
- `log`—Display the log of SPF calculations.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `results`—Display the results of SPF calculations.
- `topology (ipv4-multicast | ipv6-multicast | ipv6-unicast | unicast)`—(Optional) Display SPF calculations for the specified topology only.

**Required Privilege**

`view`

**List of Sample Output**

- `show isis spf log on page 2794`
- `show isis spf results logical-system on page 2795`
- `show isis spf results (CLNS) on page 2796`

**Output Fields**

Table 349 on page 2793 describes the output fields for the `show isis spf` command. Output fields are listed in the approximate order in which they appear.

**Table 349: show isis spf Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>System ID of a node.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric to the node.</td>
</tr>
</tbody>
</table>
Table 349: show isis spf Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface of the next hop.</td>
</tr>
<tr>
<td>Via</td>
<td>System ID of the next hop.</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment (MAC address of the next hop).</td>
</tr>
<tr>
<td>Start time</td>
<td><em>(log option only)</em> Time that the SPF computation started.</td>
</tr>
<tr>
<td>Elapsed (secs)</td>
<td><em>(log option only)</em> Length of time, in seconds, required to complete the SPF computation.</td>
</tr>
<tr>
<td>Count</td>
<td><em>(log option only)</em> Number of times the SPF was triggered.</td>
</tr>
<tr>
<td>Reason</td>
<td><em>(log option only)</em> Reason that the SPF computation was completed.</td>
</tr>
</tbody>
</table>

Sample Output

show isis spf log

```
user@host> show isis spf log logical-system lsl
IS-IS level 1 SPF log:
Start time          Elapsed (secs) Count Reason
Fri Oct 31 12:41:18        0.000069    1 Reconfig
Fri Oct 31 12:41:18        0.000107    3 Updated LSP fix.00-00
Fri Oct 31 12:41:18        0.000050    3 Address change on so-1/2/2.0
Fri Oct 31 12:41:23        0.000033    1 Updated LSP fix.00-00
Fri Oct 31 12:41:28        0.000178    5 New adjacency scat on ge-1/1/0.0
Fri Oct 31 12:41:59        0.000060    1 Updated LSP fix.00-00
Fri Oct 31 12:42:30        0.000161    2 Multi area attachment change
Fri Oct 31 12:56:58        0.000198    1 Periodic SPF
Fri Oct 31 13:10:29        0.000209    1 Periodic SPF

IS-IS level 2 SPF log:
Start time          Elapsed (secs) Count Reason
Fri Oct 31 12:41:18        0.000035    1 Reconfig
Fri Oct 31 12:41:18        0.000047    2 Updated LSP fix.00-00
Fri Oct 31 12:41:18        0.000043    1 Updated LSP fix.00-00
Fri Oct 31 12:41:23        0.000022    1 Updated LSP fix.00-00
Fri Oct 31 12:41:59        0.000144    3 New adjacency h on gr-0/2/0.0
Fri Oct 31 12:42:30        0.000257    3 New LSP skag.00-00
Fri Oct 31 12:54:37        0.000195    1 Periodic SPF
Fri Oct 31 12:55:50        0.000178    1 Updated LSP fix.00-00
Fri Oct 31 12:55:55        0.000174    1 Updated LSP h.00-00
Fri Oct 31 12:55:58        0.000176    1 Updated LSP skag.00-00
Fri Oct 31 13:08:14        0.000198    1 Periodic SPF

IPV6 Unicast IS-IS level 1 SPF log:
Start time          Elapsed (secs) Count Reason
Fri Oct 31 12:41:18        0.0000028    1 Reconfig
Fri Oct 31 12:41:18        0.0000043    3 Updated LSP fix.00-00
Fri Oct 31 12:41:18        0.000112    4 Updated LSP fix.00-00
Fri Oct 31 12:41:23        0.000059    1 Updated LSP fix.00-00
Fri Oct 31 12:41:25        0.000041    1 Updated LSP fix.00-00
```
Fri Oct 31 12:41:28        0.000103    5 New adjacency scat on ge-1/1/0.0
Fri Oct 31 12:41:59        0.000040    1 Updated LSP fix.00-00
Fri Oct 31 12:42:30        0.000118    2 Multi area attachment change
Fri Oct 31 12:56:08        0.000289    1 Periodic SPF
Fri Oct 31 13:11:07        0.000214    1 Periodic SPF
IPV6 Unicast IS-IS level 2 SPF log:

<table>
<thead>
<tr>
<th>Start time</th>
<th>Elapsed (secs)</th>
<th>Count</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000027</td>
<td>1</td>
<td>Reconfig</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000039</td>
<td>2</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:18</td>
<td>0.000049</td>
<td>6</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:23</td>
<td>0.000025</td>
<td>1</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:25</td>
<td>0.000023</td>
<td>1</td>
<td>Updated LSP fix.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:41:59</td>
<td>0.000087</td>
<td>3</td>
<td>New adjacency h on gr-0/2/0.0</td>
</tr>
<tr>
<td>Fri Oct 31 12:42:30</td>
<td>0.000123</td>
<td>3</td>
<td>New LSP skag.00-00</td>
</tr>
<tr>
<td>Fri Oct 31 12:56:08</td>
<td>0.000289</td>
<td>1</td>
<td>Periodic SPF</td>
</tr>
<tr>
<td>Fri Oct 31 13:11:07</td>
<td>0.000214</td>
<td>1</td>
<td>Periodic SPF</td>
</tr>
</tbody>
</table>

show isis spf results logical-system

display isis spf results logical-system ls1

<table>
<thead>
<tr>
<th>IS-IS level 1 SPF results:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>scat.00</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>fix.02</td>
</tr>
<tr>
<td>fix.00</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>3 nodes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IS-IS level 2 SPF results:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>skag.00</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>skag.02</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>h.00</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>fix.00</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>4 nodes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPV6 Unicast IS-IS level 1 SPF results:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>scat.00</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>fix.02</td>
</tr>
<tr>
<td>fix.00</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### IPv6 Unicast IS-IS level 2 SPF Results

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td>8009:3::a09:3200/126</td>
</tr>
<tr>
<td>skag.02</td>
<td>20</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td>8009:3::a09:3200/126</td>
</tr>
<tr>
<td>h.00</td>
<td>10</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td>8009:3::a09:3200/126</td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 nodes

### Multicast IS-IS level 1 SPF Results

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>scat.00</td>
<td>10</td>
<td>ge-1/1/0.0</td>
<td>scat</td>
<td>0:90:69:a6:48:9d</td>
</tr>
<tr>
<td>fix.02</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3 nodes

### Multicast IS-IS level 2 SPF Results

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>20</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>skag.02</td>
<td>20</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>h.00</td>
<td>10</td>
<td>gr-0/2/0.0</td>
<td>h</td>
<td>10.255.245.1/32</td>
</tr>
<tr>
<td>fix.00</td>
<td>0</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
</tbody>
</table>

3 nodes

### IS-IS level 1 SPF Results

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>skag.02</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>pro1-a.02</td>
<td>10</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
<tr>
<td>pro1-a.00</td>
<td>0</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
</tbody>
</table>

3 nodes

### IS-IS level 2 SPF Results

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>skag.02</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>pro1-a.02</td>
<td>10</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
<tr>
<td>pro1-a.00</td>
<td>0</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
</tbody>
</table>

3 nodes

---

```
show isis spf results (CLNS)
```

```
user@host> show isis spf results
IS-IS level 1 SPF results:
<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>skag.02</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>pro1-a.02</td>
<td>10</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
<tr>
<td>pro1-a.00</td>
<td>0</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
</tbody>
</table>

3 nodes

IS-IS level 2 SPF results:

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>skag.00</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>skag.02</td>
<td>10</td>
<td>fe-0/0/1.0</td>
<td>toothache</td>
<td>0:12:0:34:0:56</td>
</tr>
<tr>
<td>pro1-a.02</td>
<td>10</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
<tr>
<td>pro1-a.00</td>
<td>0</td>
<td></td>
<td></td>
<td>10.255.245.1/32</td>
</tr>
</tbody>
</table>

20 10.255.245.1/32
20 192.168.37.64/29
20 47.0005.80ff.f800.0000.0109.0010/104
```
<table>
<thead>
<tr>
<th>Node</th>
<th>Value 1</th>
<th>Value 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>pro1-a.02</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>pro1-a.00</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>10.255.245.1/32</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>192.168.37.64/29</td>
</tr>
</tbody>
</table>

3 nodes
**show isis statistics**

**Syntax**
```
show isis statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches and QFX Series)**
```
show isis statistics
<instance instance-name>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Display statistics about IS-IS traffic.

**Options**
- **none**—Display IS-IS traffic statistics for all routing instances.
- **instance instance-name**—(Optional) Display statistics for the specified routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view

**Related Documentation**
- clear isis statistics on page 2758
- List of Sample Output
  - show isis statistics on page 2800

**Output Fields**
```
Table 350 on page 2799 describes the output fields for the show isis statistics command. Output fields are listed in the approximate order in which they appear.
```
### Table 350: show isis statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PDU type</strong></td>
<td>PDU type:</td>
</tr>
<tr>
<td></td>
<td>• <strong>CSNP</strong>—Complete sequence number PDUs contain a complete list of all link-state PDUs in the IS-IS database. CSNPs are sent periodically on all links, and the receiving systems use the information in the CSNP to update and synchronize their link-state PDU databases. The designated router multicasts CSNPs on broadcast links in place of sending explicit acknowledgments for each link-state PDU.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IIH</strong>—IS-IS hello packets are broadcast to discover the identity of neighboring IS-IS systems and to determine whether the neighbors are Level 1 or Level 2 intermediate systems.</td>
</tr>
<tr>
<td></td>
<td>• <strong>LSP</strong>—Link-state PDUs contain information about the state of adjacencies to neighboring IS-IS systems. Link-state PDUs are flooded periodically throughout an area.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PSNP</strong>—Partial sequence number PDUs are sent multicast by a receiver when it detects that it is missing a link-state PDU (when its link-state PDU database is out of date). The receiver sends a PSNP to the system that transmitted the CSNP, effectively requesting that the missing link-state PDU be transmitted. That routing device, in turn, forwards the missing link-state PDU to the requesting routing device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unknown</strong>—The PDU type is unknown.</td>
</tr>
<tr>
<td><strong>Received</strong></td>
<td>Number of PDUs received since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Processed</strong></td>
<td>Number of PDUs received less the number dropped.</td>
</tr>
<tr>
<td><strong>Drops</strong></td>
<td>Number of PDUs dropped.</td>
</tr>
<tr>
<td><strong>Sent</strong></td>
<td>Number of PDUs transmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Rexmit</strong></td>
<td>Number of PDUs retransmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Total packets received/sent</strong></td>
<td>Total number of PDUs received and transmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>SNP queue length</strong></td>
<td>Number of CSPN and PSNP packets currently waiting in the queue for processing. This value is almost always 0.</td>
</tr>
<tr>
<td><strong>LSP queue length</strong></td>
<td>Number of link-state PDUs waiting in the queue for processing. This value is almost always 0.</td>
</tr>
<tr>
<td><strong>SPF runs</strong></td>
<td>Number of shortest-path-first (SPF) calculations that have been performed. If this number is incrementing rapidly, it indicates that the network is unstable.</td>
</tr>
<tr>
<td><strong>Fragments rebuilt</strong></td>
<td>Number of link-state PDU fragments that the local system has computed.</td>
</tr>
<tr>
<td><strong>LSP regenerations</strong></td>
<td>Number of link-state PDUs that have been regenerated. A link-state PDU is regenerated when it is nearing the end of its lifetime and it has not changed.</td>
</tr>
<tr>
<td><strong>Purges initiated</strong></td>
<td>Number of purges that the system initiated. A purge is initiated if the software decides that a link-state PDU must be removed from the network.</td>
</tr>
</tbody>
</table>
Sample Output
show isis statistics

user@host> show isis statistics
IS-IS statistics for merino:

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Rexmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>12227</td>
<td>12227</td>
<td>0</td>
<td>8184</td>
<td>683</td>
</tr>
<tr>
<td>IIH</td>
<td>113808</td>
<td>113808</td>
<td>0</td>
<td>115817</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>198868</td>
<td>198868</td>
<td>0</td>
<td>198934</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>6985</td>
<td>6979</td>
<td>6</td>
<td>8274</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>331888</td>
<td>331882</td>
<td>6</td>
<td>331209</td>
<td>683</td>
</tr>
</tbody>
</table>

Total packets received: 331888 Sent: 331892

SNP queue length: 0 Drops: 0
LSP queue length: 0 Drops: 0

SPF runs: 1014
Fragments rebuilt: 1038
LSP regenerations: 425
Purges initiated: 0
PART 18

OSPF

- Overview on page 2803
- Configuration on page 2811
- Administration on page 2881
CHAPTER 54

Overview

- Layer 3 Protocols on page 2803
- OSPF Overview on page 2806

Layer 3 Protocols

- Layer 3 Protocols Supported on EX Series Switches on page 2803
- Layer 3 Protocols Not Supported on EX Series Switches on page 2804

Layer 3 Protocols Supported on EX Series Switches

EX Series switches support the Junos OS Layer 3 features and configuration statements listed in Table 326 on page 2553:

Table 351: Supported Junos OS Layer 3 Protocol Statements and Features

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Fully supported.</td>
<td><em>Junos OS Routing Protocols Configuration Guide</em></td>
</tr>
<tr>
<td>BFD</td>
<td>Fully supported.</td>
<td><em>Junos OS Routing Protocols Configuration Guide</em></td>
</tr>
<tr>
<td>ICMP</td>
<td>Fully supported.</td>
<td><em>Junos OS Routing Protocols Configuration Guide</em></td>
</tr>
<tr>
<td>IGMPv1, v2, and v3</td>
<td>Fully supported.</td>
<td><em>Junos OS Multicast Protocols Configuration Guide</em></td>
</tr>
<tr>
<td>IS-IS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td><em>Junos OS Routing Protocols Configuration Guide</em></td>
</tr>
<tr>
<td>MLD</td>
<td>Fully supported (MLD versions 1 and 2).</td>
<td><em>Junos OS Multicast Protocols Configuration Guide</em></td>
</tr>
<tr>
<td>MPLS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td><em>Junos OS MPLS Applications Configuration Guide</em></td>
</tr>
<tr>
<td>OSPFv1, v2 and v3</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td><em>Junos OS Routing Protocols Configuration Guide</em></td>
</tr>
</tbody>
</table>
Table 351: Supported Junos OS Layer 3 Protocol Statements and Features (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td>Fully supported on EX3200, EX3300, EX4200, EX6200, and EX8200 switches.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>PPM</td>
<td>Supported. See “EX Series Switch Software Features Overview” on page 27 for specific platform information.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIPng</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>SNMP</td>
<td>Fully supported.</td>
<td>Junos OS Network Management Configuration Guide</td>
</tr>
<tr>
<td>VRRP</td>
<td>Fully supported.</td>
<td>See “Understanding VRRP on EX Series Switches” on page 2220. See also Junos OS High Availability Guide.</td>
</tr>
</tbody>
</table>

Related Documentation
- Layer 3 Protocols Not Supported on EX Series Switches on page 2554
- EX Series Switch Software Features Overview on page 27

Layer 3 Protocols Not Supported on EX Series Switches
EX Series switches do not support the Junos OS Layer 3 protocols and features listed in Table 327 on page 2554:

Table 352: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVMRP</td>
<td>• dvmrp and subordinate statements</td>
</tr>
<tr>
<td>Flow aggregation (cflowd)</td>
<td>• cflow and subordinate statements</td>
</tr>
<tr>
<td>IPSec</td>
<td>• [edit services] statements related to IPSec</td>
</tr>
<tr>
<td>IS-IS:</td>
<td>• cns-routing statement</td>
</tr>
<tr>
<td>• ES-IS</td>
<td>• ipv6-multicast statement</td>
</tr>
<tr>
<td>• IPv6 in multicast routing protocols</td>
<td>• lsp-interval statement</td>
</tr>
<tr>
<td></td>
<td>• label-switched-path statement</td>
</tr>
<tr>
<td></td>
<td>• lsp-lifetime statement</td>
</tr>
<tr>
<td></td>
<td>• te-metric statement</td>
</tr>
<tr>
<td>Logical routers</td>
<td>• logical-routers and subordinate statements</td>
</tr>
</tbody>
</table>
Table 352: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
</table>
| MPLS:  | • Fast Reroute (FRR)  
|        | • Label Distribution Protocol (LDP) (except on EX8200 switches)  
|        | • Layer 3 VPNs (except on EX8200 switches)  
|        | • Multiprotocol BGP (MP-BGP) for VPN-IPv4 family  
|        | • Pseudowire emulation (PWE3)  
|        | • Routing policy statements related to Layer 3 VPNs and MPLS (except on EX8200 switches)  
|        | • Virtual Private LAN Service (VPLS)  
|        | • ldp and all subordinate statements (except on EX8200 switches)  
|        | • nat and subordinate statements  
|        | • Policy statements related to NAT  
|        | • demand-circuit statement  
|        | • label-switched-path and subordinate statements  
|        | • neighbor statement within an OSPF area  
|        | • peer-interface and subordinate statements within an OSPF area  
|        | • sham-link statement  
|        | • te-metric statement  
| OSPF    | • Not supported on EX2200 switches  
| PIM SM  | • Not supported on EX2200 switches  
| PIM SSM | • Not supported on EX2200 switches  
| PIM DM  | • Not supported on EX2200 or EX4500 switches  
| PIM:    | • inet6 family (EX2200 and EX4500 switches)  
|        | • inet6 family (EX2200 and EX4500 switches)  
| PPM     | • Not supported on EX2200 and EX3300 switches  
| Routing instances: | • l2vpn and subordinate statements (except on EX8200 switches)  
|        | • ldp and subordinate statements (except on EX8200 switches)  
|        | • ldp and subordinate statements (except on EX8200 switches)  
|        | • vpls and subordinate statements  
| Routed VLAN interfaces (RVIs) | • family mpls statement |
### Table 352: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP and SDP</td>
<td>• sap and all subordinate statements</td>
</tr>
<tr>
<td>General routing options in the routing-options hierarchy:</td>
<td>• auto-export and subordinate statements</td>
</tr>
<tr>
<td>• MPLS and label-switched-paths</td>
<td>• dynamic-tunnels and subordinate statements</td>
</tr>
<tr>
<td>• lsp-next-hop</td>
<td>• multicast and subordinate statements</td>
</tr>
<tr>
<td>• p2mp-lsp-next-hop</td>
<td>• route-distinguisher-id statement (except on EX8200 switches)</td>
</tr>
<tr>
<td>• route-distinguisher-id statement (except on EX8200 switches)</td>
<td>• accounting and subordinate statements</td>
</tr>
<tr>
<td>• family mpls and family multiservice under hash-key hierarchy:</td>
<td>• family mpls and family multiservice under hash-key hierarchy:</td>
</tr>
<tr>
<td>• Under monitoring group-name family inet output hierarchy:</td>
<td>• cflowd statement</td>
</tr>
<tr>
<td>• port-mirroring statement (On EX Series switches, port mirroring is implemented using the analyzer statement.)</td>
<td>• flow-export-destination statement</td>
</tr>
<tr>
<td>• sampling and subordinate statements</td>
<td>• flow-inactive-timeout statement</td>
</tr>
<tr>
<td>•</td>
<td>• interface statement</td>
</tr>
</tbody>
</table>

### Related Documentation

- Layer 3 Protocols Supported on EX Series Switches on page 2553
- EX Series Switch Software Features Overview on page 27

### OSPF Overview

- Understanding IPsec Authentication for OSPF Packets on EX Series Switches on page 2807
Understanding IPsec Authentication for OSPF Packets on EX Series Switches

IP Security (IPsec) provides a secure way to authenticate senders and encrypt IP version 4 (IPv4) traffic between network devices. IPsec offers network administrators for Juniper Networks EX Series Ethernet Switches and their users the benefits of data confidentiality, data integrity, sender authentication, and anti-replay services.

IPsec is a framework for ensuring secure private communication over IP networks and is based on standards developed by the International Engineering Task Force (IETF). IPsec provides security services at the network layer of the Open Systems Interconnection (OSI) model by enabling a system to select required security protocols, determine the algorithms to use for the security services, and implement any cryptographic keys required to provide the requested services. You can use IPsec to protect one or more paths between a pair of hosts, between a pair of security gateways (such as switches), or between a security gateway and a host.

OSPF version 3 (OSPFv3), unlike OSPF version 2 (OSPFv2), does not have a built-in authentication method and relies on IPsec to provide this functionality. You can secure specific OSPFv3 interfaces and protect OSPFv3 virtual links.

- Authentication Algorithms on page 2807
- Encryption Algorithms on page 2808
- IPsec Protocols on page 2808
- Security Associations on page 2808
- IPsec Modes on page 2809

Authentication Algorithms

Authentication is the process of verifying the identity of the sender. Authentication algorithms use a shared key to verify the authenticity of the IPsec devices. The Juniper Networks Junos operating system (Junos OS) uses the following authentication algorithms:

- Message Digest 5 (MD5) uses a one-way hash function to convert a message of arbitrary length to a fixed-length message digest of 128 bits. Because of the conversion process, it is mathematically infeasible to calculate the original message by computing it backwards from the resulting message digest. Likewise, a change to a single character in the message will cause it to generate a very different message digest number.

To verify that the message has not been tampered with, Junos OS compares the calculated message digest against a message digest that is decrypted with a shared key. Junos OS uses the MD5 hashed message authentication code (HMAC) variant that provides an additional level of hashing. MD5 can be used with an authentication header (AH) and Encapsulating Security Payload (ESP).

- Secure Hash Algorithm 1 (SHA-1) uses a stronger algorithm than MD5. SHA-1 takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest ensures that the data has not been changed and that it originates from the correct source. Junos OS uses the SHA-1 HMAC variant that provides an
additional level of hashing. SHA-1 can be used with AH, ESP, and Internet Key Exchange (IKE).

Encryption Algorithms

Encryption encodes data into a secure format so that it cannot be deciphered by unauthorized users. As with authentication algorithms, a shared key is used with encryption algorithms to verify the authenticity of IPsec devices. Junos OS uses the following encryption algorithms:

- Data Encryption Standard cipher-block chaining (DES-CBC) is a symmetric secret-key block algorithm. DES uses a key size of 64 bits, where 8 bits are used for error detection and the remaining 56 bits provide encryption. DES performs a series of simple logical operations on the shared key, including permutations and substitutions. CBC takes the first block of 64 bits of output from DES, combines this block with the second block, feeds this back into the DES algorithm, and repeats this process for all subsequent blocks.

- Triple DES-CBC (3DES-CBC) is an encryption algorithm that is similar to DES-CBC but provides a much stronger encryption result because it uses three keys for 168-bit (3 x 56-bit) encryption. 3DES works by using the first key to encrypt the blocks, the second key to decrypt the blocks, and the third key to reencrypt the blocks.

IPsec Protocols

IPsec protocols determine the type of authentication and encryption applied to packets that are secured by the switch. Junos OS supports the following IPsec protocols:

- AH—Defined in RFC 2402, AH provides connectionless integrity and data origin authentication for IPv4. It also provides protection against replays. AH authenticates as much of the IP header as possible, as well as the upper-level protocol data. However, some IP header fields might change in transit. Because the value of these fields might not be predictable by the sender, they cannot be protected by AH. In an IP header, AH can be identified with a value of 51 in the Protocol field of an IPv4 packet.

- ESP—Defined in RFC 2406, ESP can provide encryption and limited traffic flow confidentiality or connectionless integrity, data origin authentication, and an anti-replay service. In an IP header, ESP can be identified with a value of 50 in the Protocol field of an IPv4 packet.

Security Associations

An IPsec consideration is the type of security association (SA) that you wish to implement. An SA is a set of IPsec specifications that are negotiated between devices that are establishing an IPsec relationship. These specifications include preferences for the type of authentication, encryption, and IPsec protocol to be used when establishing the IPsec connection. An SA can be either unidirectional or bidirectional, depending on the choices made by the network administrator. An SA is uniquely identified by a Security Parameter Index (SPI), an IPv4 or IPv6 destination address, and a security protocol (AH or ESP) identifier.
IPsec Modes

Junos OS supports the following IPsec modes:

- Tunnel mode is supported for both AH and ESP in Junos OS. In tunnel mode, the SA and associated protocols are applied to tunneled IPv4 or IPv6 packets. For a tunnel mode SA, an outer IP header specifies the IPsec processing destination and an inner IP header specifies the ultimate destination for the packet. The security protocol header appears after the outer IP header and before the inner IP header. In addition, there are slight differences for tunnel mode when you implement it with AH and ESP:
  - For AH, portions of the outer IP header are protected, as well as the entire tunneled IP packet.
  - For ESP, only the tunneled packet is protected, not the outer header.

When one side of an SA is a security gateway (such as a switch), the SA must use tunnel mode. However, when traffic (for example, SNMP commands or BGP sessions) is destined for a switch, the system acts as a host. Transport mode is allowed in this case because the system does not act as a security gateway and does not send or receive transit traffic.

**NOTE:** Tunnel mode is not supported for OSPFv3 control packet authentication.

- Transport mode provides an SA between two hosts. In transport mode, the protocols provide protection primarily for upper-layer protocols. A transport mode security protocol header appears immediately after the IP header and any options and before any higher-layer protocols (for example, TCP or UDP). There are slight differences for transport mode when you implement it with AH and ESP:
  - For AH, selected portions of the IP header are protected, as well as selected portions of the extension headers and selected options within the IPv4 header.
  - For ESP, only the higher-layer protocols are protected, not the IP header or any extension headers preceding the ESP header.

Related Documentation:
- Using IPsec to Secure OSPFv3 Networks (CLI Procedure) on page 2815
- Configuring an OSPF Network (J-Web Procedure) on page 2811
CHAPTER 55

Configuration

- Configuration Tasks on page 2811
- Configuration Statements on page 2817

Configuration Tasks

- Configuring an OSPF Network (J-Web Procedure) on page 2811
- Using IPsec to Secure OSPFv3 Networks (CLI Procedure) on page 2815

Configuring an OSPF Network (J-Web Procedure)

You can use the J-Web interface to create multiarea OSPF networks on an EX Series switch.

To configure a multiarea OSPF network:

1. Select Configure > Routing > OSPF.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - Add—Adds an OSPF area. Enter information into the configuration page as described in Table 353 on page 2812.
   - Edit—Modifies an existing OSPF area. Enter information into the configuration page as described in Table 353 on page 2812.
   - Delete—Deletes an existing OSPF area.

3. To modify OSPF global settings, click Edit. Enter information as described in Table 354 on page 2813.

4. To disable OSPF, click Disable.
Table 353: OSPF Routing Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area Id</td>
<td>Uniquely identifies the area within its AS.</td>
<td>Type a 32-bit numeric identifier for the area. Type an integer or select and edit the value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3, the value assigned to the area is 0.0.0.3.</td>
</tr>
<tr>
<td>Area Ranges</td>
<td>Specifies a range of IP addresses for an area when sending summary link advertisements (within an area).</td>
<td>To add a range:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Type the area range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the subnet mask.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. To override the metric for the IP address range, type a specific metric value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. If you do not want to display the routes that are contained within a summary, select Restrict advertisements of this area range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. If you want a summary of a route to be advertised only when an exact match is made with the configured summary range, select Enforce exact match for advertisement of this area range.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To modify an existing area range, select the area range, click Edit, and edit the value. Click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete an area range, select the area range and click Delete.</td>
</tr>
<tr>
<td>Area Type</td>
<td>Designates the type of OSPF area.</td>
<td>Select the type of OSPF area you are creating from the list.</td>
</tr>
<tr>
<td></td>
<td>• regular—A regular OSPF area, including the backbone area</td>
<td>If you select stub:</td>
</tr>
<tr>
<td></td>
<td>• stub—A stub area</td>
<td>1. Enter the default metric.</td>
</tr>
<tr>
<td></td>
<td>• nssa—A not-so-stubby area (NSSA)</td>
<td>2. To flood summary LSAs into the stub area, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select nssa:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Specify the metric type.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the default metric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. To flood summary LSAs into the nssa area, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. To flood Type-7 LSAs into the nssa area, select the check box.</td>
</tr>
</tbody>
</table>

Interfaces tab
Table 353: OSPF Routing Configuration Summary  (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>Specifies the interfaces to be associated with the OSPF configuration</td>
<td>To associate an interface with the configuration, select the interface from the list, select Associate and click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To edit an interface’s configuration:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select the interface from the list and click Edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the cost of an OSPF interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the traffic engineering metric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Specify how often the routing device sends hello packets from the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Specify how long the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface’s neighbors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. To enable OSPF on the interface, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. To inform other protocols about neighbor down events, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. To treat the interface as a secondary interface, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. To only advertise OSPF, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Click OK.</td>
</tr>
<tr>
<td>Policies tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import Policy</td>
<td>Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas.</td>
<td>Click Add to add an import policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click Move up or Move down to move the selected policy up or down the list of policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click Remove to remove an import policy.</td>
</tr>
<tr>
<td>Export Policy</td>
<td>Specifies one or more policies to control which summary LSAs are flooded into an area.</td>
<td>Click Add to add an export policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click Move up or Move down to move the selected policy up or down the list of policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click Remove to remove an export policy.</td>
</tr>
</tbody>
</table>

Table 354: Edit OSPF Global Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router Id</td>
<td>Specifies the ID for the routing device.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>RIB Group</td>
<td>Installs the routes learned from OSPF routing instances into routing tables in the OSPF routing table group.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Internal Route Preference</td>
<td>Specifies the route preference for internal groups.</td>
<td>Type or select and edit the value.</td>
</tr>
</tbody>
</table>
Table 354: Edit OSPF Global Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Route Preference</td>
<td>Specifies the route preference for external groups.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Configures graceful restart for OSPF.</td>
<td>To configure graceful restart:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Specify the estimated time to send out purged grace LSAs over all the interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specified the estimated time to reacquire a full OSPF neighbor from each area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. To disable No Strict LSA Checking, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. To disable graceful restart helper capability, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click OK.</td>
</tr>
<tr>
<td>SPF Options</td>
<td>Configure options for running the shortest-path-first (SPF) algorithm.</td>
<td>To configure SPF:</td>
</tr>
<tr>
<td></td>
<td>The SPF algorithm can run in succession, and a hold-down interval after the SPF algorithm runs the maximum number of times.</td>
<td>1. Specify the time interval between the detection of a topology change and when the SPF algorithm runs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the time interval to hold down, or wait before a subsequent SPF algorithm runs after the SPF algorithm has run the configured maximum number of times in succession.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the maximum number of times the SPF algorithm can run in succession. After the maximum is reached, the hold-down interval begins.</td>
</tr>
</tbody>
</table>

Policies tab

| Import Policy          | Specifies one or more policies to control which routes learned from an area are used to generate summary link-state advertisements (LSAs) into other areas. | Click Add to add an import policy.                                    |
|                       |                                                                                                                                         | Click Move up or Move down to move the selected policy up or down the list of policies. |
|                       |                                                                                                                                         | Click Remove to remove an import policy.                               |
| Export Policy         | Specifies one or more policies to control which summary LSAs are flooded into an area.                                                 | Click Add to add an export policy.                                    |
|                       |                                                                                                                                         | Click Move up or Move down to move the selected policy up or down the list of policies. |
|                       |                                                                                                                                         | Click Remove to remove an export policy.                               |

Trace Options tab

| File Name              | Specifies the name of the file to receive the output of the tracing operation.                                                         | Type or select and edit the name.                                      |
|                       |                                                                                                                                         |                                                                         |
| Number of Files       | Specifies the maximum number of trace files.                                                                                            | Type or select and edit the name.                                      |
|                       |                                                                                                                                         |                                                                         |
| File Size             | Specifies the maximum size for each trace file.                                                                                         | Type or select and edit the name.                                      |
Table 354: Edit OSPF Global Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>World Readable</td>
<td>Specifies whether the trace file can be read by any user or not.</td>
<td>Select True to allow any user to read the file. Select False to disallow all users being able to read the file.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies the tracing operation to perform.</td>
<td>Select a value from the list.</td>
</tr>
</tbody>
</table>

Related Documentation
- Monitoring OSPF Routing Information on page 2881
- Layer 3 Protocols Supported on EX Series Switches on page 2553

Using IPsec to Secure OSPFv3 Networks (CLI Procedure)

OSPF version 3 (OSPFv3) does not have a built-in authentication method and relies on IP Security (IPsec) to provide this functionality. You can use IPsec to secure OSPFv3 interfaces on EX Series switches.

This topic includes:
- Configuring Security Associations on page 2815
- Securing OPSFv3 Networks on page 2816

Configuring Security Associations

When you configure a security association (SA), include your choices for authentication, encryption, direction, mode, protocol, and security parameter index (SPI).

To configure a security association:

1. Specify a name for the security association:
   ```
   [edit security ipsec]
   user@switch# set security-association sa-name
   ```
2. Specify the mode of the security association:
   ```
   [edit security ipsec security-association sa-name]
   user@switch# set mode transport
   ```
3. Specify the type of security association:
   ```
   [edit security ipsec security-association sa-name]
   user@switch# set type manual
   ```
4. Specify the direction of the security association:
   ```
   [edit security ipsec security-association sa-name]
   user@switch# set direction bidirectional
   ```
5. Specify the value of the security parameter index:
   ```
   [edit security ipsec security-association sa-name]
   user@switch# set spi spi-value
   ```
6. Specify the type of authentication to be used:
   ```
   [edit security ipsec security-association sa-name]
   ```
7. Specify the encryption algorithm and key:

   [edit security ipsec security-association sa-name]
   user@switch# set encryption algorithm algorithm key type

Securing OSPFv3 Networks

You can secure the OSPFv3 network by applying the SA to the OSPFv3 configuration.

To secure the OSPFv3 network:

   [edit protocols ospf3 area area-number interface interface-name]
   user@switch# set ipsec-sa sa-name

Related Documentation

- Understanding IPsec Authentication for OSPF Packets on EX Series Switches on page 2807
- Configuring an OSPF Network (J-Web Procedure) on page 2811
- Junos OS System Basics Configuration Guide
Configuration Statements
area

Syntax

```
area area-id {
    interface interface-name {
        passive;
        topology (ipv4-multicast | name) {
            disable;
        }
    }
    virtual-link neighbor-id router-id transit-area area-id {
        topology (ipv4-multicast | name) {
            disable;
        }
    }
}
```

Hierarchy Level

[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Specify the area identifier for this routing device to use when participating in OSPF routing. All routing devices in an area must use the same area identifier to establish adjacencies.

Specify multiple `area` statements to configure the routing device as an area border router. An area border router does not automatically summarize routes between areas. Use the `area-range` statement to configure route summarization. By definition, an area border router must be connected to the backbone area either through a physical link or through a virtual link. To create a virtual link, include the `virtual-link` statement.

To specify that the routing device is directly connected to the OSPF backbone, include the `area 0.0.0.0` statement.

All routing devices on the backbone must be contiguous. If they are not, use the `virtual-link` statement to create the appearance of connectivity to the backbone.
You can also configure any interface that belongs to one or more topologies to advertise the direct interface addresses without actually running OSPF on that interface. By default, OSPF must be configured on an interface in order for direct interface addresses to be advertised as interior routes.

**NOTE:** If you configure an interface with the `passive` statement, it applies to all the topologies to which the interface belongs. You cannot configure an interface as passive for only one specific topology and have it remain active for any other topologies to which it belongs.

### Options

- **area-id**—Area identifier. The identifier can be up to 32 bits. It is common to specify the area number as a simple integer or an IP address. Area number `0.0.0.0` is reserved for the OSPF backbone area.

### Required Privilege

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

### Related Documentation

- [OSPF Areas and Router Functionality Overview](#)
- [Understanding Multiple Address Families for OSPFv3](#)
- [virtual-link on page 2880](#)
area-range

Syntax  area-range network/mask-length <exact> <override-metric metric> <restrict>;

Hierarchy Level  [edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id nssa],
[edit logical-systems logical-system-name realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa],
[edit logical-systems logical-system-name routing-instances routing-instance-name realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit protocols (ospf | ospf3) area area-id],
[edit protocols (ospf | ospf3) area area-id nssa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa],
[edit routing-instances routing-instance-name realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  (Area border routers only) For an area, summarize a range of IP addresses when sending summary link advertisements (within an area). To summarize multiple ranges, include multiple area-range statements.

For a not-so-stubby area (NSSA), summarize a range of IP addresses when sending NSSA link-state advertisements. The specified prefixes are used to aggregate external routes learned within the area when the routes are advertised to other areas. To specify multiple prefixes, include multiple area-range statements. All external routes learned within the area that do not fall into one of the prefixes are advertised individually to other areas.

Default  By default, area border routing devices do not summarize routes being sent from one area to other areas, but rather send all routes explicitly.

Options  exact—(Optional) Summarization of a route is advertised only when an exact match is made with the configured summary range.

mask-length—Number of significant bits in the network mask.

network—IP address. You can specify one or more IP addresses.
override-metric metric—(Optional) Override the metric for the IP address range and configure a specific metric value.

restrict—(Optional) Do not advertise the configured summary. This hides all routes that are contained within the summary, effectively creating a route filter.

Range: 1 through 16,777,215

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Example: Summarizing Ranges of Routes in OSPF Link-State Advertisements
**bandwidth-based-metrics**

**Syntax**

```plaintext
bandwidth-based-metrics {
  bandwidth value;
  metric number;
}
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name]`
- `[edit logical-systems logical-system-name protocols ospf area area-id interface interface-name topology topology-name]`
- `[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name topology topology-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instances protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]`
- `[edit protocols (ospf | ospf3) area area-id interface interface-name]`
- `[edit protocols ospf area area-id interface interface-name topology topology-name]`
- `[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]`
- `[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name]`
- `[edit routing-instances routing-instance-name protocols ospf area area-id interface interface-name topology topology-name]`
- `[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]`

**Release Information**

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.

**Description**

Specify a set of bandwidth threshold values and associated metric values for an OSPF interface or for a topology on an OSPF interface. When the bandwidth of an interface changes, Junos OS automatically sets the interface metric to the value associated with the appropriate bandwidth threshold value.

**Options**

- **bandwidth value**—Specify the bandwidth threshold in bits per second.
  - **Range:** 9600 through 1,000,000,000,000,000

- **metric number**—Specify a metric value to associate with a specific bandwidth value.
  - **Range:** 1 through 65,535

**NOTE:** You must also configure a static metric value for the OSPF interface or topology with the metric statement. Junos OS uses this value to calculate the cost of a route from the OSPF interface or topology if the bandwidth for the interface is higher than of any bandwidth threshold values configured for bandwidth-based metrics.
Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Dynamically Adjusting OSPF Interface Metrics Based on Bandwidth
• metric on page 2849
• Example: Dynamically Adjusting OSPF Interface Metrics Based on Bandwidth
**bfd-liveness-detection (Protocols OSPF)**

**Syntax**

```
bfd-liveness-detection {
  authentication {
    algorithm algorithm-name;
    key-chain key-chain-name;
    loose-check;
  }
  detection-time {
    threshold milliseconds;
  }
  full-neighbors-only
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  version (1 | automatic);
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
`detection-time threshold` and `transmit-interval threshold` options added in Junos OS Release 8.2.
Support for logical systems introduced in Junos OS Release 8.3.
`no-adaptation` option introduced in Junos OS Release 9.0.
`no-adaptation` option introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 introduced in Junos OS Release 9.3.
Support for OSPFv3 introduced in Junos OS Release 9.3 for EX Series switches.
`full-neighbors-only` option introduced in Junos OS Release 9.5.
`full-neighbors-only` option introduced in Junos OS Release 9.5 for EX Series switches.
authentication algorithm, authentication key-chain, and authentication loose-check options introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**  Configure bidirectional failure detection timers and authentication for OSPF.

The remaining statements are explained separately.
Options  

**authentication algorithm algorithm-name** — Configure the algorithm used to authenticate the specified BFD session: simple-password, keyed-md5, keyed-sha-1, meticulous-keyed-md5, or meticulous-keyed-sha-1.

**authentication key-chain key-chain-name** — Associate a security key with the specified BFD session using the name of the security keychain. The name you specify must match one of the keychains configured in the authentication-key-chains key-chain statement at the [edit security] hierarchy level.

**authentication loose-check** — (Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication may not be configured at both ends of the BFD session.

**detection-time threshold milliseconds** — Configure a threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

**full-neighbors-only** — Establish BFD sessions only for OSPF neighbors in the full state. The default behavior is to establish BFD sessions for all OSPF neighbors.

**minimum-interval milliseconds** — Configure the minimum interval after which the local routing device transmits a hello packet and then expects to receive a reply from the neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum transmit and receive intervals separately using the transmit-interval minimum-interval and minimum-receive-interval statements.

**Range:** 1 through 255,000 milliseconds

**minimum-receive-interval milliseconds** — Configure the minimum interval after which the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum receive interval using the minimum-interval statement.

**Range:** 1 through 255,000 milliseconds

**multiplier number** — Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.

**Range:** 1 through 255

**Default:** 3

**no-adaptation** — Specify that BFD sessions should not adapt to changing network conditions. We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

**transmit-interval threshold milliseconds** — Configure the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent. The interval threshold must be greater than the minimum transmit interval.

**Range:** 0 through 4,294,967,295 (2^{32} – 1)

**transmit-interval minimum-interval milliseconds** — Configure the minimum interval at which the routing device transmits hello packets to a neighbor with which it has established
a BFD session. Optionally, instead of using this statement, you can configure the minimum transmit interval using the `minimum-interval` statement.

**Range:** 1 through 255,000

**version**—Configure the BFD version to detect: 1 (BFD version 1) or `automatic` (autodetect the BFD version).

**Default:** automatic

**Required Privilege**

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring BFD for OSPF
- Example: Configuring BFD Authentication for OSPF
dead-interval

Syntax  
dead-interval seconds;

Hierarchy Level  
[edit logical-systems logical-system-name protocols ospf area area-id peer-interface interface-name],
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id virtual-link],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit protocols ospf area area-id peer-interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

Description  
Specify how long OSPF waits before declaring that a neighboring routing device is unavailable. This is an interval during which the routing device receives no hello packets from the neighbor.

Options  
seconds—Interval to wait.
Range: 1 through 65,535 seconds
Default: Four times the hello interval—40 seconds (broadcast and point-to-point networks); 120 seconds (nonbroadcast multiple access (NBMA) networks)

Required Privilege Level  
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  
• Example: Configuring OSPF Timers
• Configuring RSVP and OSPF for LMP Peer Interfaces
default-lsa

Syntax
default-lsa {
    default-metric metric;
    metric-type type;
    type-7;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id nssa],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa],
[edit protocols (ospf | ospf3) area area-id nssa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

Description
On area border routers only, for a not-so-stubby area (NSSA), inject a default link-state advertisement (LSA) with a specified metric value into the area. The default route matches any destination that is not explicitly reachable from within the area.

The remaining statements are explained separately.

Required Privilege
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• OSPF Areas and Router Functionality Overview
• Example: Configuring OSPF Not-So-Stubby Areas
• nssa on page 2854
• stub on page 2871
**default-metric**

**Syntax**
```
default-metric metric;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id stub],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id stub],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id stub],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id stub],
[edit protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit protocols (ospf | ospf3) area area-id stub],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id stub],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id stub]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**
On area border routing devices only, for a stub area, inject a default route with a specified metric value into the area. The default route matches any destination that is not explicitly reachable from within the area.

**Options**
- `metric`—Metric value.
  
  **Range:** 1 through 16,777,215

**Required Privilege**
```
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
```

**Related Documentation**
- [OSPF Areas and Router Functionality Overview](#)
- [nssa on page 2854](#)
• stub on page 2871
disable (OSPF)

Syntax
disable;

Hierarchy Level
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols ospf area area-id peer-interface interface-name],
[edit logical-systems logical-system-name protocols ospf area area-id peer-interface interface-name],
[edit logical-systems logical-system-name protocols ospf3 area area-id interface interface-name],
[edit logical-systems logical-system-name protocols ospf3 area area-id peer-interface interface-name],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) virtual-link],
[edit logical-systems logical-system-name routing-instances routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit protocols (ospf | ospf3)],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols (ospf | ospf3) virtual-link],
[edit protocols ospf area area-id peer-interface interface-name],
[edit protocols ospf area area-id peer-interface interface-name],
[edit protocols ospf area area-id virtual-link neighbor-id router-id transit-area area-id],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) virtual-link],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Disable OSPF, an OSPF interface, or an OSPF virtual link.

By default, control packets sent to the remote end of a virtual link must be forwarded using the default topology. In addition, the transit area path consists only of links that
are in the default topology. You can disable a virtual link for a configured topology, but not for a default topology. Include the `disable` statement at the [edit protocols ospf area area-id virtual-link neighbor-id router-id transit-area area-id topology name] hierarchy level.

**NOTE:** If you disable the virtual link by including the `disable` statement at the [edit protocols ospf area area-id virtual-link neighbor-id router-id transit-area area-id] hierarchy level, you disable the virtual link for all topologies, including the default topology. You cannot disable the virtual link only in the default topology.

**Default**
The configured object is enabled (operational) unless explicitly disabled.

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- *OSPF Configuration Overview*
- *Configuring RSVP and OSPF for LMP Peer Interfaces*

---

### domain-id

**Syntax**
domain-id domain-id;

**Hierarchy Level**
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
- [edit routing-instances routing-instance-name protocols (ospf | ospf3)]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Specify a domain ID for a route. The domain ID identifies the OSPF domain from which the route originated.

**Options**
- **domain-id**—You can specify either an IP address or an IP address and a local identifier using the following format: `ip-address:local-identifier`. If you do not specify a local identifier with the IP address, the identifier is assumed to have a value of 0.

**Default:** If the router ID is not configured in the routing instance, the router ID is derived from an interface address belonging to the routing instance.

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- *Configuring Routing Between PE and CE Routers in Layer 3 VPNs*
# domain-vpn-tag

**Syntax**

```plaintext
domain-vpn-tag number;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Set a virtual private network (VPN) tag for OSPFv2 external routes generated by the provider edge (PE) routing device.

**Options**

- `number`—VPN tag.

**Required Privilege**

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring Routing Between PE and CE Routers in Layer 3 VPNs](#)
export (Protocols OSPF)

Syntax

```
export [policy-names];
```

Hierarchy Level

- `[edit logical-systems logical-system-name protocols (ospf | ospf3)]`
- `[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`
- `[edit protocols (ospf | ospf3)]`
- `[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`
- `[edit routing-instances routing-instance-name protocols (ospf | ospf3)]`
- `[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for the `realm` statement introduced in Junos OS Release 9.2.
- Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Apply one or more policies to routes being exported from the routing table into OSPF.

Options

- `policy-names`—Name of one or more policies.

Required Privilege

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation

- [Understanding OSPF Routing Policy](#)
- [Import and Export Policies for Network Summaries Overview](#)
- [import on page 2841](#)
- [Routing Policy Feature Guide for Routing Devices](#)
external-preference (Protocols OSPF)

**Syntax**

```
external-preference preference;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast)]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Set the route preference for OSPF external routes.

**Options**

- `preference`—Preference value.
  - **Range:** 0 through 4,294,967,295 ($2^{32} - 1$)
  - **Default:** 150

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Controlling OSPF Route Preferences
- preference on page 2860
graceful-restart (Protocols OSPF)

Syntax
graceful-restart {
  disable;
  helper-disable (standard | restart-signaling | both);
  no-strict-lsa-checking;
  notify-duration seconds;
  restart-duration seconds;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf]

Release Information
Statement introduced before Junos OS Release 7.4.
Support for the no-strict-lsa-checking statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the helper mode standard, restart-signaling, and both options introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Configure graceful restart for OSPF.

Graceful restart allows a routing device to restart with minimal effects to the network, and is enabled for all routing protocols at the [edit routing-options] hierarchy level.

Options
disable—Disable graceful restart for OSPF.

helper-disable (standard | restart-signaling | both)—Disable helper mode for graceful restart. When helper mode is disabled, a device cannot help a neighboring device that is attempting to restart. Beginning with Junos OS Release 11.4, you can configure restart signaling-based helper mode for OSPFv2 graceful restart configurations. The standard, restart-signaling, and both options are only supported for OSPFv2. Specify standard to disable helper mode for standard graceful restart (based on RFC 3623). Specify restart-signaling to disable helper mode for restart signaling-based graceful restart (based on RFC 4811, RFC 4812, and RFC 4813). Specify both to disable helper mode for both standard and restart signaling-based graceful restart. The last committed statement takes precedence over the previously configured statement.

Default: Helper mode is enabled by default. For OSPFv2, both standard and restart-signaling based helper modes are enabled by default.

no-strict-lsa-checking—Disable strict OSPF link-state advertisement (LSA) checking to prevent the termination of graceful restart by a helping router. LSA checking is enabled by default.

NOTE: The helper-disable statement and the no-strict-lsa-checking statement cannot be configured at the same time. If you attempt to configure both
Statements at the same time, the routing device displays a warning message when you enter the `show protocols (ospf | ospf3)` command.

**notify-duration seconds**—Estimated time needed to send out purged grace LSAs over all the interfaces.  
**Range:** 1 through 3600 seconds  
**Default:** 30 seconds

**restart-duration seconds**—Estimated time needed to reacquire a full OSPF neighbor from each area.  
**Range:** 1 through 3600 seconds  
**Default:** 180 seconds

**Required Privilege Level**  
- **routing**—To view this statement in the configuration.  
- **routing-control**—To add this statement to the configuration.

**Related Documentation**  
- [Example: Configuring Graceful Restart for OSPF](#)  
- [Example: Configuring the Helper Capability Mode for OSPFv2 Graceful Restart](#)  
- [Example: Configuring the Helper Capability Mode for OSPFv3 Graceful Restart](#)  
- [Example: Disabling Strict LSA Checking for OSPF Graceful Restart](#)  
- [Configuring Graceful Restart for QFabric Systems](#)  
- [Junos OS High Availability Library for Routing Devices](#)
**hello-interval (Protocols OSPF)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>hello-interval seconds;</th>
</tr>
</thead>
</table>
| **Hierarchy Level** | [edit logical-systems logical-system-name protocols ospf area area-id peer-interface interface-name],  
|               | [edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],  
|               | [edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id virtual-link],  
|               | [edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],  
|               | [edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],  
|               | [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],  
|               | [edit protocols ospf area area-id peer-interface interface-name],  
|               | [edit protocols (ospf | ospf3) area area-id interface interface-name],  
|               | [edit protocols (ospf | ospf3) area area-id virtual-link],  
|               | [edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],  
|               | [edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],  
|               | [edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name] |

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**
Specify how often the routing device sends hello packets out the interface. The hello interval must be the same for all routing devices on a shared logical IP network.

**Options**
- **seconds**—Time between hello packets, in seconds.
  - **Range:** 1 through 255 seconds
  - **Default:** 10 seconds (broadcast and point-to-point networks); 30 seconds (nonbroadcast multiple access [NBMA] networks)

**Required Privilege Level**
- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring OSPF Timers*
- *Configuring RSVP and OSPF for LMP Peer Interfaces*
- *dead-interval on page 2828*
ignore-lsp-metrics

Syntax
ignore-lsp-metrics;

Hierarchy Level
[edit logical-systems logical-system-name protocols ospf traffic-engineering shortcuts],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf traffic-engineering shortcuts],
[edit protocols ospf traffic-engineering],
[edit routing-instances routing-instance-name protocols ospf traffic-engineering shortcuts]

Release Information
Statement introduced in Junos OS Release 7.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for (OSPFv3) introduced in Junos OS Release 9.4.
Support for (OSPFv3) introduced in Junos OS Release 9.4 for EX Series switches.

Description
Ignore RSVP LSP metrics in OSPF traffic engineering shortcut calculations.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Enabling OSPF Traffic Engineering Support
import (Protocols OSPF)

Syntax

import [ policy-names ];

Hierarchy Level

[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Filter OSPF routes from being added to the routing table.

Options

policy-names—Name of one or more policies.

Required Privilege

Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Understanding OSPF Routing Policy
• Import and Export Policies for Network Summaries Overview
  • export on page 2835
  • Routing Policy Feature Guide for Routing Devices
inter-area-prefix-export

**Syntax**

inter-area-prefix-export [ policy-names ];

**Hierarchy Level**

[edit logical-systems logical-system-name protocols ospf3 area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit protocols ospf3 area area-id],
[edit protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit routing-instances routing-instance-name protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit routing-instances routing-instance-name protocols ospf3 realm (ip4-unicast | ipv4-multicast | ipv6-multicast) area area-id],

**Release Information**

Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Apply an export policy for OSPFv3 to specify which interarea prefix link-state advertisements (LSAs) are flooded into an area.

**Options**

- *policy-name*—Name of a policy configured at the [edit policy-options policy-statement policy-name term term-name] hierarchy level.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Import and Export Policies for Network Summaries Overview
- inter-area-prefix-import on page 2843
- Routing Policy Feature Guide for Routing Devices
**inter-area-prefix-import**

**Syntax**
```
inter-area-prefix-import [ policy-names ];
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols ospf3 area area-id],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit protocols ospf3 area area-id],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit routing-instances routing-instance-name protocols ospf3 area area-id]
```

**Release Information**
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**
Apply an import policy for OSPFv3 to specify which routes learned from an area are used to generate interarea prefixes into other areas.

**Options**
- `policy-name`—Name of a policy configured at the `[edit policy-options policy-statement policy-name term term-name]` hierarchy level.

**Required Privilege**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- *Import and Export Policies for Network Summaries Overview*
- *inter-area-prefix-export on page 2842*
- *Routing Policy Feature Guide for Routing Devices*
interface (Protocols OSPF)

```plaintext
Syntax

interface interface-name {
  disable;
  authentication key <key-id identifier>;
  bfd-liveness-detection {
    authentication {
      algorithm algorithm-name;
      key-chain key-chain-name;
      loose-check;
    }
    detection-time {
      threshold milliseconds;
    }
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    transmit-interval {
      threshold milliseconds;
      minimum-interval milliseconds;
    }
    multiplier number;
  }
  dead-interval seconds;
  demand-circuit;
  hello-interval seconds;
  ipsec-sa name;
  interface-type type;
  ldp-synchronization {
    disable;
    hold-time seconds;
  }
  metric metric;
  neighbor address <eligible>;
  no-interface-state-traps;
  passive;
  poll-interval seconds;
  priority number;
  retransmit-interval seconds;
  te-metric metric;
  topology (ipv4-multicast | name) {
    metric metric;
  }
  transmit-delay seconds;
  transmit-interval seconds;
}

Hierarchy Level

[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit protocols (ospf | ospf3) area area-id],
```

---

Copyright © 2013, Juniper Networks, Inc.
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the topology statement introduced in Junos OS Release 9.0.
Support for the topology statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.
Support for the no-interface-state-traps statement introduced in Junos OS Release 10.3.
This statement is supported only for OSPFv2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Enable OSPF routing on a routing device interface.

You must include at least one interface statement in the configuration to enable OSPF on the routing device.

Options
interface-name—Name of the interface. Specify the interface by IP address or interface name for OSPFv2, or only the interface name for OSPFv3. Using both the interface name and IP address of the same interface produces an invalid configuration. To configure all interfaces, you can specify all. Specifying a particular interface and all produces an invalid configuration.

NOTE: For nonbroadcast interfaces, specify the IP address of the nonbroadcast interface as interface-name.

The remaining statements are explained separately.

NOTE: You cannot run both OSPF and ethernet-tcc encapsulation between two Juniper Networks routing devices.

Required Privilege
Level
routing—To view this statement in the configuration.
routeing-control—To add this statement to the configuration.
Related Documentation

- OSPF Configuration Overview
- Example: Configuring Multitopology Routing Based on Applications
- Example: Configuring Multitopology Routing Based on a Multicast Source
- Example: Configuring Multiple Address Families for OSPFv3
- neighbor
interface-type (Protocols OSPF)

Syntax

```
interface-type (nbma | p2mp | p2p);
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area area-id interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-multicast | ipv4-unicast | ipv6-multicast) area area-id interface interface-name],
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 for interface type p2p only introduced in Junos OS Release 9.4. You cannot configure other interface types for OSPFv3.
Support for OSPFv3 for interface type p2p only introduced in Junos OS Release 9.4 for EX Series switches.

Description

Specify the type of interface.

By default, the software chooses the correct interface type based on the type of physical interface. Therefore, you should never have to set the interface type. The exception to this is for NBMA interfaces, which default to an interface type of point-to-multipoint. To have these interfaces explicitly run in Nonbroadcast multiaccess (NBMA) mode, configure the nbma interface type, using the IP address of the local ATM interface.

In Junos OS Release 9.3 and later, a point-to-point interface can be an Ethernet interface without a subnet.

Default

The software chooses the correct interface type based on the type of physical interface.

Options

- **nbma** (OSPFV2 only)—Nonbroadcast multiaccess (NBMA) interface.
- **p2mp** (OSPFV2 only)—Point-to-multipoint interface.
- **p2p**—Point-to-point interface.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.
Related Documentation

- About OSPF Interfaces
- Example: Configuring an OSPFv2 Interface on a Nonbroadcast Multiaccess Network

**lsp-metric-into-summary**

**Syntax**
```
lsp-metric-into-summary;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols (ospf | ospf3) traffic-engineering shortcuts],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) traffic-engineering shortcuts],
[edit protocols (ospf | ospf3) traffic-engineering shortcuts],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) traffic-engineering shortcuts]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for OSPFv3 (ospf3) introduced in Junos OS Release 9.4.
Support for OSPFv3 (ospf3) introduced in Junos OS Release 9.4 for EX Series switches.

**Description**
Advertise the LSP metric in summary LSAs.

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- OSPF Support for Traffic Engineering
- Example: Enabling OSPF Traffic Engineering Support
**metric (Protocols OSPF Interface)**

**Syntax**

```
metric metric;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols ospf area area-id interface interface-name topology (ipv4-multicast | name)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf area area-id id interface interface-name shaw-link-remote],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols ospf area area-id interface interface-name topology (ipv4-multicast | name)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf area area-id id interface interface-name shaw-link-remote],
[edit routing-instances routing-instance-name protocols ospf area area-id interface interface-name topology (ipv4-multicast | name)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for Multitopology Routing introduced in Junos OS Release 9.0.
Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Specify the cost of an OSPF interface. The cost is a routing metric that is used in the link-state calculation.

To set the cost of routes exported into OSPF, configure the appropriate routing policy.

**Options**

- **metric**—Cost of the route.

  **Range:** 1 through 65,535

  **Default:** By default, the cost of an OSPF route is calculated by dividing the reference-bandwidth value by the bandwidth of the physical interface. Any specific value you configure for the `metric` overrides the default behavior of using the reference-bandwidth value to calculate the cost of the route for that interface.
Required Privilege
Level routing—To view this statement in the configuration.
          routing-control—To add this statement to the configuration.

Related Documentation
• Example: Controlling the Cost of Individual OSPF Network Segments
• Example: Configuring OSPFv2 Sham Links
• Example: Configuring Multitopology Routing Based on Applications
• Example: Configuring Multitopology Routing Based on a Multicast Source
• bandwidth-based-metrics on page 2822
• reference-bandwidth on page 2864
**metric-type**

**Syntax**

```
metric-type type;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit routing-instances routing-instances protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for the `realm` statement introduced in Junos OS Release 9.2.
- Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Specify the external metric type for the default LSA.

The configured metric determines the method used to compute the cost to a destination:

- The Type 1 external metric is equivalent to the link-state metric. The path cost uses the advertised external path cost and the path cost to the AS boundary router (the route is equal to the sum of all internal costs and the external cost).
- The Type 2 external metric uses the cost assigned by the AS boundary router (the route is equal to the external cost alone). By default, OSPF uses the Type 2 external metric.

**Options**

```
type—Metric type: 1 or 2
```

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- *OSPF Areas and Router Functionality Overview*
- *Example: Configuring OSPF Not-So-Stubby Areas*
no-nssa-abr

Syntax  

```  no-nssa-abr;  ```

Hierarchy Level  

```  [edit logical-systems logical-system-name protocols (ospf | ospf3)],  ```

```  [edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],  ```

```  [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],  ```

```  [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],  ```

```  [edit protocols (ospf | ospf3)],  ```

```  [edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],  ```

```  [edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],  ```

```  [edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],  ```

Release Information  

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  

Disable exporting Type 7 link-state advertisements into not-so-stubby-areas (NSSAs) for an autonomous system boundary router (ASBR) or an area border router (ABR).

Required Privilege Level  

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation  

- Example: Configuring OSPF Not-So-Stubby Areas
## no-rfc-1583

**Syntax**  
```
no-rfc-1583;
```

**Hierarchy Level**  
```
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]
```

**Release Information**  
Statement introduced in Junos OS Release 8.5.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Support for the `realm` statement introduced in Junos OS Release 9.2.  
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**  
Disable compatibility with RFC 1583, OSPF Version 2. If the same external destination is advertised by AS boundary routers that belong to different OSPF areas, disabling compatibility with RFC 1583 can prevent routing loops.

**Default**  
Compatibility with RFC 1583 is enabled by default.

**Required Privilege Level**  
```
routing—To view this statement in the configuration.
routeing-control-level—To add this statement to the configuration.
```

**Related Documentation**  
- Example: Disabling OSPFv2 Compatibility with RFC 1583
**nssa**

**Syntax**

```
 nssa {
    area-range network/mask-length <restrict> <exact> <override-metric metric>;
    default-lsa {
        default-metric metric;
        metric-type type;
        type-7;
    }
    (no-summaries | summaries);
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3) area area-id],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Configure a not-so-stubby area (NSSA). An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas.

You cannot configure an area as being both a stub area and an NSSA.

The remaining statements are explained separately.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- OSPF Areas and Router Functionality Overview
- Example: Configuring OSPF Not-So-Stubby Areas
- stub on page 2871
### ospf

**Syntax**  
ospf {...}

**Hierarchy Level**  
[edit logical-systems logical-system-name protocols],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols],  
[edit protocols],  
[edit routing-instances routing-instance-name protocols]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**  
Enable OSPF routing on the routing device.

You must include the ospf statement to enable OSPF on the routing device.

**Default**  
OSPF is disabled on the routing device.

**Required Privilege Level**  
routing—to view this statement in the configuration.  
routing-control—to add this statement to the configuration.

**Related Documentation**  
- OSPF Configuration Overview  
- [edit protocols ospf] Hierarchy Level
ospf3

Syntax

ospf3 { ... }

Hierarchy Level

[edit logical-systems logical-system-name protocols],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols],
[edit protocols],
[edit routing-instances routing-instance-name protocols]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable OSPFv3 routing on the routing device.

You must include the ospf3 statement to enable OSPFv3.

Default

OSPFv3 is disabled on the routing device.

Required Privilege

Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• OSPF Configuration Overview
• [edit protocols ospf3] Hierarchy Level
overload (Protocols OSPF)

Syntax
overload {
    timeout seconds;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf topology (default | ipv4-multicast | name)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf topology (default | ipv4-multicast | name)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf topology (default | ipv4-multicast | name)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf topology (default | ipv4-multicast | name)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for Multitopology Routing introduced in Junos OS Release 9.0.
Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure the local routing device so that it appears to be overloaded. You might do this when you want the routing device to participate in OSPF routing, but do not want it to be used for transit traffic.

NOTE: Traffic destined to directly attached interfaces continues to reach the routing device.

Options
timeout seconds—(Optional) Number of seconds at which the overloading is reset. If no timeout interval is specified, the routing device remains in overload state until the overload statement is deleted or a timeout is set.

Range: 60 through 1800 seconds
Default: 0 seconds
NOTE: Multitopology Routing does not support the timeout option.

Required Privilege
Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring OSPF to Make Routing Devices Appear Overloaded
- Example: Configuring Multitopology Routing Based on Applications
- Example: Configuring Multitopology Routing Based on a Multicast Source
passive (Protocols OSPF)

**Syntax**

```
passive {
  traffic-engineering {
    remote-node-id address;
  }
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast | ipv6-multicast) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast | ipv6-multicast) area area-id interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

traffic-engineering and remote-node-id address statements introduced in Junos OS Release 8.0.

traffic-engineering and remote-node-id address statements introduced in Junos OS Release 8.0 for EX Series switches.

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Support for the realm statement introduced in Junos OS Release 9.2.

Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Advertise the direct interface addresses on an interface without actually running OSPF on that interface. A passive interface is one for which the address information is advertised as an internal route in OSPF, but on which the protocol does not run.

To configure an interface in OSPF passive traffic engineering mode, include the traffic-engineering statement. Configuring OSPF passive traffic engineering mode enables the dynamic discovery of OSPF AS boundary routers.

Enable OSPF on an interface by including the interface statement at the [edit protocols (ospf | ospf3) area area-id] or the [edit routing-instances routing-instance-name protocols ospf area area-id] hierarchy levels. Disable it by including the disable statement. To prevent OSPF from running on an interface, include the passive statement. These three states are mutually exclusive.

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.
Related Documentation

- Example: Configuring a Passive OSPF Interface
- Example: Configuring OSPF Passive Traffic Engineering Mode
- disable on page 2832

preference (Protocols OSPF)

Syntax

```
preference preference;
```

Hierarchy Level

[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the `realm` statement introduced in Junos OS Release 9.2.
Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Set the route preference for OSPF internal routes.

Options

- `preference`—Preference value.
  
  **Range:** 0 through 4,294,967,295 ($2^{32} - 1$)
  
  **Default:** 10

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Controlling OSPF Route Preferences
- external-preference on page 2836
prefix-export-limit (Protocols OSPF)

Syntax  
prefix-export-limit *number*;

Hierarchy Level  
[edit logical-systems *logical-system-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* protocols ospf topology (default | ipv4-multicast | name)],
[edit logical-systems *logical-system-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | name)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf topology (default | ipv4-multicast | name)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances *routing-instance-name* protocols (ospf | ospf3)],
[edit routing-instances *routing-instance-name* protocols ospf topology (default | ipv4-multicast | name)],
[edit routing-instances *routing-instance-name* protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for Multitopology Routing introduced in Junos OS Release 9.0.
Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure a limit to the number of prefixes exported into OSPF.

Options
number—Prefix limit.

Range: 0 through 4,294,967,295 (2^32 – 1)

Default: None

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Limiting the Number of Prefixes Exported to OSPF
• Example: Configuring Multitopology Routing Based on Applications
• Example: Configuring Multitopology Routing Based on a Multicast Source
priority (Protocols OSPF)

Syntax

```
priority number;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) | area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) | area area-id interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) | area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) | area area-id interface interface-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Specify the routing device’s priority for becoming the designated routing device. The routing device that has the highest priority value on the logical IP network or subnet becomes the network’s designated router. You must configure at least one routing device on each logical IP network or subnet to be the designated router. You also should specify a routing device’s priority for becoming the designated router on point-to-point interfaces.

Options

```
number—Routing device’s priority for becoming the designated router. A priority value of 0 means that the routing device never becomes the designated router. A value of 1 means that the routing device has the least chance of becoming a designated router.
```

Range: 0 through 255
Default: 128

Required Privilege Level

```
routing—to view this statement in the configuration.
```

```
routing-control—to add this statement to the configuration.
```

Related Documentation

- OSPF Designated Router Overview
- Example: Controlling OSPF Designated Router Election
realm

Syntax  realm (ipv4-unicast | ipv4-multicast | ipv6-unicast) {
  area area-id {
    interface interface-name;
  }
}

Hierarchy Level  [edit logical-systems logical-system-name protocols ospf3],
  [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3],
  [edit protocols ospf3],
  [edit routing-instances routing-instance-name protocols ospf3]

  Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description  Configure OSPFv3 to advertise address families other than unicast IPv6. Junos OS maps each address family you configure to a separate realm with its own set of neighbors and link-state database.

Options  ipv4-unicast—Configure a realm for IPv4 unicast routes.
  ipv4-multicast—Configure a realm for IPv4 multicast routes.
  ipv6-multicast—Configure a realm for IPv6 multicast routes.

The remaining statements are explained separately.

Required Privilege Level  routing—to view this statement in the configuration.
  routing-control—to add this statement to the configuration.

Related Documentation  • Example: Configuring Multiple Address Families for OSPFv3
reference-bandwidth (Protocols OSPF)

**Syntax**
```
reference-bandwidth reference-bandwidth;
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for the `realm` statement introduced in Junos OS Release 9.2.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Set the reference bandwidth used in calculating the default interface cost. The cost is calculated using the following formula:

\[
\text{cost} = \frac{\text{ref-bandwidth}}{\text{bandwidth}}
\]

**Options**
- `reference-bandwidth`—Reference bandwidth, in bits per second.
  - **Range:** 9600 through 1,000,000,000,000 bits
  - **Default:** 100 Mbps (100,000,000 bits)

**NOTE:** The default behavior is to use the reference-bandwidth value to calculate the cost of OSPF interfaces. You can override this behavior for any OSPF interface by configuring a specific cost with the `metric` statement.

**Required Privilege Level**
- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

**Related Documentation**
- Example: Controlling the Cost of Individual OSPF Network Segments
- metric on page 2849
retransmit-interval (OSPF)

**Syntax**
```yaml
retransmit-interval seconds;
```

**Hierarchy Level**
- `edit logical-systems logical-system-name protocols ospf area area-id peer-interface interface-name`,
- `edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name`,
- `edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id virtual-link`,
- `edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name`,
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name`,
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name`,
- `edit protocols ospf area area-id peer-interface interface-name`,
- `edit protocols (ospf | ospf3) area area-id interface interface-name`,
- `edit protocols (ospf | ospf3) area area-id virtual-link`,
- `edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name`,
- `edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id interface interface-name`,
- `edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name`,
- `edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name`.

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for the `realm` statement introduced in Junos OS Release 9.2.
- Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**
Specify how long the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements (LSAs) to an interface’s neighbors.

**Options**
- **seconds**—Interval to wait.
  - **Range:** 1 through 65,535 seconds
  - **Default:** 5 seconds

**NOTE:** You must configure LSA retransmit intervals to be equal to or greater than 3 seconds to avoid triggering a retransmit trap, because Junos OS delays LSA acknowledgments by up to 2 seconds.
Required Privilege  routing—To view this statement in the configuration.
Level routing-control—To add this statement to the configuration.

Related Documentation  •  Example: Configuring OSPF Timers
  •  Configuring RSVP and OSPF for LMP Peer Interfaces

rib-group (Protocols OSPF)

Syntax  rib-group group-name;

Hierarchy Level  [edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3)],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Install routes learned from OSPF routing instances into routing tables in the OSPF routing table group.

Options  group-name—Name of the routing table group.

Required Privilege  routing—To view this statement in the configuration.
Level routing-control—To add this statement to the configuration.

Related Documentation  •  Example: Exporting Specific Routes from One Routing Table Into Another Routing Table
  •  Example: Importing Direct and Static Routes Into a Routing Instance
  •  Understanding Multiprotocol BGP
  •  interface-routes on page 3071
  •  rib-group on page 3106
## route-type-community

**Syntax**  
route-type-community (iana | vendor);

**Hierarchy Level**  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],  
[edit routing-instances routing-instance-name protocols (ospf | ospf3)]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**  
Specify an extended community value to encode the OSPF route type. Each extended community is coded as an eight-octet value. This statement sets the most significant bit to either an IANA or vendor-specific route type.

**Options**  
- **iana**—Encode a route type with the value **0x0306**. This is the default value.  
- **vendor**—Encode the route type with the value **0x8000**.

**Required Privilege**  
- **routing**—To view this statement in the configuration.  
- **routing-control**—To add this statement to the configuration.

**Related Documentation**  
- Configuring Routing Between PE and CE Routers in Layer 3 VPNs
shortcuts (Protocols OSPF)

Syntax
```
shortcuts {
    lsp-metric-into-summary;
}
```

Hierarchy Level
```
[edit logical-systems logical-system-name protocols (ospf | ospf3) traffic-engineering],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) traffic-engineering],
[edit protocols (ospf | ospf3) traffic-engineering],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) traffic-engineering]
```

Release Information
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for OSPFv3 (ospf3) introduced in Junos OS Release 9.4.
- Support for OSPFv3 (ospf3) introduced in Junos OS Release 9.4 for EX Series switches.

Description
Configure OSPF to use MPLS label-switched paths (LSPs) as shortcut next hops. By default, shortcut routes calculated through OSPFv2 are installed in the inet.3 routing table, and shortcut routes calculated through OSPFv3 are installed in the inet6.3 routing table.

Required Privilege
- Level routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Example: Enabling OSPF Traffic Engineering Support
**spf-options (Protocols OSPF)**

**Syntax**

```plaintext
code
spf-options {
    delay milliseconds;
    holddown milliseconds;
    rapid-runs number;
}
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols (ospf | ospf3)]`
- `[edit logical-systems logical-system-name protocols ospf topology (default | ipv4-multicast | name)]`
- `[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf | ospf3)]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf topology (default | ipv4-multicast | name)]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`
- `[edit protocols (ospf | ospf3)]`
- `[edit protocols ospf topology (default | ipv4-multicast | name)]`
- `[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`
- `[edit routing-instances routing-instance-name protocols ospf | ospf3)]`
- `[edit routing-instances routing-instance-name protocols ospf topology (default | ipv4-multicast | name)]`
- `[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]`

**Release Information**

- Statement introduced in Junos OS Release 8.5.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for Multitopology Routing introduced in Junos OS Release 9.0.
- Support for Multitopology Routing introduced in Junos OS Release 9.0 for EX Series switches.
- Support for the `realm` statement introduced in Junos OS Release 9.2.
- Support for the `realm` statement introduced in Junos OS Release 9.2 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure options for running the shortest-path-first (SPF) algorithm. You can configure the following:

- A delay for when to run the SPF algorithm after a network topology change is detected.
- The maximum number of times the SPF algorithm can run in succession.
- A hold-down interval after the SPF algorithm runs the maximum number of times.

Running the SPF algorithm is usually the beginning of a series of larger system-wide events. For example, the SPF algorithm can lead to interior gateway protocol (IGP) prefix changes, which then lead to BGP nexthop resolution changes. Consider what happens if there are rapid link changes in the network. The local routing device can become overwhelmed. This is why it sometimes makes sense to throttle the scheduling of the SPF algorithm.
Options  delay milliseconds—Time interval between the detection of a topology change and when
the SPF algorithm runs.
Range: 50 through 8000 milliseconds
Default: 200 milliseconds

holddown milliseconds—Time interval to hold down, or to wait before a subsequent SPF
algorithm runs after the SPF algorithm has run the configured maximum number of
times in succession.
Range: 2000 through 20,000 milliseconds
Default: 5000 milliseconds

rapid-runs number—Maximum number of times the SPF algorithm can run in succession.
After the maximum is reached, the hold down interval begins.
Range: 1 through 10
Default: 3

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring SPF Algorithm Options for OSPF
• Example: Configuring Multitopology Routing Based on Applications
• Example: Configuring Multitopology Routing Based on a Multicast Source
stub

Syntax

stub <default-metric metric> <(no-summaries | summaries)>;

Hierarchy Level

[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit protocols (ospf | ospf3) area area-id],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

Description

Specify that this area not be flooded with AS external link-state advertisements (LSAs).
You must include the stub statement when configuring all routing devices that are in the stub area.

The backbone cannot be configured as a stub area.

You cannot configure an area to be both a stub area and a not-so-stubby area (NSSA).

Options

no-summaries—(Optional) Do not advertise routes into the stub area. If you include the default-metric option, only the default route is advertised.

summaries—(Optional) Flood summary LSAs into the stub area.

The remaining statement is explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• OSPF Areas and Router Functionality Overview
• Example: Configuring OSPF Stub and Totally Stubby Areas
• nssa on page 2854
summaries

Syntax  (summaries | no-summaries);

Hierarchy Level  [edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id nssa],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa],
[edit protocols (ospf | ospf3) area area-id nssa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

Description  Configure whether or not area border routers advertise summary routes into an not-so-stubby area (NSSA):

- summaries—Flood summary link-state advertisements (LSAs) into the NSSA.
- no-summaries—Prevent area border routers from advertising summaries into an NSSA. If default-metric is configured for an NSSA, a Type 3 LSA is injected into the area by default.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  • OSPF Areas and Router Functionality Overview
• Example: Configuring OSPF Not-So-Stubby Areas
• nssa on page 2854
• stub on page 2871
traceoptions (Protocols OSPF)

Syntax

```
traceoptions {
  file filename <files number> <size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols (ospf | ospf3)],
- [edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
- [edit protocols (ospf | ospf3)],
- [edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)],
- [edit routing-instances routing-instance-name protocols (ospf | ospf3)],
- [edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast)]

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for the `realm` statement introduced in Junos OS Release 9.2.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure OSPF protocol-level tracing options.

To specify more than one tracing operation, include multiple `flag` statements.

NOTE: The traceoptions statement is not supported on QFabric systems.

Default

The default OSPF protocol-level tracing options are those inherited from the routing protocols `traceoptions` statement included at the `[edit routing-options]` hierarchy level.

Options

- `disable`—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as `all`.

- `file filename`—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. We recommend that you place OSPF tracing output in the file `ospf-log`.

- `files number`—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.
If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

**Range:** 2 through 1000 files  
**Default:** 10 files

**flag**—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

**OSPF Tracing Flags**

- **database-description**—Database description packets, which are used in synchronizing the OSPF and OSPFv3 topological database.
- **error**—OSPF and OSPFv3 error packets.
- **event**—OSPF and OSPFv3 state transitions.
- **flooding**—Link-state flooding packets.
- **graceful-restart**—Graceful-restart events.
- **hello**—Hello packets, which are used to establish neighbor adjacencies and to determine whether neighbors are reachable.
- **ldp-synchronization**—Synchronization events between OSPF and LDP.
- **lsa-ack**—Link-state acknowledgment packets, which are used in synchronizing the OSPF topological database.
- **lsa-analysis**—Link-state analysis. Specific to the Juniper Networks implementation of OSPF, Junos OS performs LSA analysis before running the shortest-path-first (SPF) algorithm. LSA analysis helps to speed the calculations performed by the SPF algorithm.
- **lsa-request**—Link-state request packets, which are used in synchronizing the OSPF topological database.
- **lsa-update**—Link-state updates packets, which are used in synchronizing the OSPF topological database.
- **nsr-synchronization**—Nonstop routing synchronization events.
- **on-demand**—Trace demand circuit extensions.
- **packet-dump**—Content of selected packet types.
- **packets**—All OSPF packets.
- **restart-signaling**—(OSPFv2 only) Restart-signaling graceful restart events.
- **spf**—Shortest-path-first (SPF) calculations.

**Global Tracing Flags**
• **all**—All tracing operations.
• **general**—A combination of the normal and route trace operations.
• **normal**—All normal operations. If you do not specify this option, only unusual or abnormal operations are traced.
• **policy**—Policy operations and actions.
• **route**—Routing table changes.
• **state**—State transitions.
• **task**—Routing protocol task processing.
• **timer**—Routing protocol timer processing.

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

• **detail**—Detailed trace information.
• **receive**—Packets being received.
• **send**—Packets being transmitted.

**no-world-readable**—(Optional) Prevent any user from reading the log file.

**size** size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

  If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

**Syntax:** xk to specify KB, xm to specify MB, or xg to specify GB

**Range:** 10 KB through the maximum file size supported on your system

**Default:** 128 KB

**world-readable**—(Optional) Allow any user to read the log file.

**Required Privilege Level**
- routing and trace—To view this statement in the configuration.
- routing-control and trace-control—To add this statement to the configuration.

**Related Documentation**
- Example: Tracing OSPF Protocol Traffic
traffic-engineering (OSPF)

Syntax

```
traffic-engineering {
    <advertise-unnumbered-interfaces>;
    <credibility-protocol-preference>;
    ignore-lsp-metrics;
    multicast-rpf-routes;
    no-topology;
    shortcuts {
        lsp-metric-into-summary;
    }
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols (ospf | ospf3)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (ospf | ospf3)],
[edit protocols (ospf | ospf3)],
[edit routing-instances routing-instance-name protocols (ospf | ospf3)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
- `multicast-rpf-routes` option introduced in Junos OS Release 7.5.
- `advertise-unnumbered-interfaces` option introduced in Junos OS Release 8.5.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for OSPFv3 (`ospf3`) introduced in Junos OS Release 9.4.
- Support for OSPFv3 (`ospf3`) introduced in Junos OS Release 9.4 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable the OSPF traffic engineering features.

Default

Traffic engineering support is disabled.

Options

- `advertise-unnumbered-interfaces`—(Optional) (OSPFv2 only) Include the link-local identifier in the link-local traffic-engineering link-state advertisement. This statement must be included on both ends of an unnumbered link to allow an ingress LER to update the link in its traffic engineering database and use it for CSPF calculations. The link-local identifier is then used by RSVP to signal unnumbered interfaces as defined in RFC 3477.

- `credibility-protocol-preference`—(Optional) (OSPFv2 only) Use the configured preference value for OSPF routes to calculate the traffic engineering database credibility value used to select IGP routes. Use this statement to override the default behavior, in which the traffic engineering database prefers IS-IS routes even if OSPF routes are configured with a lower, that is, preferred, preference value. For example, OSPF routes have a default preference value of 10, whereas IS-IS Level 1 routes have a default preference value of 15. When protocol preference is enabled, the credibility value is determined by deducting the protocol preference value from a base value of 512. Using default protocol preference values, OSPF has a credibility value of 502.
whereas IS-IS has a credibility value of 497. Because the traffic engineering database prefers IGP routes with the highest credibility value, OSPF routes are now preferred.

**multicast-rpf-routes**—(Optional) (OSPFv2 only) Install routes for multicast RPF checks into the inet.2 routing table. The inet.2 routing table consists of unicast routes used for multicast RPF lookup. RPF is an antispoofing mechanism used to check whether the packet is coming in on an interface that is also sending data back to the packet source.

NOTE: You must enable OSPF traffic engineering shortcuts to use the multicast-rpf-routes statement. You must not allow LSP advertisements into OSPF when configuring the multicast-rpf-routes statement.

**no-topology**—(Optional) (OSPFv2 only) Disable the dissemination of the link-state topology information.

The remaining statements are explained separately.

CAUTION: When the OSPF traffic engineering configuration is considerably modified, the routing table entries are deleted and the routing table is recreated. Changes to configuration that can cause this behavior include enabling or disabling:

- Traffic engineering shortcuts
- IGP shortcuts
- LDP tunneling
- Multiprotocol LSP
- Advertise summary metrics
- Multicast RPF routes

**Required Privilege**  
Level routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**  
- Example: **Enabling OSPF Traffic Engineering Support**
transit-delay (OSPF)

**Syntax**

transit-delay seconds;

**Hierarchy Level**

[edit logical-systems logical-system-name protocols ospf area area-id peer-interface interface-name],
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id interface interface-name],
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id virtual-link],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf area area-id interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit protocols ospf area area-id peer-interface interface-name],
[edit protocols (ospf | ospf3) area area-id interface interface-name],
[edit protocols (ospf | ospf3) area area-id virtual-link],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf3 area area-id interface interface-name],
[edit routing-instances routing-instance-name protocols ospf area area-id virtual-link],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id interface interface-name]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Set the estimated time required to transmit a link-state update on the interface. When calculating this time, make sure to account for transmission and propagation delays.

You should never have to modify the transit delay time.

**Options**

seconds—Estimated time, in seconds.

Range: 1 through 65,535 seconds

Default: 1 second

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring OSPF Timers
- Configuring RSVP and OSPF for LMP Peer Interfaces
type-7

Syntax  

type-7;

Hierarchy Level  

[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id nssa
default-lsa],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast |
ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols
(ospf | ospf3) area area-id nssa default-lsa],
[edit logical-systems logical-system-name protocols ospf3 realm (ipv4-unicast |
ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa],
[edit protocols (ospf | ospf3) area area-id nssa default-lsa],
[edit protocols ospf3 realm (ipv4-unicast | ipv4-multicast | ipv6-multicast) area area-id nssa
default-lsa],
[edit routing-instances routing-instance-name protocols (ospf | ospf3) area area-id nssa
default-lsa],
[edit routing-instances routing-instance-name protocols ospf3 realm (ipv4-unicast |
ipv4-multicast | ipv6-multicast) area area-id nssa default-lsa]

Release Information  

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the realm statement introduced in Junos OS Release 9.2.
Support for the realm statement introduced in Junos OS Release 9.2 for EX Series switches.

Description  

Flood Type 7 default link-state advertisements (LSAs) if the nosummaries statement is configured.

By default, when the nosummaries statement is configured, a Type 3 LSA is injected into
not-so-stubby areas (NSSAs) for Junos OS Release 5.0 and later. To support backward
compatibility with earlier Junos OS releases, include the type-7 statement. This statement
enables NSSA ABRs to advertise a Type 7 default LSA into the NSSA if you have also
included the nosummaries statement in the configuration.

Required Privilege  

Level  

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  

• OSPF Areas and Router Functionality Overview
• Example: Configuring OSPF Not-So-Stubby Areas
• nosummaries on page 2872
virtual-link

Syntax
virtual-link neighbor-id router-id transit-area area-id {
    disable;
    authentication key <key-id identifier>;
    dead-interval seconds;
    hello-interval seconds;
    ipsec-sa name;
    retransmit-interval seconds;
    transit-delay seconds;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols (ospf | ospf3) area area-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols
ospf area area-id],
[edit protocols (ospf | ospf3) area area-id],
[edit routing-instances routing-instance-name protocols ospf area area-id]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
For backbone areas only, create a virtual link to use in place of an actual physical link. All
area border routers and other routing devices on the backbone must be contiguous. If
this is not possible and there is a break in OSPF connectivity, use virtual links to create
connectivity to the OSPF backbone. When configuring virtual links, you must configure
links on the two routing devices that form the end points of the link, and both of these
routing devices must be area border routers. You cannot configure links through stub
areas.

Options
neighbor-id router-id—IP address of the routing device at the remote end of the virtual
link.

transit-area area-id—Area identifier of the area through which the virtual link transits.
Virtual links are not allowed to transit the backbone area.

The remaining statements are explained separately.

Required Privilege
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• OSPF Areas and Router Functionality Overview
• Example: Configuring OSPF Virtual Links
CHAPTER 56

Administration

- Routine Monitoring on page 2881
- Operational Commands on page 2883

Routine Monitoring

- Monitoring OSPF Routing Information on page 2881

Monitoring OSPF Routing Information

**Purpose**  Use the monitoring functionality to monitor OSPF routing information on routing devices.

**Action**  To view OSPF routing information in the J-Web interface, select Monitor > Routing > OSPF Information.

To view OSPF routing information in the CLI, enter the following CLI commands:

- `show ospf neighbor`
- `show ospf interface`
- `show ospf statistics`

**Meaning**  Table 355 on page 2881 summarizes key output fields in the OSPF routing display in the J-Web interface.

Table 355: Summary of Key OSPF Routing Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Interfaces</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface running OSPF.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: <strong>BDR, Down, DR, DRother, Loop, PtToPt, or Waiting.</strong></td>
<td>The Down state, indicating that the interface is not functioning, and PtToPt state, indicating that a point-to-point connection has been established, are the most common states.</td>
</tr>
<tr>
<td>Area</td>
<td>Number of the area that the interface is in.</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Values</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DR ID</td>
<td>Address of the area's designated device.</td>
<td></td>
</tr>
<tr>
<td>BDR ID</td>
<td>Address of the area's backup designated device.</td>
<td></td>
</tr>
<tr>
<td>Neighbors</td>
<td>Number of neighbors on this interface.</td>
<td></td>
</tr>
<tr>
<td>Adjacency Count</td>
<td>Number of devices in the area using the same area identifier.</td>
<td></td>
</tr>
<tr>
<td>Stub Type</td>
<td>The areas into which OSPF does not flood AS external advertisements</td>
<td></td>
</tr>
<tr>
<td>Passive Mode</td>
<td>In this mode the interface is present on the network but does not transmit or receive packets.</td>
<td></td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The authentication scheme for the backbone or area.</td>
<td></td>
</tr>
<tr>
<td>Interface Address</td>
<td>The IP address of the interface.</td>
<td></td>
</tr>
<tr>
<td>Address Mask</td>
<td>The subnet mask or address prefix.</td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>The maximum transmission unit size.</td>
<td></td>
</tr>
<tr>
<td>Interface Cost</td>
<td>The path cost used to calculate the root path cost from any given LAN segment is determined by the total cost of each link in the path.</td>
<td></td>
</tr>
<tr>
<td>Hello Interval</td>
<td>How often the routing device sends hello packets out of the interface.</td>
<td></td>
</tr>
<tr>
<td>Dead Interval</td>
<td>The interval during which the routing device receives no hello packets from the neighbor.</td>
<td></td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>The interval for which the routing device waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to an interface's neighbors.</td>
<td></td>
</tr>
<tr>
<td>OSPF Statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packets tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sent</td>
<td>Displays the total number of packets sent.</td>
<td></td>
</tr>
<tr>
<td>Received</td>
<td>Displays the total number of packets received.</td>
<td></td>
</tr>
<tr>
<td>Details tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flood Queue Depth</td>
<td>Number of entries in the extended queue.</td>
<td></td>
</tr>
</tbody>
</table>
Table 355: Summary of Key OSPF Routing Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Retransmits</td>
<td>Number of retransmission entries enqueued.</td>
<td></td>
</tr>
<tr>
<td>Total Database Summaries</td>
<td>Total number of database description packets.</td>
<td></td>
</tr>
<tr>
<td>OSPF Neighbors</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td>Address of the neighbor.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>State of the neighbor: Attempt, Down, Exchange, ExStart, Full, Init, Loading, or 2way.</td>
<td>Generally, only the Down state, indicating a failed OSPF adjacency, and the Full state, indicating a functional adjacency, are maintained for more than a few seconds. The other states are transitional states that a neighbor is in only briefly while an OSPF adjacency is being established.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the neighbor.</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>Priority of the neighbor to become the designated router.</td>
<td></td>
</tr>
<tr>
<td>Activity Time</td>
<td>The activity time.</td>
<td></td>
</tr>
<tr>
<td>Area</td>
<td>Area that the neighbor is in.</td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>Option bits received in the hello packets from the neighbor.</td>
<td></td>
</tr>
<tr>
<td>DR Address</td>
<td>Address of the designated router.</td>
<td></td>
</tr>
<tr>
<td>BDR Address</td>
<td>Address of the backup designated router.</td>
<td></td>
</tr>
<tr>
<td>Uptime</td>
<td>Length of time since the neighbor came up.</td>
<td></td>
</tr>
<tr>
<td>Adjacency</td>
<td>Length of time since the adjacency with the neighbor was established.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring an OSPF Network (J-Web Procedure) on page 2811
- Layer 3 Protocols Supported on EX Series Switches on page 2553

**Operational Commands**
clear (ospf | ospf3) database

**Syntax**

```
clear (ospf | ospf3) database
<advertising-router (router-id | self)>
<area area-id>
<asbrsummary>
<external>
<instance instance-name>
<inter-area-prefix>
<inter-area-router>
<intra-area-prefix>
<link-local>
<logical-system (all | logical-system-name)>
<lsa-id lsa-id>
<netsummary>
<network>
<nssa>
<opaque-area>
<purge>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<router>
```

**Syntax (EX Series Switch and QFX Series)**

```
clear (ospf | ospf3) database
<advertising-router (router-id | self)>
<area area-id>
<asbrsummary>
<external>
<instance instance-name>
<inter-area-prefix>
<inter-area-router>
<intra-area-prefix>
<link-local>
<lsa-id lsa-id>
<netsummary>
<network>
<nssa>
<opaque-area>
<purge>
<router>
```

**Release Information**

Command introduced before Junos OS Release 7.4,
- advertising-router router-id, area area-id, asbrsummary, external, inter-area-prefix, inter-area-router, intra-area-prefix, link-local, lsa-id lsa-id, netsummary, network, nssa, opaque-area, and router options added in Junos OS Release 8.3. You must use the **purge** command with these options.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- **realm** option added in Junos OS Release 9.2.
- advertising-router (router-id | self) option added in Junos OS Release 9.5.
- advertising-router (router-id | self) option introduced in Junos OS Release 9.5 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
**Description**

With the master Routing Engine, delete entries in the Open Shortest Path First (OSPF) link-state advertisement (LSA) database. With the backup Routing Engine, delete the OSPF LSA database and sync the new database with the master Routing Engine. You can also use the `purge` command with any of the options to discard rather than delete the specified LSA entries.

[CAUTION: This command is useful only for testing. Use it with care, because it causes significant network disruption.]

**Options**

- **none**—Delete all LSAs other than the system's own LSAs, which are regenerated. To resynchronize the database, the system destroys all adjacent neighbors that are in the state **EXSTART** or higher. The neighbors are then reacquired and the databases are synchronized.

  - **advertising-router (router-id | self)**—(Optional) Discard entries for the LSA entries advertised by the specified routing device or by this routing device.
  - **area area-id**—(Optional) Discard entries for the LSAs in the specified area.
  - **asbrsummary**—(Optional) Discard summary AS boundary router LSA entries.
  - **external**—(Optional) Discard external LSAs.
  - **instance instance-name**—(Optional) Delete or discard entries for the specified routing instance only.
  - **inter-area-prefix**—(OSPFv3 only) (Optional) Discard interarea prefix LSAs.
  - **inter-area-router**—(OSPFv3 only) (Optional) Discard interarea router LSAs.
  - **intra-area-prefix**—(OSPFv3 only) (Optional) Discard intra-area prefix LSAs.
  - **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
  - **link-local**—(Optional) Delete link-local LSAs.
  - **lsa-id lsa-id**—(Optional) Discard the LSA entries with the specified LSA identifier.
  - **netsummary**—(Optional) Discard summary network LSAs.
  - **network**—(Optional) Discard network LSAs.
  - **nssa**—(Optional) Discard not-so-stubby area (NSSA) LSAs.
  - **opaque-area**—(Optional) Discard opaque area-scope LSAs.
  - **realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)**—(OSPFv3 only) (Optional) Delete the entries for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.
router—(Optional) Discard router LSAs.

purge—(Optional) Discard all entries in the link-state advertisement database. All link-state advertisements are set to MAXAGE and are flooded. The database is repopulated when the originators of the link-state advertisements receive the MAXAGE link-state advertisements and reissue them.

**Required Privilege Level**
clear

**Related Documentation**
- show ospf database on page 2925
- show ospf3 database on page 2933

**List of Sample Output**
clear ospf database on page 2886

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear ospf database

```bash
user@host> clear ospf database
```
clear (ospf | ospf3) io-statistics

| Syntax | clear (ospf | ospf3) io-statistics  
|<logical-system (all | logical-system-name)> |
| Syntax (EX Series Switch and QFX Series) | clear (ospf | ospf3) io-statistics |
| Release Information | Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series. |
| Description | Clear Open Shortest Path First (OSPF) input and output statistics. |
| Options | none—Clear OSPF input and output statistics.  
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system. |
| Required Privilege Level | clear |
| List of Sample Output | clear ospf io-statistics on page 2887 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

clear ospf io-statistics

user@host> clear ospf io-statistics
clear (ospf | ospf3) neighbor

Syntax

```
clear (ospf | ospf3) neighbor
<area area-id>
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>
<neighbor>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

Syntax (EX Series Switch and QFX Series)

```
clear (ospf | ospf3) neighbor
<area area-id>
<instance instance-name>
<interface interface-name>
<neighbor>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Tear down Open Shortest Path First (OSPF) neighbor connections.

Options

```
one—Tear down OSPF connections with all neighbors for all routing instances.
area area-id—(Optional) Tear down neighbor connections for the specified area only.
instance instance-name—(Optional) Tear down neighbor connections for the specified routing instance only.
interface interface-name—(Optional) Tear down neighbor connections for the specified interface only.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
neighbor—(Optional) Clear the state of the specified neighbor only.
realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Clear the state of the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.
```

Required Privilege Level

```
clear
```

Related Documentation

```
• show (ospf | ospf3) neighbor on page 2904
```

List of Sample Output

```
clear ospf neighbor on page 2889
```

Output Fields

When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear ospf neighbor

user@host> clear ospf neighbor
clear (ospf | ospf3) statistics

Syntax

```
clear (ospf | ospf3) statistics
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

Syntax (EX Series Switch and QFX Series)

```
clear (ospf | ospf3) statistics
  <instance instance-name>
```

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `realm` option introduced in Junos OS Release 9.2.
- Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear Open Shortest Path First (OSPF) statistics.

Options

- `none`—Clear OSPF statistics.
- `instance instance-name`—(Optional) Clear statistics for the specified routing instance only.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)`—(Optional) (OSPFv3 only) Clear statistics for the specified OSPFv3 realm, or address family. Use the `realm` option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege

```
clear
```

Related Documentation

- show (ospf | ospf3) statistics on page 2921

List of Sample Output

- clear ospf statistics on page 2890

Output Fields

See show (ospf | ospf3) statistics for an explanation of output fields.

Sample Output

clear ospf statistics

The following sample output displays OSPF statistics before and after the clear ospf statistics command is entered:

```
user@host> show ospf statistics
```

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Sent</th>
<th>Received</th>
<th>Last 5 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>3254</td>
<td>2268</td>
<td>3</td>
</tr>
<tr>
<td>DbD</td>
<td>41</td>
<td>46</td>
<td>0</td>
</tr>
</tbody>
</table>
LSReq  8   7   0   0
LSUpdate  212  154  0   0
LSAck  65  98   0   0

DBDs retransmitted : 3, last 5 seconds : 0
LSAs flooded : 12, last 5 seconds : 0
LSAs flooded high-prio : 0, last 5 seconds : 0
LSAs retransmitted : 0, last 5 seconds : 0
LSAs transmitted to nbr: 3, last 5 seconds : 0
LSAs requested : 5, last 5 seconds : 0
LSAs acknowledged : 19, last 5 seconds : 0

Flood queue depth : 0
Total rexmit entries : 0
db summaries : 0
lsreq entries : 0

Receive errors:
  626 subnet mismatches

user@host> clear ospf statistics

user@host> show ospf statistics

Packet type       Total       Last 5 seconds
                  Sent  Received  Sent  Received
Hello             3     1         3     1
DbD              0     0         0     0
LSReq            0     0         0     0
LSUpdate         0     0         0     0
LSAck            0     0         0     0

DBDs retransmitted : 0, last 5 seconds : 0
LSAs flooded : 0, last 5 seconds : 0
LSAs flooded high-prio : 0, last 5 seconds : 0
LSAs retransmitted : 0, last 5 seconds : 0
LSAs transmitted to nbr: 0, last 5 seconds : 0
LSAs requested : 0, last 5 seconds : 0
LSAs acknowledged : 0, last 5 seconds : 0

Flood queue depth : 0
Total rexmit entries : 0
db summaries : 0
lsreq entries : 0

Receive errors:
  None
clear (ospf | ospf3) overload

**Syntax**
clear (ospf | ospf3) overload
   <instance instance-name>
   <logical-system (all | logical-system-name)>

**Syntax (EX Series Switches)**
clear (ospf | ospf3) overload
   <instance instance-name>

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Clear the Open Shortest Path First (OSPF) overload bit and rebuild link-state advertisements (LSAs).

**Options**
- **none**—Clear the overload bit and rebuild LSAs for all routing instances.
- **instance instance-name**—(Optional) Clear the overload bit and rebuild LSAs for the specified routing instance only.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
clear

**List of Sample Output**
clear ospf overload on page 2892

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear ospf overload

```
user@host> clear ospf overload
```
show (ospf | ospf3) interface

Syntax
show (ospf | ospf3) interface
  <brief | detail | extensive>
  <area area-id>
  <interface-name>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
  <realm (ip4-multicast | ipv4-unicast | ipv6-multicast)>

Syntax (EX Series Switches and QFX Series)
show (ospf | ospf3) interface
  <brief | detail | extensive>
  <area area-id>
  <interface-name>
  <instance instance-name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
area option introduced in Junos OS Release 9.2.
area option introduced in Junos OS Release 9.2 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display the status of OSPF interfaces.

Options
none—Display standard information about the status of all OSPF interfaces for all routing instances

brief | detail | extensive—(Optional) Display the specified level of output.

area area-id—(Optional) Display information about the interfaces that belong to the specified area.

interface-name—(Optional) Display information for the specified interface.

instance instance-name—(Optional) Display all OSPF interfaces under the named routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display information about the interfaces for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6unicast, which is the default.

Required Privilege Level
view

List of Sample Output
show ospf interface brief on page 2896
show ospf interface detail on page 2896
show ospf3 interface detail on page 2896
show ospf interface detail (When Multiarea Adjacency Is Configured) on page 2896
show ospf interface area area-id on page 2897
show ospf interface extensive (When Flooding Reduction Is Enabled) on page 2898
show ospf interface extensive (When LDP Synchronization Is Configured) on page 2898

**Output Fields**
Table 356 on page 2894 lists the output fields for the `show (ospf | ospf3) interface` command. Output fields are listed in the approximate order in which they appear.

**Table 356: show (ospf | ospf3) interface Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface running OSPF version 2 or OSPF version 3.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: BDR, Down, DR, DRother, Loop, PToPt, or Waiting.</td>
<td>All levels</td>
</tr>
<tr>
<td>Area</td>
<td>Number of the area that the interface is in.</td>
<td>All levels</td>
</tr>
<tr>
<td>DR ID</td>
<td>Address of the area’s designated router.</td>
<td>All levels</td>
</tr>
<tr>
<td>BDR ID</td>
<td>Backup designated router for a particular subnet.</td>
<td>All levels</td>
</tr>
<tr>
<td>Nbrs</td>
<td>Number of neighbors on this interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Type</td>
<td>Type of interface: LAN, NBMA, P2MP, P2P, or Virtual.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Mask</td>
<td>Netmask of the neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-length</td>
<td>(OSPFv3) IPv6 prefix length, in bits.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>OSPF3-Intf-Index</td>
<td>(OSPFv3) OSPF version 3 interface index.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MTU</td>
<td>Interface maximum transmission unit (MTU).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Cost</td>
<td>Interface cost (metric).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DR addr</td>
<td>Address of the designated router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>BDR addr</td>
<td>Address of the backup designated router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Adj count</td>
<td>Number of adjacent neighbors.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Secondary</td>
<td>Indicates that this interface is configured as a secondary interface for this area. This interface can belong to more than one area, but can be designated as a primary interface for only one area.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flood Reduction</td>
<td>Indicates that this interface is configured with flooding reduction. All self-originated LSAs from this interface are initially sent with the DoNotAge bit set. As a result, LSAs are refreshed only when a change occurs.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 356: show (ospf | ospf3) interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Router priority used in designated router (DR) election on this interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flood list</td>
<td>List of link-state advertisements (LSAs) that might be about to flood this interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>Ack list</td>
<td>Acknowledgment list. List of pending acknowledgments on this interface.</td>
<td>extensive</td>
</tr>
<tr>
<td>Descriptor list</td>
<td>List of packet descriptors.</td>
<td>extensive</td>
</tr>
<tr>
<td>Hello</td>
<td>Configured value for the hello timer.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Dead</td>
<td>Configured value for the dead timer.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Auth type</td>
<td>(OSPFv2) Authentication mechanism for sending and receiving OSPF protocol packets:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• MD5—The MD5 mechanism is configured in accordance with RFC 2328.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• None—No authentication method is configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password—A simple password (RFC 2328) is configured.</td>
<td></td>
</tr>
<tr>
<td>Topology</td>
<td>(Multiarea adjacency) Name of topology: default or name.</td>
<td></td>
</tr>
<tr>
<td>LDP sync state</td>
<td>(OSPFv2 and LDP synchronization) Current state of LDP synchronization: in sync, in hold down, and not supported.</td>
<td>extensive</td>
</tr>
<tr>
<td>reason</td>
<td>(OSPFv2 and LDP synchronization) Reason for the current state of LDP synchronization. The LDP session might be up or down, or adjacency might be up or down.</td>
<td>extensive</td>
</tr>
<tr>
<td>config holdtime</td>
<td>(OSPFv2 and LDP synchronization) Configured value of the hold timer.</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>If the state is not synchronized, and the hold time is not infinity, the remaining field displays the number of seconds that remain until the configured hold timer expires.</td>
<td></td>
</tr>
<tr>
<td>IPSec SA name</td>
<td>(OSPFv2) Name of the IPSec security association name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Active key ID</td>
<td>(OSPFv2 and MD5) Number from 0 to 255 that uniquely identifies an MD5 key.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Start time</td>
<td>(OSPFv2 and MD5) Time at which the routing device starts using an MD5 key to authenticate OSPF packets transmitted on the interface on which this key is configured. To authenticate received OSPF protocol packets, the key becomes effective immediately after the configuration is committed. If the start time option is not configured, the key is effective immediately for send and receive and is displayed as Start time 1970 Jan 01 00:00:00 PST.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>ReXmit</td>
<td>Configured value for the Retransmit timer.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Stub, Not Stub, or Stub NSSA</td>
<td>Type of area.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Sample Output

show ospf interface brief

```plaintext
user@host> show ospf interface brief

<table>
<thead>
<tr>
<th>Intf</th>
<th>State</th>
<th>Area</th>
<th>DR ID</th>
<th>BDR ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-5/1/0.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
<tr>
<td>ge-2/3/0.0</td>
<td>DR</td>
<td>0.0.0.0</td>
<td>192.168.4.16</td>
<td>192.168.4.15</td>
<td>1</td>
</tr>
<tr>
<td>lo0.0</td>
<td>DR</td>
<td>0.0.0.0</td>
<td>192.168.4.16</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>Down</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>so-6/0/1.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
<tr>
<td>so-6/0/2.0</td>
<td>Down</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>so-6/0/3.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
</tbody>
</table>
```

show ospf interface detail

```plaintext
user@host> show ospf interface detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Area</th>
<th>DR ID</th>
<th>BDR ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/1.0</td>
<td>BDR</td>
<td>0.0.0.0</td>
<td>192.168.37.12</td>
<td>10.255.245.215</td>
<td>1</td>
</tr>
</tbody>
</table>

Type LAN, address 192.168.37.11, Mask 255.255.255.248, MTU 4460, Cost 40
DR addr 192.168.37.12, BDR addr 192.168.37.11, Adj count 1, Priority 128
Hello 10, Dead 40, ReXmit 5, Not Stub
```

show ospf3 interface detail

```plaintext
user@host> show ospf3 interface so-0/0/3.0 detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Area</th>
<th>DR-ID</th>
<th>BDR-ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/3.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
</tbody>
</table>

Address fe80::2a0:a5ff:fe28:1dfc, Prefix-length 64
OSPF3-Intf-index 1, Type P2P, MTU 4470, Cost 12, Adj-count 1
Hello 10, Dead 40, ReXmit 5, Not Stub
```

show ospf interface detail

(When Multiarea Adjacency Is Configured)

```plaintext
user@host> show ospf interface detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Area</th>
<th>DR ID</th>
<th>BDR ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>lo0.0</td>
<td>DR</td>
<td>0.0.0.0</td>
<td>10.255.245.2</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
</tbody>
</table>

Type: LAN, Address: 127.0.0.1, Mask: 255.255.255.255, MTU: 65535, Cost: 0
DR addr: 127.0.0.1, Adj count: 0, Priority: 128
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 0
```

```plaintext
user@host> show ospf interface detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Area</th>
<th>DR ID</th>
<th>BDR ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>lo0.0</td>
<td>DR</td>
<td>0.0.0.0</td>
<td>10.255.245.2</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
</tbody>
</table>

Type: LAN, Address: 10.255.245.2, Mask: 255.255.255.255, MTU: 65535, Cost: 0
DR addr: 10.255.245.2, Adj count: 0, Priority: 128
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 0
```

```plaintext
user@host> show ospf interface detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Area</th>
<th>DR ID</th>
<th>BDR ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/0.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
</tbody>
</table>

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
```
Adj count: 1
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1
so-0/0/0.0       PtToPt  0.0.0.0     0.0.0.0     0.0.0.0            0

Type: P2P, Address: 192.168.37.46, Mask: 255.255.255.254, MTU: 4470, Cost: 1
Adj count: 1
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Passive, Cost: 1
so-1/0/0.0       PtToPt  0.0.0.0     0.0.0.0     0.0.0.0            0

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
Adj count: 0
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1
so-1/0/0.0       PtToPt  0.0.0.0     0.0.0.0     0.0.0.0            1

Type: P2P, Address: 192.168.37.54, Mask: 255.255.255.254, MTU: 4470, Cost: 1
Adj count: 1
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Secondary, Cost: 1
so-0/0/0.0       PtToPt  1.1.1.1     0.0.0.0     0.0.0.0            1

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
Adj count: 1
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Secondary, Cost: 1
so-1/0/0.0       PtToPt  1.1.1.1     0.0.0.0     0.0.0.0            1

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
Adj count: 1, Secondary
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1
so-0/0/0.0       PtToPt  2.2.2.2     0.0.0.0     0.0.0.0            1

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
Adj count: 1, Secondary
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1
so-1/0/0.0       PtToPt  2.2.2.2     0.0.0.0     0.0.0.0            1

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
Adj count: 1, Secondary
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1
so-0/0/0.0       PtToPt  2.2.2.2     0.0.0.0     0.0.0.0            1

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 1
Adj count: 1, Secondary
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1
so-1/0/0.0       PtToPt  2.2.2.2     0.0.0.0     0.0.0.0            1

show ospf interface area area-id

user@host> show ospf interface area 1.1.1.1
show ospf interface extensive

(When Flooding Reduction Is Enabled)

user@host> show ospf interface extensive

Interface   State   Area      DR ID    BDR ID    Nbrs
so-0/0/0.0  PtToPt  1.1.1.1    0.0.0.0  0.0.0.0    1
so-1/0/0.0  PtToPt  1.1.1.1    0.0.0.0  0.0.0.0    1

Type: P2P, Address: 10.10.10.1, Mask: 255.255.255.0, MTU: 1500, Cost: 1
Adj count: 0
Secondary, Flood Reduction
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
Topology default (ID 0) -> Cost: 1

show ospf interface extensive

(When LDP Synchronization Is Configured)

user@host> show ospf interface extensive

Interface   State   Area      DR ID    BDR ID    Nbrs
so-1/0/3.0  Down    0.0.0.0    0.0.0.0  0.0.0.0    0

Type: P2P, Address: 0.0.0.0, Mask: 0.0.0.0, MTU: 4470, Cost: 65535
Adj count: 0
Hello: 10, Dead: 40, ReXmit: 5, Not Stub
Auth type: None
LDP sync state: in holddown, for: 00:00:08, reason: LDP down during config
config holdtime: 10 seconds, remaining: 1
show (ospf | ospf3) io-statistics

Syntax
show (ospf | ospf3) io-statistics
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and QFX Series)
show (ospf | ospf3) io-statistics

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display Open Shortest Path First (OSPF) input and output statistics.

Options
- none—Display OSPF input and output statistics.
- logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

Related Documentation
- clear (ospf | ospf3) statistics on page 2890

List of Sample Output
show ospf io-statistics on page 2899

Output Fields
Table 357 on page 2899 lists the output fields for the show ospf io-statistics command. Output fields are listed in the approximate order in which they appear.

Table 357: show (ospf | ospf3) io-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets read</td>
<td>Number of OSPF packets read since the last time the routing protocol was started.</td>
</tr>
<tr>
<td>average per run</td>
<td>Total number of packets divided by the total number of times the OSPF read operation is scheduled to run.</td>
</tr>
<tr>
<td>max run</td>
<td>Maximum number of packets for a given run among all scheduled runs.</td>
</tr>
<tr>
<td>Receive errors</td>
<td>Number of faulty packets received with errors.</td>
</tr>
</tbody>
</table>

Sample Output

show ospf io-statistics

user@host> show ospf io-statistics

Packets read: 7361, average per run: 1.00, max run: 1
Receive errors:
None
show (ospf | ospf3) log

Syntax
show (ospf | ospf3) log
<instance instance-name>
<logical-system (all | logical-system-name)>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<topology topology-name>

Syntax (EX Series Switch and QFX Series)
show (ospf | ospf3) log
<instance instance-name>
<topology topology-name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
topology option introduced in Junos OS Release 9.0.
topology option introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display the entries in the Open Shortest Path First (OSPF) log of SPF calculations.

Options
none—Display entries in the OSPF log of SPF calculations for all routing instances.

instance instance-name—(Optional) Display entries for the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

topology topology-name—(Optional) (OSPFv2 only) Display entries for the specified topology.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(OSPFv3 only) (Optional) Display entries for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level
view

List of Sample Output
show ospf log on page 2902
show ospf log topology voice on page 2902

Output Fields
Table 358 on page 2901 lists the output fields for the show (ospf | ospf3) log command.
Output fields are listed in the approximate order in which they appear.

Table 358: show (ospf | ospf3) log Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>Time, in weeks (w) and days (d), since the SPF calculation was made.</td>
</tr>
</tbody>
</table>
**Table 358: show (ospf | ospf3) log Output Fields (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Type of calculation: Cleanup, External, Interarea, NSSA, Redist, SPF, Stub, Total, or VirtualLink.</td>
</tr>
<tr>
<td><strong>Elapsed</strong></td>
<td>Amount of time, in seconds, that elapsed during the operation, or the time required to complete the SPF calculation. The start time is the time displayed in the <strong>When</strong> field.</td>
</tr>
</tbody>
</table>

### Sample Output

**show ospf log**

```plaintext
user@host> show ospf log

<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1w4d 17:25:58</td>
<td>Stub</td>
<td>0.000017</td>
</tr>
<tr>
<td>1w4d 17:25:58</td>
<td>SPF</td>
<td>0.000070</td>
</tr>
<tr>
<td>1w4d 17:25:58</td>
<td>Stub</td>
<td>0.000019</td>
</tr>
<tr>
<td>1w4d 17:25:58</td>
<td>Interarea</td>
<td>0.000054</td>
</tr>
<tr>
<td>1w4d 17:25:58</td>
<td>External</td>
<td>0.000005</td>
</tr>
<tr>
<td>1w4d 17:25:58</td>
<td>Cleanup</td>
<td>0.000203</td>
</tr>
<tr>
<td>1w4d 17:25:58</td>
<td>Total</td>
<td>0.000537</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>SPF</td>
<td>0.000125</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>Stub</td>
<td>0.000017</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>SPF</td>
<td>0.000100</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>Stub</td>
<td>0.000016</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>Interarea</td>
<td>0.000056</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>External</td>
<td>0.000005</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>Cleanup</td>
<td>0.000238</td>
</tr>
<tr>
<td>1w4d 17:24:48</td>
<td>Total</td>
<td>0.000600</td>
</tr>
</tbody>
</table>

...  
```

**show ospf log topology voice**

```plaintext
user@host> show ospf log topology voice

Topology voice SPF log:

- Last instance of each event type
  ```plaintext
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:06:11</td>
<td>SPF</td>
<td>0.000116</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Stub</td>
<td>0.000114</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Interarea</td>
<td>0.000126</td>
</tr>
<tr>
<td>00:06:11</td>
<td>External</td>
<td>0.000067</td>
</tr>
<tr>
<td>00:06:11</td>
<td>NSSA</td>
<td>0.000037</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Cleanup</td>
<td>0.000186</td>
</tr>
</tbody>
</table>
  
  - Maximum length of each event type
    ```plaintext
    | Time         | Type    | Elapsed   |
    |--------------|---------|-----------|
    | 00:13:43     | SPF     | 0.000140  |
    | 00:13:33     | Stub    | 0.000116  |
    | 00:13:43     | Interarea | 0.000128 |
    | 00:13:33     | External| 0.000075  |
    | 00:13:38     | NSSA    | 0.000039  |
    | 00:13:53     | Cleanup | 0.000657  |
    ```
```

Last 100 events
<table>
<thead>
<tr>
<th>When</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:13:53</td>
<td>SPF</td>
<td>0.000090</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Stub</td>
<td>0.000041</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Interarea</td>
<td>0.000123</td>
</tr>
<tr>
<td>00:13:53</td>
<td>External</td>
<td>0.000040</td>
</tr>
<tr>
<td>00:13:53</td>
<td>NSSA</td>
<td>0.000038</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Cleanup</td>
<td>0.000065</td>
</tr>
<tr>
<td>00:13:53</td>
<td>Total</td>
<td>0.001252</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When</th>
<th>Type</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:06:11</td>
<td>SPF</td>
<td>0.000116</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Stub</td>
<td>0.000114</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Interarea</td>
<td>0.000126</td>
</tr>
<tr>
<td>00:06:11</td>
<td>External</td>
<td>0.000067</td>
</tr>
<tr>
<td>00:06:11</td>
<td>NSSA</td>
<td>0.000037</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Cleanup</td>
<td>0.000186</td>
</tr>
<tr>
<td>00:06:11</td>
<td>Total</td>
<td>0.000818</td>
</tr>
</tbody>
</table>
show (ospf | ospf3) neighbor

**Syntax**

```
show (ospf | ospf3) neighbor
  <brief | detail | extensive>
  <area area-id>
  <instance (all | instance-name)>
  <interface interface-name>
  <logical-system (all | logical-system-name)>
  <neighbor>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

**Syntax (EX Series Switches and QFX Series)**

```
show (ospf | ospf3) neighbor
  <brief | detail | extensive>
  <area area-id>
  <instance (all | instance-name)>
  <interface interface-name>
  <neighbor>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `instance all` option introduced in Junos OS Release 9.1.
- `instance all` option introduced in Junos OS Release 9.1 for EX Series switches.
- `area`, `interface`, and `realm` options introduced in Junos OS Release 9.2.
- `area` and `interface` options introduced in Junos OS Release 9.2 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display information about OSPF neighbors.

CPU utilization might increase while the device learns its OSPF neighbors. We recommend that you use the `show (ospf | ospf3) neighbor` command after the device learns and establishes OSPF neighbor adjacencies. Depending on the size of your network, this might take several minutes. If you receive a “timeout communicating with routing daemon” error when using the `show (ospf | ospf3) neighbor` command, wait several minutes before attempting to use the command again. This is not a critical system error, but you might experience a delay in using the CLI.

**Options**

- **none**—Display standard information about all OSPF neighbors for all routing instances.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **area area-id**—(Optional) Display information about the OSPF neighbors for the specified area.
- **instance (all | instance-name)**—(Optional) Display all OSPF interfaces for all routing instances or under the named routing instance.
- **interface interface-name**—(Optional) Display information about OSPF neighbors for the specified logical interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
**neighbor**—(Optional) Display information about the specified OSPF neighbor.

**realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)**—(OSPFv3 only) (Optional) Display information about the OSPF neighbors for the specified OSPFv3 realm, or address family. Use the **realm** option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>view</td>
</tr>
</tbody>
</table>

**Related Documentation**

- clear (ospf | ospf3) neighbor on page 2888

**List of Sample Output**

- show ospf neighbor brief on page 2907
- show ospf neighbor detail on page 2907
- show ospf neighbor extensive on page 2908
- show ospf3 neighbor detail on page 2909
- show ospf neighbor area area-id on page 2909
- show ospf neighbor interface interface-name on page 2909
- show ospf3 neighbor instance all (OSPFv3 Multiple Family Address Support Enabled) on page 2909

**Output Fields**

Table 359 on page 2905 lists the output fields for the **show (ospf | ospf3) neighbor** command. Output fields are listed in the approximate order in which they appear.

**Table 359: show (ospf | ospf3) neighbor Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Address of the neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 359: show (ospf | ospf3) neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the neighbor:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Attempt</strong>—Valid only for neighbors attached to nonbroadcast networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort must be made to contact the neighbor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—Initial state of a neighbor conversation. It indicates that no recent information has been received from the neighbor. Hello packets might continue to be sent to neighbors in the <strong>Down</strong> state, although at a reduced frequency.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Exchange</strong>—Routing device is describing its entire link-state database by sending database description packets to the neighbor. Each packet has a sequence number and is explicitly acknowledged.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>ExStart</strong>—First step in creating an adjacency between the two neighboring routing devices. The goal of this step is to determine which routing device is the master, and to determine the initial sequence number.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Full</strong>—Neighboring routing devices are fully adjacent. These adjacencies appear in router link and network link advertisements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Init</strong>—A hello packet has recently been sent by the neighbor. However, bidirectional communication has not yet been established with the neighbor. This state might occur, for example, because the routing device itself did not appear in the neighbor’s hello packet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Loading</strong>—Link-state request packets are sent to the neighbor to acquire more recent advertisements that have been discovered (but not yet received) in the <strong>Exchange</strong> state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>2Way</strong>—Communication between the two routing devices is bidirectional. This state has been ensured by the operation of the Hello Protocol. This is the most advanced state short of beginning adjacency establishment. The (backup) designated router is selected from the set of neighbors in state <strong>2Way</strong> or greater.</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Router ID of the neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Pri</td>
<td>Priority of the neighbor to become the designated router.</td>
<td>All levels</td>
</tr>
<tr>
<td>Dead</td>
<td>Number of seconds until the neighbor becomes unreachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link state acknowledgment list</td>
<td>Number of link-state acknowledgments received.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>Link state retransmission list</td>
<td>Total number of link-state advertisements retransmitted. For <strong>extensive</strong> output only, the following information is also displayed:</td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Type</strong>—Type of link advertisement: ASBR, Sum, Extern, Network, NSSA, OpaqArea, Router, or Summary.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>LSA ID</strong>—LSA identifier included in the advertisement. An asterisk preceding the identifier marks database entries that originated from the local routing device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Adv rtr</strong>—Address of the routing device that sent the advertisement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Seq</strong>—Link sequence number of the advertisement.</td>
<td></td>
</tr>
</tbody>
</table>
Table 359: show (ospf | ospf3) neighbor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor-address</td>
<td>(OSPFv3 only) If the neighbor uses virtual links, the Neighbor-address is the site-local, local, or global address. If the neighbor uses a physical interface, the Neighbor-address is an IPv6 link-local address.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>area</td>
<td>Area that the neighbor is in.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>OSPF3-Intf-index</td>
<td>(OSPFv3 only) Displays the OSPFv3 interface index.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>opt</td>
<td>Option bits received in the hello packets from the neighbor.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DR or DR-ID</td>
<td>Address of the designated router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>BDR or BDR-ID</td>
<td>Address of the backup designated router.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Up</td>
<td>Length of time since the neighbor came up.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>adjacent</td>
<td>Length of time since the adjacency with the neighbor was established.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

Sample Output

**show ospf neighbor brief**

```
user@host> show ospf neighbor brief
Address   Intf     State    ID             Pri  Dead
192.168.254.225  fxp3.0  2Way      10.250.240.32    128   36
192.168.254.230  fxp3.0  Full      10.250.240.8     128   38
192.168.254.229  fxp3.0  Full      10.250.240.35    128   33
10.1.1.129      fxp2.0  Full      10.250.240.12    128   37
10.1.1.131      fxp2.0  Full      10.250.240.11    128   38
10.1.2.1        fxp1.0  Full      10.250.240.9     128   32
10.1.2.81       fxp0.0  Full      10.250.240.10    128   33
```

**show ospf neighbor detail**

```
user@host> show ospf neighbor detail
Address   Interface    State    ID             Pri  Dead
10.5.1.2   ge-1/2/0.1  Full      10.5.1.2         128   37
          area 0.0.0.1, opt 0x42, DR 10.5.1.2, BDR 10.5.1.1
          Up 06:09:28, adjacent 05:17:36
          Link state acknowledgment list: 3 entries
          Link state retransmission list: 9 entries
10.5.10.2  ge-1/2/0.10 ExStart  10.5.1.38      128   34
          area 0.0.0.1, opt 0x42, DR 10.5.10.2, BDR 10.5.10.1
          Up 06:09:28
          master, seq 0xac1530f8, rexmit DBD in 3 sec
          rexmit LSREQ in 0 sec
10.5.11.2  ge-1/2/0.11 Full      10.5.1.42    128   38
          area 0.0.0.1, opt 0x42, DR 10.5.11.2, BDR 10.5.11.1
          Up 06:09:28, adjacent 05:26:46
          Link state retransmission list: 1 entries
```
show ospf neighbor extensive

<table>
<thead>
<tr>
<th>Address</th>
<th>Interface</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.1.2</td>
<td>ge-1/2/0.1</td>
<td></td>
<td>10.5.1.2</td>
<td>128</td>
<td>33</td>
</tr>
</tbody>
</table>

area 0.0.0.1, opt 0x42, DR 10.5.1.2, BDR 10.5.1.1
Up 06:09:42, adjacent 05:17:50

Link state retransmission list:

<table>
<thead>
<tr>
<th>Type</th>
<th>LSA ID</th>
<th>Adv rtr</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>10.8.56.0</td>
<td>172.25.27.82</td>
<td>0x8000004d</td>
</tr>
<tr>
<td>Router</td>
<td>10.5.1.94</td>
<td>10.5.1.94</td>
<td>0x8000005c</td>
</tr>
<tr>
<td>Network</td>
<td>10.5.24.2</td>
<td>10.5.1.94</td>
<td>0x80000036</td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.57.0</td>
<td>172.25.27.82</td>
<td>0x80000024</td>
</tr>
<tr>
<td>Extern</td>
<td>1.10.90.0</td>
<td>10.8.1.2</td>
<td>0x80000041</td>
</tr>
<tr>
<td>Extern</td>
<td>1.4.109.0</td>
<td>10.6.1.2</td>
<td>0x80000041</td>
</tr>
<tr>
<td>Router</td>
<td>10.5.1.190</td>
<td>10.5.1.190</td>
<td>0x8000005f</td>
</tr>
<tr>
<td>Network</td>
<td>10.5.48.2</td>
<td>10.5.1.190</td>
<td>0x8000003d</td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.58.0</td>
<td>172.25.27.82</td>
<td>0x8000004d</td>
</tr>
<tr>
<td>Extern</td>
<td>1.10.91.0</td>
<td>10.8.1.2</td>
<td>0x80000041</td>
</tr>
<tr>
<td>Extern</td>
<td>1.4.110.0</td>
<td>10.6.1.2</td>
<td>0x80000041</td>
</tr>
<tr>
<td>Router</td>
<td>10.5.1.18</td>
<td>10.5.1.18</td>
<td>0x8000005f</td>
</tr>
<tr>
<td>Network</td>
<td>10.5.5.2</td>
<td>10.5.1.18</td>
<td>0x80000033</td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.59.0</td>
<td>172.25.27.82</td>
<td>0x8000003a</td>
</tr>
<tr>
<td>Summary</td>
<td>10.8.62.0</td>
<td>172.25.27.82</td>
<td>0x80000025</td>
</tr>
</tbody>
</table>

10.5.10.2  ge-1/2/0.10  ExStart  10.5.1.38  128  38

area 0.0.0.1, opt 0x42, DR 10.5.10.2, BDR 10.5.10.1
Up 06:09:42
master, seq 0xac1530f8, retransmit DBD in 2 sec
retransmit LSREQ in 0 sec

Link state retransmission list:

<table>
<thead>
<tr>
<th>Type</th>
<th>LSA ID</th>
<th>Adv rtr</th>
<th>Seq</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>10.8.58.0</td>
<td>172.25.27.82</td>
<td>0x8000004d</td>
</tr>
</tbody>
</table>
show ospf3 neighbor detail

user@host> show ospf3 neighbor detail
ID               Interface              State     Pri   Dead
10.255.71.13     fe-0/0/2.0             Full      128   30
Neighbor-address fe80::290:69ff:fe9b:e002
area 0.0.0.0, opt 0x13, OSPF3-Intf-Index 2
DR-ID 10.255.71.13, BDR-ID 10.255.71.12
Up 02:51:43, adjacent 02:51:43

show ospf neighbor area area-id

user@host > show ospf neighbor area 1.1.1.1
Address          Interface              State     ID               Pri  Dead
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128    33
Area 1.1.1.1
192.168.37.55    so-1/0/0.0             Full      10.255.245.5     128    37
Area 1.1.1.1

show ospf neighbor interface interface-name

user@host > show ospf neighbor interface so-0/0/0.0
Address          Interface              State     ID               Pri  Dead
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128    33
Area 0.0.0.0
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128    37
Area 1.1.1.1
192.168.37.47    so-0/0/0.0             Full      10.255.245.4     128    32
Area 2.2.2.2

show ospf3 neighbor instance all (OSPFv3 Multiple Family Address Support Enabled)

user@host > show ospf3 neighbor instance all
Instance: ina
Realm: ipv6-unicast
ID               Interface              State     Pri   Dead
100.1.1.1        fe-0/0/2.0             Full      128     37
Neighbor-address fe80::217:cb00:c87c:8c03
Instance: inb
Realm: ipv4-unicast
ID               Interface              State     Pri   Dead
100.1.2.1        fe-0/0/2.1             Full      128     33
Neighbor-address fe80::217:cb00:c97c:8c03
show (ospf | ospf3) overview

**Syntax**

```
show (ospf | ospf3) overview

<brief | extensive>

<instance instance-name>

<logical-system (all | logical-system-name)>

<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
```

**Syntax (EX Series Switch and QFX Series)**

```
show (ospf | ospf3) overview

<brief | extensive>

<instance instance-name>
```

**Release Information**

Command introduced in Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Database protection introduced in Junos 10.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display Open Shortest Path First (OSPF) overview information.

**Options**

- **none**—Display standard information about all OSPF neighbors for all routing instances.
- **brief | extensive**—(Optional) Display the specified level of output.
- **instance instance-name**—(Optional) Display all OSPF interfaces under the named routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)**—(Optional) (OSPFv3 only) Display information about the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

**Required Privilege Level**

view

**List of Sample Output**

- show ospf overview on page 2912
- show ospf overview (With Database Protection) on page 2913
- show ospf3 overview (With Database Protection) on page 2913
- show ospf overview extensive on page 2913

**Output Fields**

Table 360 on page 2910 lists the output fields for the `show ospf overview` command. Output fields are listed in the approximate order in which they appear.

**Table 360: show ospf overview Output Fields**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>OSPF routing instance.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

2910 Copyright © 2013, Juniper Networks, Inc.
Table 360: show ospf overview Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>Router ID of the routing device.</td>
<td>All levels</td>
</tr>
<tr>
<td>Route table index</td>
<td>Route table index.</td>
<td>All levels</td>
</tr>
<tr>
<td>Configured overload</td>
<td>Overload capability is enabled. If the overload timer is also configured, display the time that remains before it is set to expire. This field is not displayed after the timer expires.</td>
<td>All levels</td>
</tr>
<tr>
<td>Topology</td>
<td>Topology identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Prefix export count</td>
<td>Number of prefixes exported into OSPF.</td>
<td>All levels</td>
</tr>
<tr>
<td>Full SPF runs</td>
<td>Number of complete Shortest Path First calculations.</td>
<td>All levels</td>
</tr>
<tr>
<td>SPF delay</td>
<td>Delay before performing consecutive Shortest Path First calculations.</td>
<td>All levels</td>
</tr>
<tr>
<td>SPF holddown</td>
<td>Delay before performing additional Shortest Path First (SPF) calculations after the maximum number of consecutive SPF calculations is reached.</td>
<td>All levels</td>
</tr>
<tr>
<td>SPF rapid runs</td>
<td>Maximum number of Shortest Path First calculations that can be performed in succession before the hold-down timer begins.</td>
<td>All levels</td>
</tr>
<tr>
<td>LSA refresh time</td>
<td>Refresh period for link-state advertisement (in minutes).</td>
<td>All levels</td>
</tr>
<tr>
<td>Database protection state</td>
<td>Current state of database protection.</td>
<td>All levels</td>
</tr>
<tr>
<td>Warning threshold</td>
<td>Threshold at which a warning message is logged (percentage of maximum LSA count).</td>
<td>All levels</td>
</tr>
<tr>
<td>Non self-generated LSAs</td>
<td>Number of LSAs whose router ID is not equal to the local router ID: Current, Warning (threshold), and Allowed.</td>
<td>All levels</td>
</tr>
<tr>
<td>Ignore time</td>
<td>How long the database has been in the ignore state.</td>
<td>All levels</td>
</tr>
<tr>
<td>Reset time</td>
<td>How long the database must stay out of the ignore or isolated state before it returns to normal operations.</td>
<td>All levels</td>
</tr>
<tr>
<td>Ignore count</td>
<td>Number of times the database has been in the ignore state: Current and Allowed.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart</td>
<td>Graceful restart capability: enabled or disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart duration</td>
<td>Time period for complete reacquisition of OSPF neighbors.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart grace period</td>
<td>Time period for which the neighbors should consider the restarting routing device as part of the topology.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 360: show ospf overview Output Fields (continued)

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful restart helper mode</td>
<td>(OSPFV2) Standard graceful restart helper capability (based on RFC 3623): enabled or disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Restart-signaling helper mode</td>
<td>(OSPFV2) Restart signaling-based graceful restart helper capability (based on RFC 4811, RFC 4812, and RFC 4813): enabled or disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Helper mode</td>
<td>(OSPFV3) Graceful restart helper capability: enabled or disabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Trace options</td>
<td>OSPF-specific trace options.</td>
<td>extensive</td>
</tr>
<tr>
<td>Trace file</td>
<td>Name of the file to receive the output of the tracing operation.</td>
<td>extensive</td>
</tr>
<tr>
<td>Area</td>
<td>Area number. Area 0.0.0.0 is the backbone area.</td>
<td>All levels</td>
</tr>
<tr>
<td>Stub type</td>
<td>Stub type of area: Normal Stub, Not Stub, or Not so Stubby Stub.</td>
<td>All levels</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Type of authentication: None, Password, or MD5.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The Authentication Type field refers to the authentication configured at the [edit protocols ospf area area-id] level. Any authentication configured for an interface in this area will not affect the value of this field.</td>
<td></td>
</tr>
<tr>
<td>Area border routers</td>
<td>Number of area border routers.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Number of autonomous system boundary routers.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output
show ospf overview

user@host> show ospf overview
Instance: master
     Router ID: 10.255.245.6
     Route table index: 0
     Configured overload, expires in 118 seconds
     LSA refresh time: 50 minutes
     Restart: Enabled
         Restart duration: 20 sec
         Restart grace period: 40 sec
         Helper mode: enabled
     Area: 0.0.0.0
     Stub type: Not Stub
     Authentication Type: None
     Area border routers: 0, AS boundary routers: 0
     Neighbors
         Up (in full state): 0
     Topology: default (ID 0)
     Prefix export count: 0
     Full SPF runs: 1
SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3

show ospf overview (With Database Protection)

user@host> show ospf overview
Instance: master
    Router ID: 10.255.112.218
    Route table index: 0
    LSA refresh time: 50 minutes
    Traffic engineering
        Restart: Enabled
            Restart duration: 180 sec
            Restart grace period: 210 sec
            Graceful restart helper mode: Enabled
            Restart-signaling helper mode: Enabled
    Database protection state: Normal
        Warning threshold: 70 percent
        Non self-generated LSAs: Current 582, Warning 700, Allowed 1000
        Ignore time: 30, Reset time: 60
        Ignore count: Current 0, Allowed 1
    Area: 0.0.0.0
        Stub type: Not Stub
        Authentication Type: None
        Area border routers: 0, AS boundary routers: 0
        Neighbors
            Up (in full state): 160
    Topology: default (ID 0)
        Prefix export count: 0
        Full SPF runs: 70
        SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
        Backup SPF: Not Needed

show ospf3 overview (With Database Protection)

user@host> show ospf3 overview
Instance: master
    Router ID: 10.255.112.128
    Route table index: 0
    LSA refresh time: 50 minutes
    Database protection state: Normal
        Warning threshold: 80 percent
        Non self-generated LSAs: Current 3, Warning 8, Allowed 10
        Ignore time: 30, Reset time: 60
        Ignore count: Current 0, Allowed 2
    Area: 0.0.0.0
        Stub type: Not Stub
        Area border routers: 0, AS boundary routers: 0
        Neighbors
            Up (in full state): 1
    Topology: default (ID 0)
        Prefix export count: 0
        Full SPF runs: 7
        SPF delay: 0.200000 sec, SPF holddown: 5 sec, SPF rapid runs: 3
        Backup SPF: Not Needed

show ospf overview extensive

user@host> show ospf overview extensive
Instance: master
    Router ID: 1.1.1.103
    Route table index: 0
Full SPF runs: 13, SPF delay: 0.200000 sec
LSA refresh time: 50 minutes
Restart: Disabled
Trace options: lsa
Trace file: /var/log/ospf size 131072 files 10
Area: 0.0.0.0
  Stub type: Not Stub
  Authentication Type: None
  Area border routers: 0, AS boundary routers: 0
Neighbors
  Up (in full state): 1
show (ospf | ospf3) route

Syntax

show (ospf | ospf3) route
  <brief | detail | extensive>
  <abr | asbr | extern | inter | intra>
  <destination>
  <instance (default | ipv4-multicast | instance-name)>
  <logical-system (default | ipv4-multicast | logical-system-name)>
  <network>
  <no-backup-coverage>
  <realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
  <router>
  <topology (default | ipv4-multicast | topology-name)>
  <transit>

Syntax (EX Series Switch and QFX Series)

show (ospf | ospf3) route
  <brief | detail | extensive>
  <abr | asbr | extern | inter | intra>
  <destination>
  <instance instance-name>
  <network>
  <no-backup-coverage>
  <router>
  <topology (default | ipv4-multicast | topology-name)>
  <transit>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
topology option introduced in Junos OS Release 9.0.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display the entries in the Open Shortest Path First (OSPF) routing table.

Options

none—Display standard information about all entries in the OSPF routing table for all routing instances and all topologies.

destination—Display routes to the specified IP address (with optional destination prefix length).

brief | detail | extensive—(Optional) Display the specified level of output.

abr—(Optional) Display routes to area border routers.

asbr—(Optional) Display routes to autonomous system border routers.

extern—(Optional) Display external routes.

inter—(Optional) Display interarea routes.

intra—(Optional) Display intra-area routes.
**instance (default | ipv4-multicast | instance-name)**—(Optional) Display entries for the default routing instance, the IPv4 multicast routing instance, or for the specified routing instance.

**logical-system (default | ipv4-multicast | logical-system-name)**—(Optional) Perform this operation on the default logical system, the IPv4 multicast logical system, or on a particular logical system.

**network**—(Optional) Display routes to networks.

**no-backup-coverage**—(Optional) Display routes with no backup coverage.

**realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)**—(OSPFv3 only) (Optional) Display entries in the routing table for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

**router**—(Optional) Display routes to all routers.

**topology (default | ipv4-multicast | topology-name)**—(OSPFv2 only) (Optional) Display routes for the default OSPF topology, IPv4 multicast topology, or for a particular topology.

**transit**—(Optional) (OSPFv3 only) Display OSPFv3 routes to pseudonodes.

**Required Privilege**

**Level**

**view**

**List of Sample Output**

- show ospf route on page 2918
- show ospf route detail on page 2918
- show ospf3 route on page 2918
- show ospf3 route detail on page 2919
- show ospf route topology voice on page 2919

**Output Fields**

Table 361 on page 2916 list the output fields for the show (ospf | ospf3) route command. Output fields are listed in the approximate order in which they appear.

**Table 361: show (ospf | ospf3) route Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>Name of the topology.</td>
<td>All levels</td>
</tr>
<tr>
<td>Prefix</td>
<td>Destination of the route.</td>
<td>All levels</td>
</tr>
<tr>
<td>Path type</td>
<td>How the route was learned:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Intera—Interarea route</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ext1—External type 1 route</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ext2—External type 2 route</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Intra—Intra-area route</td>
<td></td>
</tr>
</tbody>
</table>
Table 361: show (ospf | ospf3) route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route type</td>
<td>The type of routing device from which the route was learned:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• AS BR—Route to AS border router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Area BR—Route to area border router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Area/AS BR—Route to router that is both an Area BR and AS BR.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Network—Network router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Router—Route to a router that is neither an Area BR nor an AS BR.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transit—(OSPFv3 only) Route to a pseudonode representing a transit network, LAN, or nonbroadcast multiaccess (NBMA) link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Discard—Route to a summary discard.</td>
<td></td>
</tr>
<tr>
<td>NH Type</td>
<td>Next-hop type: LSP or IP.</td>
<td>All levels</td>
</tr>
<tr>
<td>Metric</td>
<td>Route’s metric value.</td>
<td>All levels</td>
</tr>
<tr>
<td>NH-interface</td>
<td>(OSPFv3 only) Interface through which the route’s next hop is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>NH-addr</td>
<td>(OSPFv3 only) IPv6 address of the next hop.</td>
<td>All levels</td>
</tr>
<tr>
<td>NextHop Interface</td>
<td>(OSPFv2 only) Interface through which the route’s next hop is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Nexthop addr/label</td>
<td>(OSPFv2 only) If the NH Type is IP, then it is the address of the next hop. If the NH Type is LSP, then it is the name of the label-switched path.</td>
<td>All levels</td>
</tr>
<tr>
<td>Area</td>
<td>Area ID of the route.</td>
<td>detail</td>
</tr>
<tr>
<td>Origin</td>
<td>Router from which the route was learned.</td>
<td>detail</td>
</tr>
<tr>
<td>Type 7</td>
<td>Route was learned through a not-so-stubby area (NSSA) link-state advertisement (LSA).</td>
<td>detail</td>
</tr>
<tr>
<td>P-bit</td>
<td>Route was learned through NSSA LSA and the propagate bit was set.</td>
<td>detail</td>
</tr>
<tr>
<td>Fwd NZ</td>
<td>Forwarding address is nonzero. Fwd NZ is only displayed if the route is learned through an NSSA LSA.</td>
<td>detail</td>
</tr>
<tr>
<td>optional-capability</td>
<td>Optional capabilities propagated in the router LSA. This field is in the output for intra-area router routes only (when Route Type is Area BR, AS BR, Area/AS BR, or Router), not for interarea router routes or network routes. Three bits in this field are defined as follows:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• 0x4 (V)—Routing device is at the end of a virtual active link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x2 (E)—Routing device is an autonomous system boundary router.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0x1 (B)—Routing device is an area border router.</td>
<td></td>
</tr>
</tbody>
</table>
Table 361: show (ospf | ospf3) route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Output Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>The priority assigned to the prefix:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• high</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• low</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: The priority field applies only to routes of type Network.

Sample Output

show ospf route

```
user@host> show ospf route
Prefix       Path  Route    NH  Metric  NextHop     Nexthop
Type         Type  Type     Interface addr/label
10.255.71.12  Intra Router IP    1       fe-0/0/2.0  192.16.22.86
10.255.71.13/32 Intra Network IP   0       lo0.0
192.168.222.84/30 Intra Network LSP 1       fe-0/0/2.0  lsp-ab
```

show ospf route detail

```
user@host> show ospf route detail
Topology default Route Table:

Prefix       Path  Route    NH  Metric  NextHop     Nexthop
Type         Type  Type     Interface addr/label
10.255.14.174 Inter AS BR     IP     210   t1-3/0/1.0
    area 0.0.0.2, origin 10.255.14.185
10.255.14.178 Intra Router IP  200   t3-3/1/3.0
    area 0.0.0.2, origin 10.255.14.178, optional-capability 0x0
10.210.1.0/30  Intra Network IP  10    t3-3/1/2.0
    area 0.0.0.2, origin 10.255.14.172, priority medium
100.1.1.1/32   Intra Network IP  210   t1-3/0/1.0
    area 0.0.0.2, origin 10.255.14.185, priority low
112.3.3.0/24   Ext2 Network IP  0      t1-3/0/1.0
    area 0.0.0.0, origin 10.255.14.174, priority high
200.3.3.0/30   Inter Network IP  220   t1-3/0/1.0
    area 0.0.0.2, origin 10.255.14.185, priority high
```

show ospf3 route

```
user@host> show ospf3 route
Prefix       Path  Route    NH  Metric  NextHop     Nexthop
Type         Type  Type     Interface addr/label
10.255.71.13  Intra Router IP    1       fxp1.1    192.168.36.17
    NH-interface fe-0/0/2.0, NH-addr fe80::290:69ff:fe9b:e002
10.255.71.13/32 Intra Network IP  0      fxp2.3    192.168.36.34
10.255.245.1  Intra Router IP  40      fxp1.1    192.168.36.17
    area 0.0.0.0, origin 10.255.245.3, optional-capability 0x0
10.255.245.3  Intra AS BR       IP      1        fxp2.3    192.168.36.34
    area 0.0.0.0, origin 10.255.245.3, optional-capability 0x0
10.255.245.1/32 Intra Network IP  40      fxp1.1    192.168.36.17
    area 0.0.0.0, origin 10.255.245.3, optional-capability 0x0
```
### show ospf3 route detail

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path</th>
<th>Route</th>
<th>NH</th>
<th>Metric</th>
<th>NextHop</th>
<th>Nexthop addr/label</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.174</td>
<td>Intra</td>
<td>Area/AS BR</td>
<td>IP</td>
<td>110</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NH-interface so-1/2/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.174, Optional-capability 0x3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.255.14.178</td>
<td>Intra</td>
<td>Router</td>
<td>IP</td>
<td>200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NH-interface t3-3/1/3.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.178, Optional-capability 0x0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.255.14.185/0.0.0.2</td>
<td>Intra</td>
<td>Transit</td>
<td>IP</td>
<td>200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NH-interface so-1/2/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.185</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000:1:1::1/128</td>
<td>Inter</td>
<td>Network</td>
<td>IP</td>
<td>110</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>NH-interface so-1/2/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.174, Priority low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1001:2:1::/48</td>
<td>Ext1</td>
<td>Network</td>
<td>IP</td>
<td>110</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>NH-interface so-1/2/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.174, Fwd NZ, Priority medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1002:1:7::/48</td>
<td>Ext2</td>
<td>Network</td>
<td>IP</td>
<td>0</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>NH-interface so-1/2/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.174, Fwd NZ, Priority low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1002:3:4::/48</td>
<td>Ext2</td>
<td>Network</td>
<td>IP</td>
<td>0</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>NH-interface so-1/2/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.174, Fwd NZ, Priority high</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>abcd::10:255:14:172/128</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>0</td>
<td>lo0.0</td>
<td></td>
</tr>
<tr>
<td>NH-interface lo0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Area 0.0.0.0, Origin 10.255.14.174, Priority low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### show ospf route topology voice

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path</th>
<th>Route</th>
<th>NH</th>
<th>Metric</th>
<th>NextHop</th>
<th>Nexthop addr/label</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.8.2</td>
<td>Intra</td>
<td>Router</td>
<td>IP</td>
<td>1</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>10.255.8.3</td>
<td>Intra</td>
<td>Router</td>
<td>IP</td>
<td>2</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>10.255.8.1/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>0</td>
<td>lo0.0</td>
<td></td>
</tr>
<tr>
<td>10.255.8.2/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>1</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>10.255.8.3/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>2</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>192.168.8.0/29</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>2</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>192.168.8.44/30</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>2</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>192.168.8.46/32</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>1</td>
<td>so-0/2/0.0</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Network</td>
<td>Type</td>
<td>VLAN</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>--------</td>
<td>------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.8.48/30</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>1 so-0/2/1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show (ospf | ospf3) statistics

Syntax

show (ospf | ospf3) statistics
<instance instance-name>
<logical-system (all | logical-system-name)>
realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)

Syntax (EX Series Switch and QFX Series)

show (ospf | ospf3) statistics
<instance instance-name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display OSPF statistics.

Options

none—Display OSPF statistics for all routing instances.

instance instance-name—(Optional) Display all statistics for the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) (OSPFv3 only) Display all statistics for the specified OSPFv3 realm, or address family. Use the realm option to specify an address family for OSPFv3 other than IPv6 unicast, which is the default.

Required Privilege Level
view

Related Documentation
• clear (ospf | ospf3) statistics on page 2890

List of Sample Output
show ospf statistics on page 2923
show ospf statistics logical-system all on page 2923
show ospf3 statistics on page 2924

Output Fields
Table 362 on page 2921 lists the output fields for the show (ospf | ospf3) statistics command. Output fields are listed in the approximate order in which they appear.

Table 362: show (ospf | ospf3) statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet type</td>
<td>Type of OSPF packet.</td>
</tr>
<tr>
<td>Total Sent/Total Received</td>
<td>Total number of packets sent and received.</td>
</tr>
<tr>
<td>Last 5 seconds Sent/Last 5 seconds Received</td>
<td>Total number of packets sent and received in the last 5 seconds.</td>
</tr>
</tbody>
</table>
### Table 362: show (ospf | ospf3) statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBDs retransmitted</td>
<td>Total number of database description packets retransmitted, and number retransmitted in the last 5 seconds.</td>
</tr>
<tr>
<td>LSAs flooded</td>
<td>Total number of link-state advertisements flooded, and number flooded in the last 5 seconds.</td>
</tr>
</tbody>
</table>
| LSAs flooded high-prio      | Total number of high priority link-state advertisements flooded, and number flooded in the last 5 seconds.  
A link-state advertisement is deemed a high priority if it has changed since it was last sent. |
| LSAs retransmitted          | Total number of link-state advertisements retransmitted, and number retransmitted in the last 5 seconds. |
| LSAs transmitted to nbr     | Total number of link-state advertisements transmitted to a neighbor, and number transmitted in the last 5 seconds. |
| LSAs requested              | Total number of link-state advertisements requested by neighboring devices, and number requested in the last 5 seconds. |
| LSAs acknowledged           | Total number of link-state advertisements acknowledged, and number acknowledged in the last 5 seconds. |
| Flood queue depth           | Total number of entries in the extended queue.                                     |
| Total rexmit entries        | Total number of retransmission entries waiting to be sent from the OSPF routing instance. |
| db summaries                | Total number of database description summaries waiting to be sent from the OSPF routing instance. |
| Isreq entries               | Total number of link-state request entries waiting to be sent from the OSPF routing instance. |
| Receive errors              | Number and type of receive errors. Some sample receive errors include:               |
|                             | - mtu mismatches                                                                  |
|                             | - no interface found                                                               |
|                             | - no virtual link found                                                            |
|                             | - nssa mismatches                                                                 |
|                             | - stub area mismatches                                                             |
|                             | - subnet mismatches                                                                |
|                             | If there are no receive errors, the output displays none.                           |
### Sample Output

#### show ospf statistics

```
user@host> show ospf statistics

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total</th>
<th>Last 5 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Received</td>
</tr>
<tr>
<td>Hello</td>
<td>31</td>
<td>14</td>
</tr>
<tr>
<td>DbD</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>LSReq</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>LSUpdate</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>LSAck</td>
<td>9</td>
<td>9</td>
</tr>
</tbody>
</table>

DBDs retransmitted : 3, last 5 seconds : 0
LSAs flooded : 12, last 5 seconds : 0
LSAs flooded high-prio : 0, last 5 seconds : 0
LSAs retransmitted : 0, last 5 seconds : 0
LSAs transmitted to nbr: 3, last 5 seconds : 0
LSAs requested : 5, last 5 seconds : 0
LSAs acknowledged : 19, last 5 seconds : 0

Flood queue depth : 0
Total retransmit entries : 0
db summaries : 0
lsreq entries : 0

Receive errors:
862 no interface found
115923 no virtual link found
```

#### show ospf statistics logical-system all

```
user@host> show ospf statistics logical-system all

logical-system: C
OSPF instance is not running

logical-system: B

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total</th>
<th>Last 5 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Received</td>
</tr>
<tr>
<td>Hello</td>
<td>313740</td>
<td>313653</td>
</tr>
<tr>
<td>DbD</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>LSReq</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>LSUpdate</td>
<td>2752</td>
<td>1825</td>
</tr>
<tr>
<td>LSAck</td>
<td>1821</td>
<td>2747</td>
</tr>
</tbody>
</table>

DBDs retransmitted : 0, last 5 seconds : 0
LSAs flooded : 2741, last 5 seconds : 0
LSAs flooded high-prio : 10, last 5 seconds : 0
LSAs retransmitted : 0, last 5 seconds : 0
LSAs transmitted to nbr: 2, last 5 seconds : 0
LSAs requested : 1, last 5 seconds : 0
LSAs acknowledged : 1831, last 5 seconds : 0

Flood queue depth : 0
Total retransmit entries : 0
db summaries : 0
lsreq entries : 0

Receive errors:
```
logical-system: A

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total</th>
<th>Last 5 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Received</td>
</tr>
<tr>
<td>Hello</td>
<td>313698</td>
<td>313695</td>
</tr>
<tr>
<td>DbD</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>LSReq</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>LSUpdate</td>
<td>1825</td>
<td>2752</td>
</tr>
<tr>
<td>LSAck</td>
<td>2747</td>
<td>1821</td>
</tr>
<tr>
<td>DBDs retransmitted</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs flooded</td>
<td>:</td>
<td>1825, last 5 seconds</td>
</tr>
<tr>
<td>LSAs flooded high-prio</td>
<td>:</td>
<td>10, last 5 seconds</td>
</tr>
<tr>
<td>LSAs retransmitted</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs transmitted to nbr:</td>
<td>:</td>
<td>1, last 5 seconds</td>
</tr>
<tr>
<td>LSAs requested</td>
<td>:</td>
<td>2, last 5 seconds</td>
</tr>
<tr>
<td>LSAs acknowledged</td>
<td>:</td>
<td>2748, last 5 seconds</td>
</tr>
<tr>
<td>Flood queue depth</td>
<td>:</td>
<td>0</td>
</tr>
<tr>
<td>Total rexmit entries</td>
<td>:</td>
<td>0</td>
</tr>
<tr>
<td>db summaries</td>
<td>:</td>
<td>0</td>
</tr>
<tr>
<td>lsreq entries</td>
<td>:</td>
<td>0</td>
</tr>
</tbody>
</table>

Receive errors:
None

show ospf3 statistics

<table>
<thead>
<tr>
<th>Packet type</th>
<th>Total</th>
<th>Last 5 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sent</td>
<td>Received</td>
</tr>
<tr>
<td>Hello</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DbD</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LSReq</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LSUpdate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LSAck</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DBDs retransmitted</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs flooded</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs flooded high-prio</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs retransmitted</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs transmitted to nbr:</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs requested</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>LSAs acknowledged</td>
<td>:</td>
<td>0, last 5 seconds</td>
</tr>
<tr>
<td>Flood queue depth</td>
<td>:</td>
<td>0</td>
</tr>
<tr>
<td>Total rexmit entries</td>
<td>:</td>
<td>0</td>
</tr>
<tr>
<td>db summaries</td>
<td>:</td>
<td>0</td>
</tr>
<tr>
<td>lsreq entries</td>
<td>:</td>
<td>0</td>
</tr>
</tbody>
</table>

Receive errors:
None
**show ospf database**

**Syntax**
```
show ospf database
  <brief | detail | extensive | summary>
  <advertising-router (address | self)>
  <area area-id>
  <asbrsummary>
  <external>
  <instance instance-name>
  <link-local>
  <logical-system (all | logical-system-name)>
  <lsa-id lsa-id>
  <netsummary>
  <network>
  <nssa>
  <opaque-area>
  <router>
```

**Syntax (EX Series Switches and QFX Series)**
```
show ospf database
  <brief | detail | extensive | summary>
  <advertising-router (address | self)>
  <area area-id>
  <asbrsummary>
  <external>
  <instance instance-name>
  <link-local>
  <logical-system (all | logical-system-name)>
  <lsa-id lsa-id>
  <netsummary>
  <network>
  <nssa>
  <opaque-area>
  <router>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`advertising-router self (address | self)` option introduced in Junos OS Release 9.5.
`advertising-router self (address | self)` option introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Display the entries in the OSPF version 2 (OSPFv2) link-state database, which contains data about link-state advertisement (LSA) packets.

**Options**
- `none`—Display standard information about entries in the OSPFv2 link-state database for all routing instances.
- `brief | detail | extensive | summary`—(Optional) Display the specified level of output.
- `advertising-router (address | self)`—(Optional) Display the LSAs advertised either by a particular routing device or by this routing device.
- `area area-id`—(Optional) Display the LSAs in a particular area.
asbr-summary—(Optional) Display summary AS boundary router LSA entries.

external—(Optional) Display external LSAs.

instance instance-name—(Optional) Display all OSPF database information under the named routing instance.

link-local—(Optional) Display information about link-local LSAs.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

lsa-id lsa-id—(Optional) Display the LSA with the specified LSA identifier.

netsummary—(Optional) Display summary network LSAs.

network—(Optional) Display information about network LSAs.

nssa—(Optional) Display information about not-so-stubby area (NSSA) LSAs.

opaque-area—(Optional) Display opaque area-scope LSAs.

router—(Optional) Display information about router LSAs.

Required Privilege Level view

Related Documentation

• clear (ospf | ospf3) database on page 2884

List of Sample Output

show ospf database on page 2928
show ospf database brief on page 2928
show ospf database detail on page 2928
show ospf database extensive on page 2930
show ospf database summary on page 2932

Output Fields

Table 363 on page 2926 describes the output fields for the show ospf database command. Output fields are listed in the approximate order in which they appear.

Table 363: show ospf database Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Area number. Area 0.0.0.0 is the backbone area.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Type

Type of link advertisement: ASBRSum, Extern, Network, NSSA, OpaqArea, Router, or Summary.

ID

LSA identifier included in the advertisement. An asterisk preceding the identifier marks database entries that originated from the local routing device.

Adv Rtr

Address of the routing device that sent the advertisement.

Seq

Link sequence number of the advertisement.
Table 363: show ospf database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Time elapsed since the LSA was originated, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Opt</td>
<td>Optional OSPF capabilities associated with the LSA.</td>
<td>All levels</td>
</tr>
<tr>
<td>Cksum</td>
<td>Checksum value of the LSA.</td>
<td>All levels</td>
</tr>
<tr>
<td>Len</td>
<td>Length of the advertisement, in bytes.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Router</strong></td>
<td><strong>Router link-state advertisement information:</strong></td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>bits</strong>—Flags describing the routing device that generated the LSP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>link count</strong>—Number of links in the advertisement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>id</strong>—ID of a routing device or subnet on the link.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>data</strong>—For stub networks, the subnet mask. Otherwise, the IP address of the routing device that generated the LSP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>type</strong>—Type of link. It can be <strong>PointToPoint</strong>, <strong>Transit</strong>, <strong>Stub</strong>, or <strong>Virtual</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>TOS count</strong>—Number of type-of-service (ToS) entries in the advertisement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>TOS 0 metric</strong>—Metric for ToS 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>TOS</strong>—Type-of-service (ToS) value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>metric</strong>—Metric for the ToS.</td>
<td></td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td><strong>Network link-state advertisement information:</strong></td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>mask</strong>—Network mask.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>attached router</strong>—ID of the attached neighbor.</td>
<td></td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td><strong>Summary link-state advertisement information:</strong></td>
<td><strong>detail extensive</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>mask</strong>—Network mask.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>TOS</strong>—Type-of-service (ToS) value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>metric</strong>—Metric for the ToS.</td>
<td></td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>Installed <strong>hh:mm:ss ago</strong></td>
<td>How long ago the route was installed.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>expires in <strong>hh:mm:ss</strong></td>
<td>How long until the route expires.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>sent <strong>hh:mm:ss ago</strong></td>
<td>How long ago the LSA was sent.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>Last changed <strong>hh:mm:ss ago</strong></td>
<td>How long ago the route was changed.</td>
<td><strong>extensive</strong></td>
</tr>
<tr>
<td>Change count</td>
<td>Number of times the route has changed.</td>
<td><strong>extensive</strong></td>
</tr>
</tbody>
</table>
Table 363: show ospf database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ours</td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
<tr>
<td>Router LSAs</td>
<td>Number of router link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>Network LSAs</td>
<td>Number of network link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>Summary LSAs</td>
<td>Number of summary link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>NSSA LSAs</td>
<td>Number of not-so-stubby area link-state advertisements in the link-state database.</td>
<td>summary</td>
</tr>
</tbody>
</table>

Sample Output

```
show ospf database

user@host> show ospf database
OSPF link state database, Area 0.0.0.1
Type   ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router 10.255.70.103    10.255.70.103    0x80000002   215  0x20 0x4112  48
Router *10.255.71.242    10.255.71.242    0x80000002   214  0x20 0x11b1  48
Summary *23.1.1.0       10.255.71.242    0x80000002   172  0x20 0x6d72  28
Summary *24.1.1.0       10.255.71.242    0x80000002   177  0x20 0x607e  28
NSA    *33.1.1.1        10.255.71.242    0x80000002   217  0x20 0x73bd  36

OSPF link state database, Area 0.0.0.2
Type   ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router 10.255.71.52     10.255.71.52     0x80000004   174  0x20 0x0d01  36
Router *10.255.71.242    10.255.71.242    0x80000003   173  0x20 0x191   36
Network *23.1.1.1       10.255.71.242    0x80000002   173  0x20 0x9c76  32
Summary *12.1.1.0       10.255.71.242    0x80000001   217  0x20 0xfeec  28
Summary *24.1.1.0       10.255.71.242    0x80000002   177  0x20 0x6d72  28
NSA    *33.1.1.1        10.255.71.242    0x80000001   222  0x28 0xe047  36

OSPF link state database, Area 0.0.0.3
Type   ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router 10.255.71.238    10.255.71.238    0x80000003   179  0x20 0x3942  36
Router *10.255.71.242    10.255.71.242    0x80000003   177  0x20 0xf37d  36
Network *24.1.1.1       10.255.71.242    0x80000002   177  0x20 0xc591  32
Summary *12.1.1.0       10.255.71.242    0x80000001   217  0x20 0xfeec  28
Summary *23.1.1.0       10.255.71.242    0x80000002   172  0x20 0x6d72  28
NSA    *33.1.1.1        10.255.71.242    0x80000001   222  0x28 0xe047  36
```

display ospf database brief

The output for the show ospf database brief command is identical to that for the show ospf database command. For sample output, see show ospf database on page 2928.

display ospf database detail

```
user@host> show ospf database detail
OSPF link state database, Area 0.0.0.1
Type   ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router 10.255.70.103    10.255.70.103    0x80000002   261  0x20 0x4112  48

OSPF link state database, Area 0.0.0.2
Type   ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router 10.255.71.52     10.255.71.52     0x80000004   174  0x20 0x0d01  36
Router *10.255.71.242    10.255.71.242    0x80000003   173  0x20 0x191   36
Network *23.1.1.1       10.255.71.242    0x80000002   173  0x20 0x9c76  32
Summary *12.1.1.0       10.255.71.242    0x80000001   217  0x20 0xfeec  28
Summary *24.1.1.0       10.255.71.242    0x80000002   177  0x20 0x6d72  28
NSA    *33.1.1.1        10.255.71.242    0x80000001   222  0x28 0xe047  36

OSPF link state database, Area 0.0.0.3
Type   ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router 10.255.71.238    10.255.71.238    0x80000003   179  0x20 0x3942  36
Router *10.255.71.242    10.255.71.242    0x80000003   177  0x20 0xf37d  36
Network *24.1.1.1       10.255.71.242    0x80000002   177  0x20 0xc591  32
Summary *12.1.1.0       10.255.71.242    0x80000001   217  0x20 0xfeec  28
Summary *23.1.1.0       10.255.71.242    0x80000002   172  0x20 0x6d72  28
NSA    *33.1.1.1        10.255.71.242    0x80000001   222  0x28 0xe047  36
```
OSPF link state database, Area 0.0.0.2

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.71.52</td>
<td>10.255.71.52</td>
<td>0x80000004</td>
<td>220</td>
<td>0x20</td>
<td>0xd021</td>
<td>36</td>
</tr>
</tbody>
</table>
| bits 0x0, link count 1
| id 23.1.1.1, data 23.1.1.2, Type Transit (2) |
| Router     | *10.255.71.242   | 10.255.71.242     | 0x80000003 | 219  | 0x20 | 0x6e191 | 36  |
| bits 0x0, link count 1
| id 23.1.1.1, data 23.1.1.1, Type Transit (2) |
| Network    | *23.1.1.1        | 10.255.71.242     | 0x80000002 | 219  | 0x20 | 0x9c76  | 32  |
| mask 255.255.255.0
| attached router 10.255.71.242
| attached router 10.255.71.52 |
| Summary    | *12.1.1.0        | 10.255.71.242     | 0x80000001 | 263  | 0x20 | 0xfeec  | 28  |
| mask 255.255.255.0
| attached router 10.255.71.242
| Summary    | *24.1.1.0        | 10.255.71.242     | 0x80000002 | 223  | 0x20 | 0x607e  | 28  |
| mask 255.255.255.0
| Summary    | *33.1.1.1        | 10.255.71.242     | 0x80000002 | 268  | 0x28 | 0xe047  | 36  |
| mask 255.255.255.255
| NSSA     | *33.1.1.1        | 10.255.71.242     | 0x80000002 | 263  | 0x28 | 0x73bd  | 36  |
| mask 255.255.255.255
| Type 2, TOS 0x0, metric 0, fwd addr 23.1.1.2, tag 0.0.0.0 |

OSPF link state database, Area 0.0.0.3

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.71.238</td>
<td>10.255.71.238</td>
<td>0x80000003</td>
<td>225</td>
<td>0x20</td>
<td>0x3942</td>
<td>36</td>
</tr>
</tbody>
</table>
| bits 0x0, link count 1
| id 24.1.1.1, data 24.1.1.2, Type Transit (2) |
| Router     | *10.255.71.242   | 10.255.71.242     | 0x80000003 | 223  | 0x20 | 0xdf37d | 36  |
| bits 0x0, link count 1
| id 24.1.1.1, data 24.1.1.1, Type Transit (2) |
| Network    | *24.1.1.1        | 10.255.71.242     | 0x80000002 | 223  | 0x20 | 0xc591  | 32  |
| mask 255.255.255.0
| attached router 10.255.71.242
| attached router 10.255.71.238 |
| Summary    | *12.1.1.0        | 10.255.71.242     | 0x80000001 | 263  | 0x20 | 0xfeec  | 28  |
| mask 255.255.255.0

Copyright © 2013, Juniper Networks, Inc.
show ospf database extensive

user@host> show ospf database extensive
OSPF link state database, Area 0.0.0.1

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.70.103</td>
<td>10.255.70.103</td>
<td>0x80000002</td>
<td>286</td>
<td>0x20</td>
<td>0x4112</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>id 10.255.71.242, data 12.1.1.1, Type PointToPoint (1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOS count 0, TOS 0 metric 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>id 12.1.1.0, data 255.255.255.0, Type Stub (3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOS count 0, TOS 0 metric 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:55:14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Installed 00:04:43 ago, expires in 00:55:14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Last changed 00:04:43 ago, Change count: 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Router  *10.255.71.242* 10.255.71.242 0x80000002 285 0x20 0x11b1 48
bits 0x3, link count 2
id 10.255.70.103, data 12.1.1.2, Type PointToPoint (1)
TOS count 0, TOS 0 metric 1
id 12.1.1.0, data 255.255.255.0, Type Stub (3)
TOS count 0, TOS 0 metric 1
Gen timer 00:45:15
Aging timer 00:55:15
Installed 00:04:45 ago, expires in 00:55:15, sent 00:04:43 ago
Last changed 00:04:45 ago, Change count: 2, Ours

Summary *23.1.1.0* 10.255.71.242 0x80000002 283 0x20 0x6d72 28
mask 255.255.255.0
TOS 0x0, metric 1
Gen timer 00:45:57
Aging timer 00:55:57
Installed 00:04:03 ago, expires in 00:55:57, sent 00:04:01 ago
Last changed 00:04:48 ago, Change count: 1, Ours

Summary *24.1.1.0* 10.255.71.242 0x80000002 248 0x20 0x607e 28
mask 255.255.255.0
TOS 0x0, metric 1
Gen timer 00:45:52
Aging timer 00:55:52
Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago
Last changed 00:04:48 ago, Change count: 1, Ours

NSSA *33.1.1.1* 10.255.71.242 0x80000002 288 0x28 0x73bd 36
mask 255.255.255.255
Type 2, TOS 0x0, metric 0, fwd addr 24.1.1.1, tag 0.0.0.0
Gen timer 00:45:12
Aging timer 00:55:12
Installed 00:04:48 ago, expires in 00:55:12, sent 00:04:48 ago
Last changed 00:04:48 ago, Change count: 2, Ours

OSPF link state database, Area 0.0.0.2

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Opt</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.255.71.52</td>
<td>10.255.71.52</td>
<td>0x80000004</td>
<td>245</td>
<td>0x20</td>
<td>0x0d021</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>id 23.1.1.1, data 23.1.1.2, Type Transit (2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TOS count 0, TOS 0 metric 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aging timer 00:55:55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Installed 00:04:02 ago, expires in 00:55:55
Last changed 00:04:02 ago, Change count: 2

Router  *10.255.71.242  10.255.71.242  0x80000003  244  0x20 0xe191  36
bits 0x3, link count 1
id 23.1.1.1, data 23.1.1.1, Type Transit (2)
TOS count 0, TOS 0 metric 1
Gen timer 00:45:56
Aging timer 00:55:56
Installed 00:04:04 ago, expires in 00:55:56, sent 00:04:02 ago
Last changed 00:04:04 ago, Change count: 2, Ours

Network *23.1.1.1         10.255.71.242    0x80000002   244  0x20 0x9c76  32
mask 255.255.255.0
attached router 10.255.71.242
attached router 10.255.71.52
Gen timer 00:45:56
Aging timer 00:55:56
Installed 00:04:04 ago, expires in 00:55:56, sent 00:04:02 ago
Last changed 00:04:04 ago, Change count: 1, Ours

Summary *12.1.1.0         10.255.71.242    0x80000001   288  0x20 0xfeec  28
mask 255.255.255.0
TOS 0x0, metric 1
Gen timer 00:45:12
Aging timer 00:55:12
Installed 00:04:48 ago, expires in 00:55:12, sent 00:04:04 ago
Last changed 00:04:48 ago, Change count: 1, Ours

Summary *24.1.1.0         10.255.71.242    0x80000002   248  0x20 0x607e  28
mask 255.255.255.0
TOS 0x0, metric 1
Gen timer 00:45:52
Aging timer 00:55:52
Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:04 ago
Last changed 00:04:08 ago, Change count: 1, Ours

NSSA    *33.1.1.1         10.255.71.242    0x80000001   293  0x28 0xe047  36
mask 255.255.255.255
Type 2, TOS 0x0, metric 0, fwd addr 23.1.1.1, tag 0.0.0.0
Gen timer 00:45:07
Aging timer 00:55:07
Installed 00:04:53 ago, expires in 00:55:07, sent 00:04:04 ago
Last changed 00:04:53 ago, Change count: 1, Ours

OSPF link state database, Area 0.0.0.3

Type       ID               Adv Rtr           Seq      Age  Opt  Cksum  Len
Router  10.255.71.238    10.255.71.238    0x80000003  250  0x20 0x3942  36
bits 0x0, link count 1
id 24.1.1.1, data 24.1.1.2, Type Transit (2)
TOS count 0, TOS 0 metric 1
Aging timer 00:55:50
Installed 00:04:07 ago, expires in 00:55:50
Last changed 00:04:07 ago, Change count: 2

Router  *10.255.71.242    10.255.71.242    0x80000003  248  0x20 0xf37d  36
bits 0x3, link count 1
id 24.1.1.1, data 24.1.1.1, Type Transit (2)
TOS count 0, TOS 0 metric 1
Gen timer 00:45:52
Aging timer 00:55:52
Installed 00:04:08 ago, expires in 00:55:52, sent 00:04:06 ago
Last changed 00:04:08 ago, Change count: 2, Ours

Network *24.1.1.1         10.255.71.242    0x80000002   248  0x20 0xc591  32
mask 255.255.255.0
attached router 10.255.71.242
attached router 10.255.71.238
show ospf database summary

user@host> show ospf database summary

Area 0.0.0.1:
  2 Router LSAs
  2 Summary LSAs
  1 NSSA LSAs

Area 0.0.0.2:
  2 Router LSAs
  1 Network LSAs
  2 Summary LSAs
  1 NSSA LSAs

Area 0.0.0.3:
  2 Router LSAs
  1 Network LSAs
  2 Summary LSAs
  1 NSSA LSAs

Externals:
  Interface fe-2/2/1.0:
  Interface ge-0/3/2.0:
  Interface so-0/1/2.0:
  Interface so-0/1/2.0:
show ospf3 database

Syntax
show ospf3 database
<brief | detail | extensive | summary>
<advertising-router (address | self)>
<area area-id>
<external>
<instance instance-name>
<inter-area-prefix>
<inter-area-router>
<intera-area-prefix>
<link>
<link-local>
<logical-system (all | logical-system-name)>
<lsa-id lsa-id>
<network>
<nssa>
<realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)>
<router>

Syntax (EX Series Switches and QFX Series)
show ospf3 database
<brief | detail | extensive | summary>
<advertising-router (address | self)>
<area area-id>
<external>
<instance instance-name>
<inter-area-prefix>
<inter-area-router>
<intera-area-prefix>
<link>
<link-local>
<lsa-id lsa-id>
<network>
<nssa>
<realm>
<router>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
realm option introduced in Junos OS Release 9.2.
advertising-router (address | self) option introduced in Junos Release 9.5.
advertising-router (address | self) option introduced in Junos OS Release 9.5 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display the entries in the OSPF version 3 (OSPFv3) link-state database, which contains data about link-state advertisement (LSA) packets.

Options
none—Display standard information about all entries in the OSPFv3 link-state database.
brief | detail | extensive | summary—(Optional) Display the specified level of output.
advertising-router (address | self)—(Optional) Display the LSAs advertised either by a particular routing device or by this routing device.
area area-id—(Optional) Display the LSAs in a particular area.

external—(Optional) Display external LSAs.

instance instance-name—(Optional) Display all OSPF database information under the named routing instance.

inter-area-prefix—(Optional) Display information about interarea-prefix LSAs.

inter-area-router—(Optional) Display information about interarea-router LSAs.

intra-area-prefix—(Optional) Display information about intra-area-prefix LSAs.

link—(Optional) Display information about link LSAs.

link-local—(Optional) Display information about link-local LSAs.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

lsa-id lsa-id—(Optional) Display the LSA with the specified LSA identifier.

network—(Optional) Display information about network LSAs.

nssa—(Optional) Display information about not-so-stubby area (NSSA) LSAs.

realm (ipv4-multicast | ipv4-unicast | ipv6-multicast)—(Optional) Display information about the specified OSPFv3 realm, or address family. Use the realm option to specify an address family other than IPv6 unicast, which is the default.

router—(Optional) Display information about router LSAs.

Required Privilege
Level
view

Related
Documentation
• clear (ospf | ospf3) database on page 2884

List of Sample Output
show ospf3 database brief on page 2939
show ospf3 database extensive on page 2939
show ospf3 database summary on page 2942

Output Fields
Table 364 on page 2934 lists the output fields for the show ospf3 database command. Output fields are listed in the approximate order in which they appear.

Table 364: show ospf3 database Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF link state database, area area-number</td>
<td>Entries in the link-state database for this area.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td>OSPF AS SCOPE link state database</td>
<td>Entries in the AS scope link-state database.</td>
<td>brief detail extensive</td>
</tr>
</tbody>
</table>
Table 364: show ospf3 database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OSPF Link-Local</strong>&lt;br&gt;link state database, interface &lt;br&gt;interface-name</td>
<td>Entries in the link-local link-state database for this interface.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>area</strong></td>
<td>Area number. Area 0.0.0.0 is the backbone area.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of link advertisement: Extern, InterArPfx, InterArRtr, IntraArPrx, Link, Network, NSSA, or Router.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>Link identifier included in the advertisement. An asterisk (*) preceding the identifier marks database entries that originated from the local routing device.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Adv Rtr</strong></td>
<td>Address of the routing device that sent the advertisement.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Seq</strong></td>
<td>Link sequence number of the advertisement.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>Time elapsed since the LSA was originated, in seconds.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Cksum</strong></td>
<td>Checksum value of the LSA.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Len</strong></td>
<td>Length of the advertisement, in bytes.</td>
<td>brief detail extensive</td>
</tr>
<tr>
<td><strong>Router (Router Link-State Advertisements)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>bits</strong></td>
<td>Flags describing the routing device that generated the LSP.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>Option bits carried in the router LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>For Each Router Link</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of interface. The value of all other output fields describing a routing device interface depends on the interface’s type:</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• PointToPoint (1)—Point-to-point connection to another routing device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transit (2)—Connection to a transit network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual (4)—Virtual link.</td>
<td></td>
</tr>
<tr>
<td><strong>Loc-if-id</strong></td>
<td>Local interface ID assigned to the interface that uniquely identifies the interface with the routing device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Nbr-if-id</strong></td>
<td>Interface ID of the neighbor’s interface for this routing device link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Nbr-rtr-id</strong></td>
<td>Router ID of the neighbor routing device (for type 2 interfaces, the attached link’s designated router).</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Cost of the router link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Gen timer</strong></td>
<td>How long until the LSA is regenerated, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 364: show ospf3 database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed $nn:nn:nn$ ago</td>
<td>How long ago the route was installed, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in $nn:nn:nn$</td>
<td>How long until the route expires, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent $nn:nn:nn$ ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>Ours</td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

**Network (Network Link-State Advertisements)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Option bits carried in the network LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Attached Router</td>
<td>Router IDs of each of the routing devices attached to the link. Only routing devices that are fully adjacent to the designated router are listed. The designated router includes itself in this list.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>

**InterArPfx (Interarea-Prefix Link-State Advertisements)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of this route. Expressed in the same units as the interface costs in the router LSAs. When the interarea-prefix LSA is describing a route to a range of addresses, the cost is set to the maximum cost to any reachable component of the address range.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed $nn:nn:nn$ ago</td>
<td>How long ago the route was installed, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in $nn:nn:nn$</td>
<td>How long until the route expires, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent $nn:nn:nn$ ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format \textit{hours}:\textit{minutes}:\textit{seconds}.</td>
<td>extensive</td>
</tr>
<tr>
<td>Ours</td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

**InterArRtr (Interarea-Router Link-State Advertisements)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest-router-id</td>
<td>Router ID of the routing device described by the LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>options</td>
<td>Optional capabilities supported by the routing device.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 364: show ospf3 database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric</td>
<td>Cost of this route. Expressed in the same units as the interface costs in the router LSAs. When the interarea-prefix LSA is describing a route to a range of addresses, the cost is set to the maximum cost to any reachable component of the address range.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>extensive</td>
</tr>
<tr>
<td>Extern (External Link-State Advertisements)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of the route, which depends on the value of Type.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Type n</td>
<td>Type of external metric: Type 1 or Type 2.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed nn:nn:nn ago</td>
<td>How long ago the route was installed, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires in nn:nn:nn</td>
<td>How long until the route expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent nn:nn:nn ago</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Link (Link-State Advertisements)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6-Address</td>
<td>IPv6 link-local address on the link for which this link LSA originated.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Options</td>
<td>Option bits carried in the link LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>priority</td>
<td>Router priority of the interface attaching the originating routing device to the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-count</td>
<td>Number of IPv6 address prefixes contained in the LSA. The rest of the link LSA contains a list of IPv6 prefixes to be associated with the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 364: show ospf3 database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>How long ago the route was installed, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires</td>
<td>How long until the route expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Ours</td>
<td>Indicates that this is a local advertisement.</td>
<td>extensive</td>
</tr>
<tr>
<td>IntraArPfx</td>
<td>(Intra-Area-Prefix Link-State Advertisements)</td>
<td></td>
</tr>
<tr>
<td>Ref-lsa-type</td>
<td>LSA type of the referenced LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>• Router—Address prefixes are associated with a router LSA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Network—Address prefixes are associated with a network LSA.</td>
<td></td>
</tr>
<tr>
<td>Ref-lsa-id</td>
<td>Link-state ID of the referenced LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Ref-router-id</td>
<td>Advertising router ID of the referenced LSA.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-count</td>
<td>Number of IPv6 address prefixes contained in the LSA. The rest of the link LSA contains a list of IPv6 prefixes to be associated with the link.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix</td>
<td>IPv6 address prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Prefix-options</td>
<td>Option bit associated with the prefix.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost of this prefix. Expressed in the same units as the interface costs in the router LSAs.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Gen timer</td>
<td>How long until the LSA is regenerated, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Aging timer</td>
<td>How long until the LSA expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>Installed</td>
<td>How long ago the route was installed, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>expires</td>
<td>How long until the route expires, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>sent</td>
<td>Time elapsed since the LSA was last transmitted or flooded to an adjacency or an interface, respectively, in the format hours:minutes:seconds.</td>
<td>extensive</td>
</tr>
<tr>
<td>n Router LSAs</td>
<td>Number of router LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>n Network LSAs</td>
<td>Number of network LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>n InterArPfx LSAs</td>
<td>Number of interarea-prefix LSAs in the link-state database.</td>
<td>summary</td>
</tr>
</tbody>
</table>
Table 364: show ospf3 database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>n InterArRtr LSAs</td>
<td>Number of interarea-router LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>n IntraArPfx LSAs</td>
<td>Number of intra-area-prefix LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>Externals</td>
<td>Display of the external LSA database.</td>
<td>summary</td>
</tr>
<tr>
<td>n Extern LSAs</td>
<td>Number of external LSAs in the link-state database.</td>
<td>summary</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface for which link-local LSA information is displayed.</td>
<td>summary</td>
</tr>
<tr>
<td>interface-name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>n Link LSAs</td>
<td>Number of link LSAs in the link-state database.</td>
<td>summary</td>
</tr>
</tbody>
</table>

Sample Output

show ospf3 database brief

```
user@host> show ospf3 database brief
OSP3 link state database, area 0.0.0.0
Type       ID               Adv Rtr           Seq         Age   Cksum  Len
Router     0.0.0.1          10.255.4.85      0x80000003   885   0xa697  40
Router     *0.0.0.1         10.255.4.93      0x80000002   953   0xc677  40
InterArPfx *0.0.0.2         10.255.4.93      0x80000001   910   0xb96f  44
InterArRtr *0.0.0.1         10.255.4.93      0x80000001   910   0xe159  32
IntraArPfx *0.0.0.1         10.255.4.93      0x80000002   432   0x788f  72
OSP3 link state database, area 0.0.0.1
Type       ID               Adv Rtr           Seq         Age   Cksum  Len
Router     *0.0.0.1         10.255.4.93      0x80000003   916   0xea40  40
Router     0.0.0.1          10.255.4.97      0x80000006   851   0xc95b  40
Network    0.0.0.2          10.255.4.97      0x80000002   916   0x4598  32
InterArPfx *0.0.0.1         10.255.4.93      0x80000002   117   0xa980  44
InterArPfx *0.0.0.2         10.255.4.93      0x80000002    62   0xd47e  44
NSSA       0.0.0.1          10.255.4.97      0x80000002   362   0x45ee  44
IntraArPfx *0.0.0.1         10.255.4.97      0x80000006   851   0x2f77  52
OSP3 AS SCOPE link state database
Type       ID               Adv Rtr           Seq         Age   Cksum  Len
Extern     0.0.0.1          10.255.4.85      0x80000002   63    0x9b86  44
Extern     *0.0.0.1         10.255.4.93      0x80000001   910   0x59c9  44
OSP3 Link-Local link state database, interface ge-1/3/0.0
Type       ID               Adv Rtr           Seq         Age   Cksum  Len
Link       *0.0.0.2         10.255.4.93      0x80000003   916   0x4dab  64
```

show ospf3 database extensive

```
user@host> show ospf3 database extensive
OSP3 link state database, area 0.0.0.0
Type       ID               Adv Rtr           Seq         Age   Cksum  Len
Router     0.0.0.1          10.255.4.85      0x80000003  1028   0xa697  40
bits 0x2, Options 0x13
Type PointToPoint (1), Metric 10
```

Copyright © 2013, Juniper Networks, Inc.
Loc-If-Id 2, Nbr-If-Id 3, Nbr-Rtr-Id 10.255.4.93
Aging timer 00:42:51
Installed 00:17:05 ago, expires in 00:42:52, sent 02:37:54 ago
Router *0.0.0.1 10.255.4.93 0x80000002 1096 0xc677 40
bits 0x3, Options 0x13
Type PointToPoint (1), Metric 10
Loc-If-Id 3, Nbr-If-Id 2, Nbr-Rtr-Id 10.255.4.85
Gen timer 00:00:40
Aging timer 00:41:44
Installed 00:18:16 ago, expires in 00:41:44, sent 00:18:14 ago
Ours
InterArPfx *0.0.0.2 10.255.4.93 0x80000001 1053 0xb96f 44
Prefix feee::10:10:2:0/126
Prefix-options 0x0, Metric 10
Gen timer 00:17:02
Aging timer 00:42:26
Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago
Ours
InterArPfx *0.0.0.3 10.255.4.93 0x80000001 1053 0x71d3 44
Prefix feee::10:255:4:97/128
Prefix-options 0x0, Metric 10
Gen timer 00:17:07
Aging timer 00:42:26
Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago
Ours
InterArRtr *0.0.0.1 10.255.4.93 0x80000001 1053 0xe159 32
Dest-router-id 10.255.4.97, Options 0x19, Metric 10
Gen timer 00:29:18
Aging timer 00:42:26
Installed 00:17:33 ago, expires in 00:42:27, sent 00:17:31 ago
Ours
IntraArPfx 0.0.0.1 10.255.4.85 0x80000002 1028 0x2403 72
Ref-lsa-type Router, Ref-lsa-id 0.0.0.0, Ref-router-id 10.255.4.85
Prefix-count 2
Prefix feee::10:255:4:85/128
Prefix-options 0x0, Metric 10
Prefix feee::10:10:1:0/126
Prefix-options 0x0, Metric 10
Aging timer 00:42:51
Installed 00:17:05 ago, expires in 00:42:52, sent 02:37:54 ago
IntraArPfx *0.0.0.1 10.255.4.93 0x80000002 575 0x788f 72
Ref-lsa-type Router, Ref-lsa-id 0.0.0.0, Ref-router-id 10.255.4.93
Prefix-count 2
Prefix feee::10:255:4:93/128
Prefix-options 0x2, Metric 0
Prefix feee::10:10:1:0/126
Prefix-options 0x0, Metric 10
Gen timer 00:33:23
Aging timer 00:50:24
Installed 00:09:35 ago, expires in 00:50:25, sent 00:09:33 ago
OSPF3 link state database, area 0.0.0.1
Type ID Adv Rtr Seq Age Cksum Len
Router *0.0.0.1 10.255.4.93 0x80000003 1059 0xea40 40
bits 0x3, Options 0x19
Type Transit (2), Metric 10
Loc-If-Id 2, Nbr-If-Id 2, Nbr-Rtr-Id 10.255.4.97
Gen timer 00:08:51
Aging timer 00:42:20
Installed 00:17:39 ago, expires in 00:42:21, sent 00:17:37 ago
Router 0.0.0.1 10.255.4.97 0x80000006 994 0xc95b 40
bits 0x2, Options 0x19
<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit (2), Metric 10</td>
<td>10.255.4.97</td>
<td>0x8000000020</td>
<td>1059</td>
<td>0x4598</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Aging timer 00:43:25</td>
<td>Installed 00:16:31 ago, expires in 00:43:26, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>0.0.0.2</td>
<td>10.255.4.97</td>
<td>0x8000000020</td>
<td>1059</td>
<td>0x4598</td>
<td>32</td>
</tr>
<tr>
<td>Options</td>
<td>0x11</td>
<td>Attached router 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr-Rtr-Id</td>
<td>10.255.4.97</td>
<td>Aging timer 00:42:20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr-If-Id</td>
<td>2</td>
<td>Installed 00:17:36 ago, expires in 00:42:21, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loc-If-Id</td>
<td>2</td>
<td>Installed 00:04:20 ago, expires in 00:55:40, sent 00:04:18 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attached router 10.255.4.97</td>
<td>Gen timer 00:45:39</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx</td>
<td>10.255.4.93</td>
<td>0x8000000020</td>
<td>260</td>
<td>0xa980</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::10:10:1:0/126</td>
<td>Prefix-options 0x0, Metric 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix-options</td>
<td>0x0</td>
<td>Gen timer 00:46:35</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aging timer</td>
<td>00:56:35</td>
<td>Installed 00:03:25 ago, expires in 00:56:35, sent 00:03:23 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx</td>
<td>10.255.4.93</td>
<td>0x8000000020</td>
<td>205</td>
<td>0xd47e</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::10:255:4:93/128</td>
<td>Prefix-options 0x0, Metric 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix-options</td>
<td>0x0</td>
<td>Gen timer 00:04:46</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aging timer</td>
<td>00:41:51</td>
<td>Installed 00:18:09 ago, expires in 00:41:51, sent 00:17:43 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InterArPfx</td>
<td>10.255.4.93</td>
<td>0x8000000020</td>
<td>1089</td>
<td>0x9bbb</td>
<td>44</td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::10:255:4:93/128</td>
<td>Prefix-options 0x0, Metric 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix-options</td>
<td>0x0</td>
<td>Gen timer 00:04:46</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aging timer</td>
<td>00:41:51</td>
<td>Installed 00:03:25 ago, expires in 00:56:35, sent 00:03:23 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSSA</td>
<td>0.0.0.1</td>
<td>10.255.4.97</td>
<td>0x8000000020</td>
<td>505</td>
<td>0x45ee</td>
<td>44</td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::200:200:1:0/124</td>
<td>Prefix-options 0x8, Metric 10, Type 2,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix-options</td>
<td>0x8</td>
<td>Gen timer 00:51:35</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aging timer</td>
<td>00:51:35</td>
<td>Installed 00:08:22 ago, expires in 00:51:35, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IntraArPfx</td>
<td>0.0.0.1</td>
<td>10.255.4.97</td>
<td>0x8000000026</td>
<td>994</td>
<td>0x2f77</td>
<td>52</td>
</tr>
<tr>
<td>Prefix-count</td>
<td>1</td>
<td>Ref-Isa-type Router, Ref-Isa-id 0.0.0.0, Ref-router-id 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::10:255:4:97/128</td>
<td>Prefix-options 0x2, Metric 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix-options</td>
<td>0x2</td>
<td>Aging timer 00:43:25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installed</td>
<td>00:16:31 ago, expires in 00:43:26, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IntraArPfx</td>
<td>0.0.0.3</td>
<td>10.255.4.97</td>
<td>0x8000000020</td>
<td>1059</td>
<td>0x4446</td>
<td>52</td>
</tr>
<tr>
<td>Prefix-count</td>
<td>1</td>
<td>Ref-Isa-type Network, Ref-Isa-id 0.0.0.2, Ref-router-id 10.255.4.97</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::10:10:2:0/126</td>
<td>Prefix-options 0x0, Metric 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix-options</td>
<td>0x0</td>
<td>Aging timer 00:42:20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installed</td>
<td>00:17:36 ago, expires in 00:42:21, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extern</td>
<td>0.0.0.1</td>
<td>10.255.4.85</td>
<td>0x8000000020</td>
<td>206</td>
<td>0x9b86</td>
<td>44</td>
</tr>
<tr>
<td>Prefix</td>
<td>feee::100:100:1:0/124</td>
<td>Prefix-options 0x0, Metric 20, Type 2,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prefix-options</td>
<td>0x0</td>
<td>Aging timer 00:56:34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Installed</td>
<td>00:03:23 ago, expires in 00:56:34, sent 02:37:54 ago</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OSPF3 AS SCOPE link state database
OSPF3 Link-Local link state database, interface ge-1/3/0.0

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>0.0.0.2</td>
<td>10.255.4.93</td>
<td>0x800000003</td>
<td>1059</td>
<td>0x4dab</td>
<td>64</td>
</tr>
<tr>
<td>Prefix</td>
<td>fe80::290:69ff:fe39:1cdb</td>
<td>Options 0x11, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:2:0/126 Prefix-options 0x0</td>
<td>Gen timer 00:12:56</td>
<td>Aging timer 00:42:20</td>
</tr>
</tbody>
</table>

Link 0.0.0.2

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>0.0.0.2</td>
<td>10.255.4.97</td>
<td>0x800000003</td>
<td>205</td>
<td>0xa87d</td>
<td>64</td>
</tr>
<tr>
<td>Prefix</td>
<td>fe80::290:69ff:fe38:883e</td>
<td>Options 0x11, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:2:0/126 Prefix-options 0x0</td>
<td>Gen timer 00:12:56</td>
<td>Aging timer 00:42:20</td>
</tr>
</tbody>
</table>

OSPF3 Link-Local link state database, interface so-2/2/0.0

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>0.0.0.0.2</td>
<td>10.255.4.85</td>
<td>0x800000002</td>
<td>506</td>
<td>0x42bb</td>
<td>64</td>
</tr>
<tr>
<td>Prefix</td>
<td>fe80::280:42ff:fe10:f169</td>
<td>Options 0x13, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:1:0/126 Prefix-options 0x0</td>
<td>Gen timer 00:51:34</td>
<td>Aging timer 00:08:23 ago, expires in 00:51:34, sent 02:37:54 ago</td>
</tr>
</tbody>
</table>

Link 0.0.0.3

<table>
<thead>
<tr>
<th>Type</th>
<th>ID</th>
<th>Adv Rtr</th>
<th>Seq</th>
<th>Age</th>
<th>Cksum</th>
<th>Len</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link</td>
<td>0.0.0.0.3</td>
<td>10.255.4.93</td>
<td>0x800000002</td>
<td>505</td>
<td>0x6b7a</td>
<td>64</td>
</tr>
<tr>
<td>Prefix</td>
<td>fe80::280:42ff:fe10:f177</td>
<td>Options 0x13, priority 128</td>
<td>Prefix-count 1</td>
<td>Prefix feee::10:10:1:0/126 Prefix-options 0x0</td>
<td>Gen timer 00:37:28</td>
<td>Aging timer 00:51:35</td>
</tr>
</tbody>
</table>

show ospf3 database summary

user@host> show ospf3 database summary

Area 0.0.0.0:
  2 Router LSAs
  1 InterArPfx LSAs
  1 InterArRtr LSAs
  1 IntraArPfx LSAs
Area 0.0.0.1:
  2 Router LSAs
  1 Network LSAs
  2 InterArPfx LSAs
  1 NSSA LSAs
  1 IntraArPfx LSAs
Externals:
  2 Extern LSAs
Interface ge-1/3/0.0:
  1 Link LSAs
Interface lo0.0:
Interface so-2/2/0.0:
  1 Link LSAs
• Overview on page 2947
• Configuration on page 2951
• Administration on page 2997
CHAPTER 57

Overview

- Layer 3 Protocols on page 2947

Layer 3 Protocols

- Layer 3 Protocols Supported on EX Series Switches on page 2947
- Layer 3 Protocols Not Supported on EX Series Switches on page 2948

Layer 3 Protocols Supported on EX Series Switches

EX Series switches support the Junos OS Layer 3 features and configuration statements listed in Table 326 on page 2553:

Table 365: Supported Junos OS Layer 3 Protocol Statements and Features

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>BFD</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>ICMP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>IGMPv1, v2, and v3</td>
<td>Fully supported.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>MLD</td>
<td>Fully supported (MLD versions 1 and 2).</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>MPLS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS MPLS Applications Configuration Guide</td>
</tr>
<tr>
<td>OSPFv1, v2 and v3</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
</tbody>
</table>
Table 365: Supported Junos OS Layer 3 Protocol Statements and Features (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td>Fully supported on EX3200, EX3300, EX4200, EX6200, and EX8200 switches.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>PPM</td>
<td>Supported. See “EX Series Switch Software Features Overview” on page 27 for specific platform information.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIPng</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>SNMP</td>
<td>Fully supported.</td>
<td>Junos OS Network Management Configuration Guide</td>
</tr>
<tr>
<td>VRRP</td>
<td>Fully supported.</td>
<td>See “Understanding VRRP on EX Series Switches” on page 2220. See also Junos OS High Availability Guide.</td>
</tr>
</tbody>
</table>

Related Documentation
- Layer 3 Protocols Not Supported on EX Series Switches on page 2554
- EX Series Switch Software Features Overview on page 27

Layer 3 Protocols Not Supported on EX Series Switches
EX Series switches do not support the Junos OS Layer 3 protocols and features listed in Table 327 on page 2554:

Table 366: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVMRP</td>
<td>• dvmrp and subordinate statements</td>
</tr>
<tr>
<td>Flow aggregation (cflowd)</td>
<td>• cflow and subordinate statements</td>
</tr>
<tr>
<td>IPSec</td>
<td>• [edit services] statements related to IPSec</td>
</tr>
<tr>
<td>IS-IS:</td>
<td>• cns-routing statement</td>
</tr>
<tr>
<td></td>
<td>• ipv6-multicast statement</td>
</tr>
<tr>
<td></td>
<td>• lsp-interval statement</td>
</tr>
<tr>
<td></td>
<td>• label-switched-path statement</td>
</tr>
<tr>
<td></td>
<td>• lsp-lifetime statement</td>
</tr>
<tr>
<td></td>
<td>• te-metric statement</td>
</tr>
<tr>
<td>Logical routers</td>
<td>• logical-routers and subordinate statements</td>
</tr>
</tbody>
</table>
Table 366: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MPLS:</strong></td>
<td>• Fast Reroute (FRR)</td>
</tr>
<tr>
<td></td>
<td>• Label Distribution Protocol (LDP) (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• Layer 3 VPNs (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• Multiprotocol BGP (MP-BGP) for VPN-IPv4 family</td>
</tr>
<tr>
<td></td>
<td>• Pseudowire emulation (PWE3)</td>
</tr>
<tr>
<td></td>
<td>• Routing policy statements related to Layer 3 VPNs and MPLS (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• Virtual Private LAN Service (VPLS)</td>
</tr>
<tr>
<td><strong>Network Address Translation (NAT)</strong></td>
<td>• nat and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• Policy statements related to NAT</td>
</tr>
<tr>
<td><strong>OSPF</strong></td>
<td>• demand-circuit statement</td>
</tr>
<tr>
<td></td>
<td>• label-switched-path and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• neighbor statement within an OSPF area</td>
</tr>
<tr>
<td></td>
<td>• peer-interface and subordinate statements within an OSPF area</td>
</tr>
<tr>
<td></td>
<td>• sham-link statement</td>
</tr>
<tr>
<td></td>
<td>• te-metric statement</td>
</tr>
<tr>
<td><strong>PIM SM</strong></td>
<td>• Not supported on EX2200 switches</td>
</tr>
<tr>
<td><strong>PIM SSM</strong></td>
<td>• Not supported on EX2200 switches</td>
</tr>
<tr>
<td><strong>PIM DM</strong></td>
<td>• Not supported on EX2200 or EX4500 switches</td>
</tr>
<tr>
<td><strong>PIM:</strong></td>
<td>• inet6 family (EX2200 and EX4500 switches)</td>
</tr>
<tr>
<td>• IPv6</td>
<td></td>
</tr>
<tr>
<td><strong>PPM</strong></td>
<td>• Not supported on EX2200 and EX3300 switches</td>
</tr>
<tr>
<td><strong>Routing instances:</strong></td>
<td>• l2vpn and subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td>• Routing instance forwarding</td>
<td>• ldp and subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td></td>
<td>• vpls and subordinate statements</td>
</tr>
<tr>
<td><strong>Routed VLAN interfaces (RVIs)</strong></td>
<td>• family mpls statement</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
### Table 366: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP and SDP</td>
<td>• sap and all subordinate statements</td>
</tr>
<tr>
<td>General routing options in the routing-options hierarchy:</td>
<td>• auto-export and subordinate statements</td>
</tr>
<tr>
<td>• MPLS and label-switched-paths</td>
<td>• dynamic-tunnels and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• lsp-next-hop and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• multicast and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• p2mp-lsp-next-hop and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• route-distinguisher-id statement (except on EX8200 switches)</td>
</tr>
<tr>
<td>Traffic sampling and forwarding in the forwarding-options hierarchy</td>
<td>• accounting and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• family mpls and family multiservice under hash-key hierarchy</td>
</tr>
<tr>
<td></td>
<td>• Under monitoring group-name family inet output hierarchy:</td>
</tr>
<tr>
<td></td>
<td>• cflowd statement</td>
</tr>
<tr>
<td></td>
<td>• export-format-cflowd-version-5 statement</td>
</tr>
<tr>
<td></td>
<td>• flow-active-timeout statement</td>
</tr>
<tr>
<td></td>
<td>• flow-export-destination statement</td>
</tr>
<tr>
<td></td>
<td>• flow-inactive-timeout statement</td>
</tr>
<tr>
<td></td>
<td>• interface statement</td>
</tr>
<tr>
<td></td>
<td>• port-mirroring statement (On EX Series switches, port mirroring is implemented using the analyzer statement.)</td>
</tr>
<tr>
<td></td>
<td>• sampling and subordinate statements</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Layer 3 Protocols Supported on EX Series Switches on page 2553
- EX Series Switch Software Features Overview on page 27
CHAPTER 58

Configuration

- Configuration Tasks on page 2951
- Configuration Statements: RIP on page 2955
- Configuration Statements: RIPng on page 2981

Configuration Tasks

- Configuring a RIP Network (J-Web Procedure) on page 2951

Configuring a RIP Network (J-Web Procedure)

You can use the J-Web interface to create RIP networks.

To configure a RIP network:

1. Select **Configure > Routing > RIP**.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Add**—Configures a RIP instance. Enter information into the RIP Configuration page as described in **Table 367 on page 2952**.
   - **Edit**—Modifies an existing RIP instance. Enter information into the configuration page for RIP as described in **Table 367 on page 2952**.
   - **Delete**—Deletes an existing RIP instance.

3. To modify RIP global settings, click **Edit**. Enter information in the configuration as described in **Table 368 on page 2952**.
### Table 367: RIP Routing Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routing instance name</td>
<td>Specifies a name for the routing instance.</td>
<td>Type or select and edit the name.</td>
</tr>
<tr>
<td>Preference</td>
<td>Specifies the preference of external routes learned by RIP as compared to those learned from other routing protocols.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Metric Out</td>
<td>Specifies the metric value to add to routes transmitted to the neighbor.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Update interval</td>
<td>Specifies an update time interval to periodically send out routes learned by RIP to neighbors.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Route timeout</td>
<td>Specifies the route timeout interval for RIP.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td><strong>Policies tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import Policy</td>
<td>Applies one or more policies to routes being imported into the local routing device from the neighbors.</td>
<td>Click <strong>Add</strong> to add an import policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Move up</strong> or <strong>Move down</strong> to move the selected policy up or down the list of policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Remove</strong> to remove an import policy.</td>
</tr>
<tr>
<td>Export Policy</td>
<td>Applies a policy to routes being exported to the neighbors.</td>
<td>Click <strong>Add</strong> to add an export policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Move up</strong> or <strong>Move down</strong> to move the selected policy up or down the list of policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Remove</strong> to remove an export policy.</td>
</tr>
<tr>
<td><strong>Neighbors tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIP-Enabled Interfaces</td>
<td>Selects the interfaces to be associated with the RIP instance.</td>
<td>To enable RIP on an interface, click the check box next to the interface name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Edit</strong> if you want to modify an interface's settings.</td>
</tr>
</tbody>
</table>

### Table 368: Edit RIP Global Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send</td>
<td>Specifies RIP send options.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Receive</td>
<td>Configure RIP receive options.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Route timeout (sec)</td>
<td>Specifies the route timeout interval for RIP.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Update interval (sec)</td>
<td>Specifies the update time interval to periodically send out routes learned by RIP to neighbors.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Field</td>
<td>Function</td>
<td>Your Action</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hold timeout (sec)</td>
<td>Specifies the time period the expired route is retained in the routing table before being removed.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Metric in</td>
<td>Specifies the metric to add to incoming routes when advertising into RIP routes that were learned from other protocols.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>RIB Group</td>
<td>Specifies a routing table group to install RIP routes into multiple routing tables.</td>
<td>Select and edit the name of the routing table group.</td>
</tr>
<tr>
<td>Message size</td>
<td>Specifies the number of route entries to be included in every RIP update message.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Check Zero</td>
<td>Specifies whether the reserved fields in a RIP packet are zero. Options are:</td>
<td>Select a value.</td>
</tr>
<tr>
<td></td>
<td>• check-zero—Discard version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements the RIP version 1 and version 2 specifications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• no-check-zero—Receive RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero. This is in spite of the fact that they are being sent in violation of the specifications in RFC 1058 and RFC 2453.</td>
<td></td>
</tr>
<tr>
<td>Graceful switchover</td>
<td>Configures graceful switchover for OSPF.</td>
<td>To disable graceful restart, select <strong>Disable</strong>. Type or select and edit the estimated time for the restart to finish, in seconds.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Specifies the type of authentication for RIP route queries received on an interface. Options are:</td>
<td>Select the authentication type. Enter the authentication key for MD5.</td>
</tr>
<tr>
<td></td>
<td>• None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Simple</td>
<td></td>
</tr>
<tr>
<td>Policies tab</td>
<td>Applies one or more policies to routes being imported into the local routing device from the neighbors.</td>
<td>Click <strong>Add</strong> to add an import policy. Click <strong>Move up</strong> or <strong>Move down</strong> to move the selected policy up or down the list of policies. Click <strong>Remove</strong> to remove an import policy.</td>
</tr>
</tbody>
</table>
Table 368: Edit RIP Global Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Policy</td>
<td>Applies a policy to routes being exported to the neighbors.</td>
<td>Click <strong>Add</strong> to add an export policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Move up</strong> or <strong>Move down</strong> to move the selected policy up or down the list of policies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click <strong>Remove</strong> to remove an export policy.</td>
</tr>
<tr>
<td>Trace Options tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File Name</td>
<td>Specifies the name of the file to receive the output of the tracing operation.</td>
<td>Type or select and edit the name.</td>
</tr>
<tr>
<td>Number of Files</td>
<td>Specifies the maximum number of trace files.</td>
<td>Type or select and edit the name.</td>
</tr>
<tr>
<td>File Size</td>
<td>Specifies the maximum size for each trace file.</td>
<td>Type or select and edit the name.</td>
</tr>
<tr>
<td>World Readable</td>
<td>Specifies whether the trace file can be read by any user or not.</td>
<td>Select <strong>True</strong> to allow any user to read the file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select <strong>False</strong> to disallow all users being able to read the file.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies the tracing operation to perform.</td>
<td>Select a value from the list.</td>
</tr>
</tbody>
</table>

Related Documentation

- Monitoring RIP Routing Information on page 2997
- Layer 3 Protocols Supported on EX Series Switches on page 2553
Configuration Statements: RIP

any-sender

Syntax     any-sender;

Hierarchy Level     [edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name],
                     [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],
                     [edit protocols rip group group-name neighbor neighbor-name],
                     [edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]

Release Information     Statement introduced in Junos OS Release 8.0.
                          Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description     Disable strict sender address checks.

If the sender of a RIP message does not belong to the subnet of the interface, the message is discarded. This situation might cause problems with dropped packets when RIP is running on point-to-point interfaces, or when the addresses on the interfaces do not fall in the same subnet. You can resolve this by disabling strict address checks on the RIP traffic.

NOTE: The any-sender statement is supported only for peer-to-peer interfaces.

Required Privilege Level     routing—To view this statement in the configuration.
                              routing-control—To add this statement to the configuration.

Related Documentation     • Example: Configuring RIP
### authentication-key (Protocols RIP)

**Syntax**

```
authentication-key password;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols rip]`
- `[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]`
- `[edit protocols rip]`
- `[edit protocols rip group group-name neighbor neighbor-name]`
- `[edit routing-instances routing-instance-name protocols rip]`
- `[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]`

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Require authentication for RIP route queries received on an interface.

**Options**

- **password**—Authentication password. If the password does not match, the packet is rejected. The password can be from 1 through 16 contiguous characters long and can include any ASCII strings.

**Required Privilege Level**

- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

**Related Documentation**

- [Example: Configuring Route Authentication for RIP](#)
authentication-type (Protocols RIP)

Syntax

```
authentication-type type;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],
[edit protocols rip],
[edit protocols rip group group-name neighbor neighbor-name],
[edit routing-instances routing-instance-name protocols rip],
[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Configure the type of authentication for RIP route queries received on an interface.

Default

If you do not include this statement and the `authentication-key` statement, RIP authentication is disabled.

Options

```
type—Authentication type:
```

- `md5`—Use the MD5 algorithm to create an encoded checksum of the packet. The encoded checksum is included in the transmitted packet. The receiving routing device uses the authentication key to verify the packet, discarding it if the digest does not match. This algorithm provides a more secure authentication scheme.

- `none`—Disable authentication. If `none` is configured, the configured authentication key is ignored.

- `simple`—Use a simple password. The password is included in the transmitted packet, which makes this method of authentication relatively insecure. The password can be from 1 through 16 contiguous letters or digits long.

Required Privilege Level

```
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.
```

Related Documentation

```
Example: Configuring Route Authentication for RIP

authentication-key on page 2956
```
## bfd-liveness-detection (Protocols RIP)

**Syntax**

```plaintext
bfd-liveness-detection {
  authentication {
    algorithm algorithm-name;
    key-chain key-chain-name;
    loose-check;
  }
  detection-time {
    threshold milliseconds;
  }
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  version (1 | automatic);
}
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols rip group group-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],
- [edit protocols rip group group-name],
- [edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]

**Release Information**

- Statement introduced in Junos OS Release 8.0.
- Options detection-time threshold and transmit-interval threshold introduced in Junos OS Release 8.2.
- Support for logical systems introduced in Junos OS Release 8.3.
- Option no-adaptation introduced in Junos OS Release 9.0.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Options authentication algorithm, authentication key-chain, and authentication loose-check introduced in Junos OS Release 9.6.
- Options authentication algorithm, authentication key-chain, and authentication loose-check introduced in Junos OS Release 9.6 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure bidirectional failure detection timers and authentication.

**Options**

- **authentication algorithm algorithm-name** — Configure the algorithm used to authenticate the specified BFD session: simple-password, keyed-md5, keyed-sha-1, meticulous-keyed-md5, or meticulous-keyed-sha-1.
- **authentication key-chain key-chain-name** — Associate a security key with the specified BFD session using the name of the security keychain. The name you specify must match one of the keychains configured in the authentication-key-chains key-chain statement at the [edit security] hierarchy level.
authentication loose-check—(Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication is not configured at both ends of the BFD session.

detection-time threshold milliseconds—Configure a threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

minimum-interval milliseconds—Configure the minimum interval after which the local routing device transmits a hello packet and then expects to receive a reply from the neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the transmit-interval minimum-interval and minimum-receive-interval statements.

Range: 1 through 255,000 milliseconds

minimum-receive-interval milliseconds—Configure the minimum interval after which the local routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum receive interval using the minimum-interval statement.

Range: 1 through 255,000 milliseconds

multiplier number—Configure the number of hello packets not received by a neighbor that causes the originating interface to be declared down.

Range: 1 through 255
Default: 3

no-adaptation—Configure BFD sessions not to adapt to changing network conditions. We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

transmit-interval threshold milliseconds—Configure the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent. The interval threshold must be greater than the minimum transmit interval.

Range: 0 through 4,294,967,295 (2^{32} – 1)

transmit-interval minimum-interval milliseconds—Configure a minimum interval after which the local routing device transmits hello packets to a neighbor. Optionally, instead of using this statement, you can configure the minimum transmit interval using the minimum-interval statement.

Range: 1 through 255,000

version—Configure the BFD version to detect: 1 (BFD version 1) or automatic (autodetect the BFD version).

Default: automatic
Related Documentation

- Example: Configuring BFD for RIP
- Example: Configuring BFD Authentication for RIP
# check-zero

**Syntax**

(check-zero | no-check-zero);

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols rip],
- [edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],
- [edit protocols rip],
- [edit protocols rip group group-name neighbor neighbor-name],
- [edit routing-instances routing-instance-name protocols rip],
- [edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Some of the reserved fields in RIP version 1 packets must be zero, whereas in RIP version 2 packets, most of these reserved fields can contain nonzero values. By default, RIP discards version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements the RIP version 1 and version 2 specifications.

If you find that you are receiving RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero, you can configure RIP to receive these packets even though they are being sent in violation of the specifications in RFC 1058 and RFC 2453.

Check whether the reserved fields in a RIP packet are zero:

- **check-zero**—Discard version 1 packets that have nonzero values in the reserved fields and version 2 packets that have nonzero values in the fields that must be zero. This default behavior implements the RIP version 1 and version 2 specifications.

- **no-check-zero**—Receive RIP version 1 packets with nonzero values in the reserved fields or RIP version 2 packets with nonzero values in the fields that must be zero. This is in spite of the fact that they are being sent in violation of the specifications in RFC 1058 and RFC 2453.

**Default**

check-zero

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring RIP
### export (Protocols RIP)

**Syntax**

```conlang
eexport [ policy-names ];
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols rip group group-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name]`
- `[edit protocols rip group group-name]`
- `[edit routing-instances routing-instance-name protocols rip group group-name]`

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Apply a policy to routes being exported to the neighbors.

By default, RIP does not export routes it has learned to its neighbors. To enable RIP to export routes, apply one or more export policies.

If no routes match the policies, the local routing device does not export any routes to its neighbors. Export policies override any metric values determined through calculations involving the values configured with the `metric-in` and `metric-out` statements.

**NOTE:** The export policy on RIP does not support manipulating routing information of the next hop.

**Options**

- `policy-names`—Name of one or more policies.

**Required Privilege**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring RIP*
- *import on page 2967*
### graceful-restart (Protocols RIP)

**Syntax**
```
graceful-restart {
    disable;
    restart-time seconds;
}
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name protocols rip],
[edit protocols rip]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure graceful restart for RIP.

**Options**
- `disable`—Disables graceful restart for RIP.
  
The remaining statement is explained separately.

**Required Privilege Level**
- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**
- [Junos OS High Availability Library for Routing Devices](#)
group (Protocols RIP)

Syntax  

```plaintext
group group-name {  
bfd-liveness-detection {  
  authentication {  
    algorithm algorithm-name;  
    key-chain key-chain-name;  
    loose-check;  
  }  
  detection-time {  
    threshold milliseconds;  
  }  
  minimum-interval milliseconds;  
  minimum-receive-interval milliseconds;  
  transmit-interval {  
    threshold milliseconds;  
    minimum-interval milliseconds;  
  }  
  multiplier number;  
  version (0 | 1 | automatic);  
}  

demand-circuit;  
export policy;  
max-retrans-time seconds;  
metric-out metric;  
preference number;  
route-timeout seconds;  
update-interval seconds;  
neighbor neighbor-name {  
  authentication-key password;  
  authentication-type type;  
  bfd-liveness-detection {  
    authentication {  
      algorithm algorithm-name;  
      key-chain key-chain-name;  
      loose-check;  
    }  
    detection-time {  
      threshold milliseconds;  
    }  
    minimum-interval milliseconds;  
    minimum-receive-interval milliseconds;  
    transmit-interval {  
      threshold milliseconds;  
      minimum-interval milliseconds;  
    }  
    multiplier number;  
    version (0 | 1 | automatic);  
  }  
  (check-zero | no-check-zero);  
demand-circuit;  
import policy-name;  
max-retrans-time seconds;  
message-size number;  
```
metric-in metric;
metric-out metric;
receive receive-options;
route-timeout seconds;
send send-options;
update-interval seconds;
}
}

Hierarchy Level
[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit protocols rip],
[edit routing-instances routing-instance-name protocols rip]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Configure a set of RIP neighbors that share an export policy and metric. The export policy and metric govern what routes to advertise to neighbors in a given group. Each group must contain at least one neighbor. You should create a group for every export policy.

Options
group-name—Name of a group, up to 16 characters long.
The remaining statements are explained separately.

Required Privilege
routing—To view this statement in the configuration.
route-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring RIP
**holddown (Protocols RIP)**

**Syntax**

`holddown seconds;`

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit protocols rip],
[edit routing-instances routing-instance-name protocols rip]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Configure how long the expired route is retained in the routing table before being removed.

When the hold-down timer runs on RIP demand circuits, routes are advertised as unreachable on other interfaces. When the hold-down timer expires, the route is removed from the routing table if all destinations detect that the route is unreachable or the remaining destinations are down.

**Options**

`seconds`—Estimated time to wait before making updates to the routing table.

- **Range:** 10 through 180 seconds
- **Default:** 120 seconds

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring RIP Timers
- RIP Demand Circuits Overview
import (Protocols RIP)

**Syntax**
```python
import [ policy-names ];
```

**Hierarchy Level**
- `[edit logical-systems logical-system-name protocols rip]`
- `[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]`
- `[edit protocols rip]`
- `[edit protocols rip group group-name neighbor neighbor-name]`
- `[edit routing-instances routing-instance-name protocols rip]`
- `[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]`

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**
Apply one or more policies to routes being imported by the local routing device from neighbors.

**Options**
- `policy-names`—Name of one or more policies.

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- *Example: Applying Policies to RIP Routes Imported from Neighbors*
- *Routing Policy Feature Guide for Routing Devices*
- *export on page 2962*
**message-size**

**Syntax**  
`message-size number;`

**Hierarchy Level**  
```
[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],
[edit protocols rip],
[edit protocols rip group group-name neighbor neighbor-name],
[edit routing-instances routing-instance-name protocols rip],
[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]
```

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement for SRX Series devices introduced in Junos OS Release 9.5.  
Statement for J Series platform introduced in Junos OS Release 8.5.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**  
Specify the number of route entries to be included in every RIP update message.

**TIP:** To ensure interoperability with other vendors' equipment, use the standard of 25 route entries per message. Do not change the default number of route entries in a RIP update message.

**Options**  
- `number`—Number of route entries per update message.  
  - **Range:** 25 through 255 entries  
  - **Default:** 25 entries

**Required Privilege**  
- `routing`—To view this statement in the configuration.  
- `routing-control`—To add this statement to the configuration.

**Related Documentation**  
- `Example: Configuring RIP`
## metric-in (Protocols RIP)

**Syntax**

```
metric-in metric;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],
[edit protocols rip],
[edit protocols rip group group-name neighbor neighbor-name],
[edit routing-instances routing-instance-name protocols rip],
[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Specify the metric to add to incoming routes when the routing device advertises into RIP routes that were learned from other protocols. Use this statement to configure the routing device to prefer RIP routes learned through a specific neighbor.

**Options**

- **metric**—Metric value.
  - **Range**: 1 through 16
  - **Default**: 1

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring the Metric Value Added to Imported RIP Routes
## metric-out (Protocols RIP)

### Syntax

```
metric-out metric;
```

### Hierarchy Level

- `[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]`
- `[edit protocols rip group group-name neighbor neighbor-name]`
- `[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]`

### Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

### Description

Specify the metric value to add to routes transmitted to the neighbor. Use this statement to control how other routing devices prefer RIP routes sent from this neighbor.

If you have included the `export` statement, RIP exports routes it has learned to the neighbors configured by including the `neighbor` statement.

The metric associated with a RIP route (unless modified by an export policy) is the normal RIP metric. For example, a RIP route with a metric of 5 learned from a neighbor configured with a `metric-in` value of 2 is advertised with a combined metric of 7 when advertised to RIP neighbors in the same group. However, if this route was learned from a RIP neighbor in a different group or from a different protocol, the route is advertised with the metric value configured for that group with the `metric-out` statement.

The metric for a route can be modified with an export policy. That metric is seen when the route is exported to the next hop.

To increase the metric for routes advertised outside a group, include the `metric-out` statement.

### Options

- **metric**—Metric value.
  - **Range**: 1 through 16
  - **Default**: 1

### Required Privilege Level

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

### Related Documentation

- *Examples: Controlling Traffic with Metrics in a RIP Network*

---

Copyright © 2013, Juniper Networks, Inc.
neighbor (Protocols RIP)

**Syntax**
```
neighbor neighbor-name {
    authentication-key password;
    authentication-type type;
    bfd-liveness-detection {
        authentication {
            algorithm algorithm-name;
            key-chain key-chain-name;
            loose-check;
        }
        detection-time {
            threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        transmit-interval {
            threshold milliseconds;
            minimum-interval milliseconds;
        }
        multiplier number;
        version (0 | 1 | automatic);
    }
    (check-zero | no-check-zero);
    demand-circuit;
    import policy-name;
    max-retrans-time seconds;
    message-size number;
    metric-in metric;
    metric-out metric;
    receive receive-options;
    route-timeout seconds;
    send send-options;
    update-interval seconds;
}
```

**Hierarchy Level**
- [edit logical-systems logical-system-name protocols rip group group-name]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name]
- [edit protocols rip group group-name]
- [edit routing-instances routing-instance-name protocols rip group group-name]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure neighbor-specific RIP parameters, thereby overriding the defaults set for the routing device.

**Options**
- **neighbor-name**—Name of an interface over which a routing device communicates to its neighbors.

The remaining statements are explained separately.
**Required Privilege**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring RIP

---

**preference (Protocols RIP)**

**Syntax**
```
preference preference;
```

**Hierarchy Level**
- [edit logical-systems logical-system-name protocols rip group group-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name],
- [edit protocols rip group group-name],
- [edit routing-instances routing-instance-name protocols rip group group-name]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Specify the preference of external routes learned by RIP as compared to those learned from other routing protocols.

By default, Junos OS assigns a preference of 100 to routes that originate from RIP. When Junos OS determines a route’s preference to become the active route, the software selects the route with the lowest preference and installs this route into the forwarding table.

**Options**
- `preference`—Preference value. A lower value indicates a more preferred route.
- **Range**: 0 through 4,294,967,295 (2^32 – 1)
- **Default**: 100

---

**Required Privilege**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- Route Preferences Overview
receive (Protocols RIP)

Syntax

```
receive receive-options;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],
[edit protocols rip],
[edit protocols rip group group-name neighbor neighbor-name],
[edit routing-instances routing-instance-name protocols rip],
[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Configure RIP receive options.

Options

```
receive-options—One of the following:

- both—Accept both RIP version 1 and version 2 packets.
- none—Do not receive RIP packets.
- version-1—Accept only RIP version 1 packets.
- version-2—Accept only RIP version 2 packets.
```

Default: both

Required Privilege Level

```
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.
```

Related Documentation

- Example: Configuring the Sending and Receiving of RIPv1 and RIPv2 Packets
- send on page 2976
riB-group (Protocols RIP)

Syntax

rib-group group-name;

Hierarchy Level
[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit protocols rip],
[edit routing-instances routing-instance-name protocols rip]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Install RIP routes into multiple routing tables by configuring a routing table group.

Options

group-name—Name of the routing table group.

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Example: Redistributing Routes Between Two RIP Instances

RIP

Syntax

rip {...}

Hierarchy Level
[edit logical-systems logical-system-name protocols],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols]
[edit protocols],
[edit routing-instances routing-instance-name protocols]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Enable RIP routing on the routing device.

Default
RIP is disabled on the routing device.

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Example: Configuring RIP

Copyright © 2013, Juniper Networks, Inc.
route-timeout (Protocols RIP)

Syntax route-timeout seconds;

Hierarchy Level
- [edit logical-systems logical-system-name protocols rip]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip]
- [edit logical-systems logical-system-name protocols rip group group-name]
- [edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]
- [edit protocols rip]
- [edit protocols rip group group-name]
- [edit protocols rip group group-name neighbor neighbor-name]
- [edit routing-instances routing-instance-name protocols rip]
- [edit routing-instances routing-instance-name protocols rip group group-name]
- [edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]

Release Information
- Statement introduced in Junos OS Release 7.6.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Configure the route timeout interval for RIP. If a route is not refreshed after being installed in the routing table by the specified timeout interval, the route is marked as invalid and is removed from the routing table after the hold-down period expires.

Options
- seconds—Estimated time to wait before making updates to the routing table.
  - Range: 30 through 360 seconds
  - Default: 180 seconds

Required Privilege Level
- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

Related Documentation
- Example: Configuring RIP Timers
- RIP Demand Circuits Overview
**send (Protocols RIP)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th><code>send send-options;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit logical-systems <em>logical-system-name</em> protocols <em>rip</em>],</td>
</tr>
<tr>
<td></td>
<td>[edit logical-systems <em>logical-system-name</em> protocols <em>group-name</em> <em>neighbor</em> <em>neighbor-name</em>],</td>
</tr>
<tr>
<td></td>
<td>[edit logical-systems <em>logical-system-name</em> routing-instances <em>routing-instance-name</em> protocols <em>rip</em>],</td>
</tr>
<tr>
<td></td>
<td>[edit logical-systems <em>logical-system-name</em> routing-instances <em>routing-instance-name</em> protocols <em>group-name</em> <em>neighbor</em> <em>neighbor-name</em>],</td>
</tr>
<tr>
<td></td>
<td>[edit protocols <em>rip</em>],</td>
</tr>
<tr>
<td></td>
<td>[edit protocols <em>group-name</em> <em>neighbor</em> <em>neighbor-name</em>],</td>
</tr>
<tr>
<td></td>
<td>[edit routing-instances <em>routing-instance-name</em> protocols <em>rip</em>],</td>
</tr>
<tr>
<td></td>
<td>[edit routing-instances <em>routing-instance-name</em> protocols <em>group-name</em> <em>neighbor</em> <em>neighbor-name</em>]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced before Junos OS Release 7.4.</td>
</tr>
<tr>
<td></td>
<td>Statement introduced in Junos OS Release 9.0 for EX Series switches.</td>
</tr>
<tr>
<td></td>
<td>Statement introduced in Junos OS Release 12.1 for the QFX Series.</td>
</tr>
<tr>
<td>Description</td>
<td>Configure RIP send options.</td>
</tr>
<tr>
<td>Options</td>
<td><code>send-options</code>—One of the following:</td>
</tr>
<tr>
<td></td>
<td>• broadcast—Broadcast RIP version 2 packets (RIP version 1 compatible).</td>
</tr>
<tr>
<td></td>
<td>• multicast—Multicast RIP version 2 packets. This is the default.</td>
</tr>
<tr>
<td></td>
<td>• none—Do not send RIP updates.</td>
</tr>
<tr>
<td></td>
<td>• version-1—Broadcast RIP version 1 packets.</td>
</tr>
<tr>
<td>Default</td>
<td>multicast</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>routing—To view this statement in the configuration.</td>
</tr>
<tr>
<td></td>
<td>routing-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• <em>Example: Configuring the Sending and Receiving of RIPv1 and RIPv2 Packets</em></td>
</tr>
<tr>
<td></td>
<td>• receive on page 2973</td>
</tr>
</tbody>
</table>
traceoptions (Protocols RIP)

Syntax

traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}

Hierarchy Level

[edit logical-systems logical-system-name protocols rip],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],
[edit protocols rip],
[edit routing-instances routing-instance-name protocols rip]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Set RIP protocol-level tracing options.

NOTE: The traceoptions statement is not supported on QFabric systems.

Default

The default RIP protocol-level trace options are inherited from the global traceoptions statement.

Options

disable—(Optional) Disable the tracing operation. One use of this option is to disable a single operation when you have defined a broad group of tracing operations, such as all.

file filename—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. We recommend that you place RIP tracing output in the file /var/log/rip-log.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Range: 2 through 1000 files
Default: 10 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

RIP Tracing Options

- auth—RIP authentication
- error—RIP error packets
• **expiration**—RIP route expiration processing
• **holddown**—RIP hold-down processing
• **nsr-synchronization**—Nonstop routing synchronization events
• **packets**—All RIP packets
• **request**—RIP information packets such as request, poll, and poll entry packets
• **trigger**—RIP triggered updates
• **update**—RIP update packets

**Global Tracing Options**

• **all**—All tracing operations
• **general**—A combination of the **normal** and **route** trace operations
• **normal**—All normal operations

**Default:** If you do not specify this option, only unusual or abnormal operations are traced.

• **policy**—Policy operations and actions
• **route**—Routing table changes
• **state**—State transitions
• **task**—Routing protocol task processing
• **timer**—Routing protocol timer processing

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

• **detail**—Provide detailed trace information.
• **receive**—Trace the packets being received.
• **receive-detail**—Provide detailed trace information for packets being received.
• **send**—Trace the packets being transmitted.
• **send-detail**—Provide detailed trace information for packets being transmitted.

**no-world-readable**—(Optional) Prevent any user from reading the log file.
**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named *trace-file* reaches this size, it is renamed *trace-file.0*. When the *trace-file* again reaches its maximum size, *trace-file.0* is renamed *trace-file.1* and *trace-file* is renamed *trace-file.0*. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option.

**Syntax:**  \(x\) to specify KB,  \(x\) to specify MB, or  \(x\) to specify GB

**Range:**  10 KB through the maximum file size supported on your system

**Default:**  128 KB

**world-readable**—(Optional) Allow any user to read the log file.

**Required Privilege**  
- **Level**  
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**  
- Example: *Tracing RIP Protocol Traffic*
update-interval (Protocols RIP)

Syntax  
update-interval seconds;

Hierarchy Level  
[edit logical-systems logical-system-name protocols rip],  
[edit logical-systems logical-system-name protocols rip group group-name],  
[edit logical-systems logical-system-name protocols rip group group-name neighbor neighbor-name],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name],  
[edit protocols rip],  
[edit protocols rip group group-name],  
[edit protocols rip group group-name neighbor neighbor-name],  
[edit routing-instances routing-instance-name protocols rip],  
[edit routing-instances routing-instance-name protocols rip group group-name],  
[edit routing-instances routing-instance-name protocols rip group group-name neighbor neighbor-name]

Release Information  
Statement introduced in Junos OS Release 7.6.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description  
Configure the interval at which routes learned by RIP are sent to neighbors. This timer controls the interval between routing updates. This timer is set to 30 seconds, by default, with a small random amount of time added when the timer is reset. This added time prevents congestion that can happen if all routing devices update their neighbors simultaneously.

Options  
seconds—Estimated time to wait before making updates to the routing table.  
Range: 10 through 60 seconds  
Default: 30 seconds

Required Privilege  
level routing—to view this statement in the configuration.  
level routing-control—to add this statement to the configuration.

Related Documentation  
• Example: Configuring RIP Timers
Configuration Statements: RIPng

export (Protocols RIPng)

Syntax

```
export [ policy-names ];
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols ripng group group-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name],
- [edit protocols ripng group group-name],
- [edit routing-instances routing-instance-name protocols ripng group group-name]

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for routing instances introduced in Junos OS Release 9.0.

Description

Apply a policy or list of policies to routes being exported to the neighbors.

By default, RIPng does not export routes it has learned to its neighbors. To have RIPng export routes, apply one or more export policies. To apply export policies and to filter routes being exported from the local routing device to its neighbors, include the `export` statement and list the name of the policy to be evaluated.

You can define one or more export policies. If no routes match the policies, the local routing device does not export any routes to its neighbors. Export policies override any metric values determined through calculations involving the values configured with the `metric-in` and `metric-out` statements.

Options

- `policy-names`—Name of one or more policies.

Required Privilege

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation

- `Example: Configuring RIPng`
- `import on page 2985`
graceful-restart (Protocols RIPng)

Syntax
graceful-restart {
  disable;
  restart-time seconds;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols ripng],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng],
[edit protocols ripng],
[edit routing-instances routing-instance-name protocols ripng]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description
Configure graceful restart for RIPng.

Options
disable—Disables graceful restart for RIPng.
The remaining statement is explained separately.

Required Privilege
Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Junos OS High Availability Library for Routing Devices
group (Protocols RIPng)

Syntax

```plaintext
group group-name {
  export [policy-names];
  metric-out metric;
  neighbor neighbor-name {
    import policy-name;
    metric-in metric;
    receive <none>;
    route-timeout seconds;
    send <none>;
    update-interval seconds;
  }
  preference number;
  route-timeout seconds;
  update-interval seconds;
}
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols ripng],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng],
- [edit protocols ripng],
- [edit routing-instances routing-instance-name protocols ripng]

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for routing instances introduced in Junos OS Release 9.0.

Description

Configure a set of RIPng neighbors that share an export policy and metric. The export policy and metric govern what routes to advertise to neighbors in a given group.

Each group must contain at least one neighbor. You should create a group for each export policy that you have.

Options

- `group-name`—Name of a group, up to 16 characters long.

The remaining statements are explained separately.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring RIPng
holddown (Protocols RIPng)

Syntax

holddown seconds;

Hierarchy Level

[edit logical-systems logical-system-name protocols ripng],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng],
[edit protocols ripng],
[edit routing-instances routing-instance-name protocols ripng]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description

Configure how long the expired route is retained in the routing table before being removed.

Options

seconds—Estimated time to wait before removing expired routes from the routing table.
Default: 180 seconds
Range: 10 through 180 seconds

Required Privilege

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring RIPng Timers
import (Protocols RIPng)

**Syntax**

```plaintext
import [ policy-names ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols ripng],
- [edit logical-systems logical-system-name protocols ripng group group-name neighbor neighbor-name],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name],
- [edit protocols ripng],
- [edit protocols ripng group group-name neighbor neighbor-name],
- [edit routing-instances routing-instance-name protocols ripng],
- [edit routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for routing instances introduced in Junos OS Release 9.0.

**Description**

Apply one or more policies to routes being imported into the local routing device from its neighbors.

**Options**

- `policy-names`—Name of one or more policies.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Applying Policies to RIPng Routes Imported from Neighbors*
- *export on page 2981*
metric-in (Protocols RIPng)

Syntax

```plaintext
metric-in metric;
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols ripng]
- [edit logical-systems logical-system-name protocols ripng group group-name neighbor neighbor-name]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng]
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name]
- [edit protocols ripng]
- [edit protocols ripng group group-name neighbor neighbor-name]
- [edit routing-instances routing-instance-name protocols ripng]
- [edit routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name]

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for routing instances introduced in Junos OS Release 9.0.

Description

Specify the metric to add to incoming routes when advertising into RIPng routes that were learned from other protocols. Use this statement to configure the routing device to prefer RIPng routes learned through a specific neighbor.

Options

- **metric**—Metric value.
  - **Range:** 1 through 16
  - **Default:** 1

Required Privilege Level

- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

Related Documentation

- Example: Configuring the Metric Value Added to Imported RIPng Routes
## metric-out (Protocols RIPng)

**Syntax**  
```plaintext
metric-out metric;
```

**Hierarchy Level**  
```plaintext
[edit logical-systems logical-system-name protocols ripng group group-name neighbor neighbor-name],  
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name],  
[edit protocols ripng group group-name neighbor neighbor-name],  
[edit routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name]
```

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Support for routing instances introduced in Junos OS Release 9.0.

**Description**  
Specify the metric value to add to routes transmitted to the neighbor. Use this statement to control how other routing devices prefer RIPng routes sent from this neighbor.

When an export policy is configured, RIPng exports all learned routes to neighbors configured with the `neighbor` statement.

If a route being exported was learned from a member of the same RIPng group, the metric associated with that route (unless modified by an export policy) is the normal RIPng metric. For example, a RIPng route with a metric of 5 learned from a neighbor configured with a `metric-in` value of 2 is advertised with a combined metric of 7 when advertised to RIPng neighbors in the same group. However, if this route was learned from a RIPng neighbor in a different group or from a different protocol, the route is advertised with the metric value configured for that group with the `metric-out` statement. The default value for `metric-out` is 1.

To modify the metric for routes advertised outside a group, include the `metric-out` statement.

**Options**  
- `metric`—Metric value.  
  - **Range:** 1 through 16  
  - **Default:** 1

**Required Privilege Level**  
- `routing`—To view this statement in the configuration.  
- `routing-control`—To add this statement to the configuration.

**Related Documentation**  
- [Example: Configuring the Metric Value Added to Imported RIPng Routes](#)
neighbor (Protocols RIPng)

Syntax

neighbor neighbor-name
  import [policy-names ];
  metric-in metric;
  receive <none>;
  route-timeout seconds;
  send <none>;
  update-interval seconds;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols ripng group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name],
[edit protocols ripng group group-name],
[edit routing-instances routing-instance-name protocols ripng group group-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description
Configure neighbor-specific RIPng parameters, thereby overriding the defaults set for the routing device.

Options
neighbor-name—Name of an interface over which a routing device communicates to its neighbors.

The remaining statements are explained separately.

Required Privilege
level routing—to view this statement in the configuration.
level routing-control—to add this statement to the configuration.

Related Documentation
• Example: Configuring RIPng
preference (Protocols RIPng)

Syntax

preference preference;

Hierarchy Level

[edit logical-systems logical-system-name protocols ripng group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name],
[edit protocols ripng group group-name],
[edit routing-instances routing-instance-name protocols ripng group group-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description

Specify the preference of external routes learned by RIPng as compared to those learned from other routing protocols.

By default, Junos OS assigns a preference of 100 to routes that originate from RIPng. When Junos OS determines that a route is to become the active route, the software selects the route with the lowest preference and installs this route into the forwarding table.

To modify the default RIPng preference value, include the preference statement.

Options

preference—Preference value. A lower value indicates a more preferred route.
Range: 0 through 4,294,967,295 (2^{32} – 1)
Default: 100

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring RIPng
receive (Protocols RIPng)

Syntax

receive <none>;

Hierarchy Level

[edit logical-systems logical-system-name protocols ripng],
[edit logical-systems logical-system-name protocols ripng group group-name neighbor neighbor-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name],
[edit protocols ripng],
[edit protocols ripng group group-name neighbor neighbor-name],
[edit routing-instances routing-instance-name protocols ripng],
[edit routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description

Enable or disable receiving of update messages.

Options

none—(Optional) Disable receiving update messages.
Default: Enabled

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• send on page 2992
• Example: Configuring RIPng
ripng

Syntax  ripng {...}

Hierarchy Level  
[edit logical-systems logical-system-name protocols],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols],
[edit protocols],
[edit routing-instances routing-instance-name protocols]

Release Information  Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description  Enable RIPng routing on the routing device.

Default  RIPng is disabled on the routing device.

Required Privilege  
Level  routing—To view this statement in the configuration.
        routing-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring RIPng

route-timeout (Protocols RIPng)

Syntax  route-timeout seconds;

Hierarchy Level  
[edit logical-systems logical-system-name protocols ripng],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng],
[edit protocols ripng],
[edit routing-instances routing-instance-name protocols ripng]

Release Information  Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description  Configure the route timeout interval for RIPng.

Options  
seconds—Estimated time to wait before making updates to the routing table.
Range: 30 through 360 seconds
Default: 180 seconds

Required Privilege  
Level  routing—To view this statement in the configuration.
        routing-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring RIPng Timers
**send (Protocols RIPng)**

**Syntax**
```
send <none>;
```

**Hierarchy Level**
- [edit logical-systems logical-system-name protocols ripng],
- [edit logical-systems logical-system-name protocols ripng group group-name neighbor neighbor-name],
- [edit logical-systems logical-system-name routing-instances routing-instances-name protocols ripng],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name],
- [edit protocols ripng],
- [edit protocols ripng group group-name neighbor neighbor-name],
- [edit routing-instances routing-instance-name protocols ripng],
- [edit routing-instances routing-instance-name protocols ripng group group-name neighbor neighbor-name]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

**Description**
Enable or disable sending of update messages.

**Options**
- **none**—(Optional) Disable sending of update messages.
- **Default**: Enabled

**Required Privilege Level**
- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**
- receive on page 2990
traceoptions (Protocols RIPng)

Syntax

traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}

Hierarchy Level

[edit logical-systems logical-system-name protocols ripng],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng],
[edit protocols ripng],
[edit routing-instances routing-instance-name protocols ripng]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for routing instances introduced in Junos OS Release 9.0.

Description

Set RIPng protocol-level tracing options.

Default

The default RIPng protocol-level trace options are inherited from the global traceoptions statement.

Options

disable—(Optional) Disable the tracing operation. One use of this option is to disable a single operation when you have defined a broad group of tracing operations, such as all.

file filename—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks. We recommend that you place RIPng tracing output in the file /var/log/ripng-log.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Range: 2 through 1000 files
Default: 10 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

RIPng Tracing Options

• error—RIPng error packets
• expiration—RIPng route expiration processing
• holddown—RIPng hold-down processing
• nsr-synchronization—Nonstop routing synchronization events
• packets—All RIPng packets
- **request**—RIPng information packets such as request, poll, and poll entry packets
- **trigger**—RIPng triggered updates
- **update**—RIPng update packets

**Global Tracing Options**
- **all**—All tracing operations
- **general**—A combination of the **normal** and **route** trace operations
- **normal**—All normal operations

**Default:** If you do not specify this option, only unusual or abnormal operations are traced.
- **policy**—Policy operations and actions
- **route**—Routing table changes
- **state**—State transitions
- **task**—Routing protocol task processing
- **timer**—Routing protocol timer processing

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:
- **detail**—Provide detailed trace information.
- **receive**—Trace the packets being received.
- **receive-detail**—Provide detailed trace information for packets being received.
- **send**—Trace the packets being transmitted.
- **send-detail**—Provide detailed trace information for packets being transmitted.

**no-world-readable**—(Optional) Do not allow any user to read the log file.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option.

**Syntax:** \( xk \) to specify KB, \( xm \) to specify MB, or \( xg \) to specify GB

**Range:** 10 KB through the maximum file size supported on your system

**Default:** 128 KB

**world-readable**—(Optional) Allow any user to read the log file.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>routing-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
Related Documentation

- Example: Tracing RIPng Protocol Traffic

**update-interval (Protocols RIPng)**

**Syntax**

```
update-interval seconds;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols ripng]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols ripng]`
- `[edit protocols ripng]`
- `[edit routing-instances routing-instance-name protocols ripng]`

**Release Information**

- Statement introduced in Junos OS Release 7.6.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for routing instances introduced in Junos OS Release 9.0.

**Description**

Configure the interval at which routes learned by RIPng are sent to neighbors.

**Options**

- `seconds`—Estimated time to wait before making updates to the routing table.
  - **Range:** 10 through 60 seconds
  - **Default:** 30 seconds

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring RIP Timers
CHAPTER 59
Administration

- Routine Monitoring on page 2997
- Operational Commands: RIP on page 2998
- Operational Commands: RIPng on page 3007

Routine Monitoring

- Monitoring RIP Routing Information on page 2997

Monitoring RIP Routing Information

**Purpose**
Use the monitoring functionality to monitor RIP routing on routing devices.

**Action**
To view RIP routing information in the J-Web interface, select **Monitor > Routing > RIP Information**.

To view RIP routing information in the CLI, enter the following CLI commands:

- show rip statistics
- show rip neighbor

**Meaning**
Table 369 on page 2997 summarizes key output fields in the RIP routing display in the J-Web interface.

Table 369: Summary of Key RIP Routing Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP Statistics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Name</td>
<td>The RIP protocol name.</td>
<td></td>
</tr>
<tr>
<td>Port number</td>
<td>The port on which RIP is enabled.</td>
<td></td>
</tr>
<tr>
<td>Hold down time</td>
<td>The interval during which routes are neither advertised nor updated.</td>
<td></td>
</tr>
<tr>
<td>Global routes learned</td>
<td>Number of RIP routes learned on the logical interface.</td>
<td></td>
</tr>
</tbody>
</table>
Table 369: Summary of Key RIP Routing Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global routes held down</td>
<td>Number of RIP routes that are not advertised or updated during the hold-down interval.</td>
<td></td>
</tr>
<tr>
<td>Global request dropped</td>
<td>Number of requests dropped.</td>
<td></td>
</tr>
<tr>
<td>Global responses dropped</td>
<td>Number of responses dropped.</td>
<td></td>
</tr>
</tbody>
</table>

**RIP Neighbors**

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Name of the RIP neighbor.</th>
<th>This value is the name of the interface on which RIP is enabled. Click the name to see the details for this neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the RIP connection: <strong>Up</strong> or <strong>Dn</strong> (Down).</td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>Local source address.</td>
<td>This value is the configured address of the interface on which RIP is enabled.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Destination address.</td>
<td>This value is the configured address of the immediate RIP adjacency.</td>
</tr>
<tr>
<td>Send Mode</td>
<td>The mode of sending RIP messages.</td>
<td></td>
</tr>
<tr>
<td>Receive Mode</td>
<td>The mode in which messages are received.</td>
<td></td>
</tr>
<tr>
<td>In Metric</td>
<td>Value of the incoming metric configured for the RIP neighbor.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring a RIP Network (J-Web Procedure) on page 2951
- Layer 3 Protocols Supported on EX Series Switches on page 2553

**Operational Commands: RIP**
### clear rip general-statistics

**Syntax**

- clear rip general-statistics
  - `<logical-system (all | logical-system-name)>

**Syntax (EX Series Switches and QFX Series)**

- clear rip general-statistics

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Clear RIP general statistics.

**Options**

- **none**—Clear RIP general statistics.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

- clear

**Related Documentation**

- [show rip general-statistics on page 3001](#)

**List of Sample Output**

- clear rip general-statistics on page 2999

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```
clear rip general-statistics

user@host> clear rip general-statistics
```
clear rip statistics

Syntax

clear rip statistics
<instance (all | instance-name)>
<logical-system (all | logical-system-name)>
<neighbor>
<peer (all | address)>

Syntax (EX Series Switches and QFX Series)
clear rip statistics
<instance (all | instance-name)>
<neighbor>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description
Clear RIP statistics.

Options
none—Reset RIP counters for all neighbors for all routing instances.

instance (all | instance-name)—(Optional) Clear RIP statistics for all instances or for the specified routing instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

neighbor—(Optional) Clear RIP statistics for the specified neighbor only.

peer (all | address)—(Optional) Clear RIP statistics for a single peer or all peers.

Required Privilege
Level
clear

Related Documentation
• show rip statistics on page 3005

List of Sample Output
clear rip statistics on page 3000

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
clear rip statistics

user@host> clear rip statistics
show rip general-statistics

Syntax

show rip general-statistics
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches and QFX Series)

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description

Display brief RIP statistics.

Options
none—Display brief RIP statistics.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

Level view

Related Documentation

• clear rip general-statistics on page 2999

List of Sample Output

show rip general-statistics on page 3001

Output Fields

Table 370 on page 3001 lists the output fields for the show rip general-statistics command. Output fields are listed in the approximate order in which they appear.

Table 370: show rip general-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad msgs</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>no recv intf</td>
<td>Number of packets received with no matching interface.</td>
</tr>
<tr>
<td>curr memory</td>
<td>Amount of memory currently used by RIP.</td>
</tr>
<tr>
<td>max memory</td>
<td>Most memory used by RIP.</td>
</tr>
</tbody>
</table>

Sample Output

show rip general-statistics

user@host> show rip general-statistics
RIPv2 I/O info:
bad msgs : 0
no recv intf : 0
<table>
<thead>
<tr>
<th>curr memory</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>max memory</td>
<td>0</td>
</tr>
</tbody>
</table>
show rip neighbor

Syntax
show rip neighbor
<instance (all | instance-name)>
<logical-system (all | logical-system-name)>
<name>

Syntax (EX Series Switches and QFX Series)
show rip neighbor
<instance (all | instance-name)>
<name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.1 for the QFX Series.

Description
Display information about RIP neighbors.

Options
none—Display information about all RIP neighbors for all instances.

instance (all | instance-name)—(Optional) Display RIP neighbor information for all instances or for only the specified routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

name—(Optional) Display detailed information about only the specified RIP neighbor.

Required Privilege Level
view

List of Sample Output
show rip neighbor on page 3004
show rip neighbor (With Demand Circuits Configured) on page 3004

Output Fields
Table 371 on page 3003 lists the output fields for the show rip neighbor command. Output fields are listed in the approximate order in which they appear.

Table 371: show rip neighbor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the RIP neighbor.</td>
</tr>
</tbody>
</table>

NOTE: Beginning with Junos OS Release 11.1, when you configure demand circuits, the output displays a demand circuit (DC) flag next to neighbor interfaces configured for demand circuits.

If you configure demand circuits at the [edit protocols rip group group-name neighbor neighbor-name] hierarchy level, the output shows only the neighboring interface that you specifically configured as a demand circuit. If you configure demand circuits at the [edit protocols rip group group-name] hierarchy level, all of the interfaces in the group are configured as demand circuits. Therefore, the output shows all of the interfaces in that group as demand circuits.
Table 371: show rip neighbor Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the connection: <strong>Up</strong> or <strong>Dn</strong> (Down).</td>
</tr>
<tr>
<td>Source Address</td>
<td>Address of the port on the local router.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Address of the port on the remote router.</td>
</tr>
<tr>
<td>Send Mode</td>
<td>Send options: <strong>broadcast</strong>, <strong>multicast</strong>, <strong>none</strong>, or <strong>version 1</strong>.</td>
</tr>
<tr>
<td>Receive Mode</td>
<td>Type of packets to accept: <strong>both</strong>, <strong>none</strong>, <strong>version 1</strong>, or <strong>version 2</strong>.</td>
</tr>
<tr>
<td>In Met</td>
<td>Metric added to incoming routes when advertising into RIP routes that were learned from other protocols.</td>
</tr>
</tbody>
</table>

Sample Output

**show rip neighbor**

```
user@host> show rip neighbor

Neighbor   Local State Address           Source Address           Destination Address    Send Mode  Receive Mode  In Met
---------- ------ ----------------- -------------- ------------------ -----------------------------
ge-2/3/0.0  Up    192.168.9.105     192.168.9.107     bcast            both         1
at-5/1/1.42 Dn    (null)             (null)            mcast            v2 only        3
at-5/1/0.42 Dn    (null)             (null)            mcast            both           3
at-5/1/0.0   Up    20.0.0.1           224.0.0.9        mcast            both           3
so-0/0/0.0   Up    192.168.9.97      224.0.0.9        mcast            both           3
```

**show rip neighbor (With Demand Circuits Configured)**

```
user@host> show rip neighbor

Neighbor   Local State Address           Source Address           Destination Address    Send Mode  Receive Mode  In Met
---------- ------ ----------------- -------------- ------------------ -----------------------------
so-0/1/0.0(DC) Up    10.10.10.2        224.0.0.9        mcast            both           1
so-0/2/0.0(DC) Up    13.13.13.2        224.0.0.9        mcast            both           1
```
show rip statistics

**Syntax**

```
show rip statistics
<instance (all | instance-name)>
<logical-system (all | logical-system-name)>
<name>
<peer (all | address)>
```

**Syntax (EX Series Switches and QFX Series)**

```
show rip statistics
<instance (all | instance-name)>
<name>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Display RIP statistics about messages sent and received on an interface, as well as information received from advertisements from other routing devices.

**Options**

- **none**—Display RIP statistics for all routing instances.
- **instance (all | instance-name)**—(Optional) Display RIP statistics for all instances or for only the specified routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **name**—(Optional) Display detailed information about only the specified RIP neighbor.
- **peer (all | address)**—(Optional) Display RIP statistics for a single peer or all peers.

**Required Privilege Level**

```
view
```

**Related Documentation**

- clear rip statistics on page 3000

**List of Sample Output**

```
show rip statistics on page 3006
```

**Output Fields**

Table 372 on page 3006 lists the output fields for the show rip statistics command. Output fields are listed in the approximate order in which they appear.
## Table 372: show rip statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RIP info</strong></td>
<td>Information about RIP on the specified interface:</td>
</tr>
<tr>
<td>port</td>
<td>UDP port number used for RIP.</td>
</tr>
<tr>
<td>update interval</td>
<td>Interval between routing table updates, in seconds.</td>
</tr>
<tr>
<td>holddown</td>
<td>Hold-down interval, in seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout interval, in seconds.</td>
</tr>
<tr>
<td>restart in progress</td>
<td>Graceful restart status. Displayed when RIP is or has been in the process of graceful restart.</td>
</tr>
<tr>
<td>restart time</td>
<td>Estimated time for the graceful restart to finish, in seconds.</td>
</tr>
<tr>
<td>restart will complete in</td>
<td>Remaining time for the graceful restart to finish, in seconds.</td>
</tr>
<tr>
<td>rts learned</td>
<td>Number of routes learned through RIP.</td>
</tr>
<tr>
<td>rts held down</td>
<td>Number of routes held down by RIP.</td>
</tr>
<tr>
<td>rqsts dropped</td>
<td>Number of received request packets that were dropped.</td>
</tr>
<tr>
<td>resps dropped</td>
<td>Number of received response packets that were dropped.</td>
</tr>
<tr>
<td><strong>logical-interface</strong></td>
<td>Name of the logical interface and its statistics:</td>
</tr>
<tr>
<td>routes learned</td>
<td>Number of routes learned on the logical interface.</td>
</tr>
<tr>
<td>routes advertised</td>
<td>Number of routes advertised by the logical interface.</td>
</tr>
<tr>
<td><strong>Counter</strong></td>
<td>List of counter types:</td>
</tr>
<tr>
<td>Updates Sent</td>
<td>Number of update messages sent.</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>Number of triggered update messages sent.</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>Number of response messages sent.</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>RIPv1 Updates Received</td>
<td>Number of RIPv1 update messages received.</td>
</tr>
<tr>
<td>RIPv1 Bad Route Entries</td>
<td>Number of RIPv1 invalid route entry messages received.</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored</td>
<td>Number of RIPv1 update messages ignored.</td>
</tr>
<tr>
<td>RIPv2 Updates Received</td>
<td>Number of RIPv2 update messages received.</td>
</tr>
<tr>
<td>RIPv2 Bad Route Entries</td>
<td>Number of RIPv2 invalid route entry messages received.</td>
</tr>
<tr>
<td>RIPv2 Updates Ignored</td>
<td>Number of RIPv2 update messages ignored.</td>
</tr>
<tr>
<td>Authentication Failures</td>
<td>Number of received update messages that failed authentication.</td>
</tr>
<tr>
<td>RIP Requests Received</td>
<td>Number of RIP request messages received.</td>
</tr>
<tr>
<td>RIP Requests Ignored</td>
<td>Number of RIP request messages ignored.</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>Total number of packets for the selected counter.</td>
</tr>
<tr>
<td><strong>Last 5 min</strong></td>
<td>Number of packets for the selected counter in the most recent 5-minute period.</td>
</tr>
<tr>
<td><strong>Last minute</strong></td>
<td>Number of packets for the selected counter in the most recent 1-minute period.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show rip statistics

user@host>  show rip statistics so-0/0/0.0
```
**RIP info:** port 520; update interval: 30s; holddown 180s; timeout 120s
restart in progress: restart time 60s; restart will complete in 55s

ts learned  rts held down  rqsts dropped  resps dropped
0              0              0              0

so-0/0/0.0:  0 routes learned; 501 routes advertised

<table>
<thead>
<tr>
<th>Counter</th>
<th>Total</th>
<th>Last 5 min</th>
<th>Last minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Updates Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Bad Route Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Updates Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Bad Route Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Authentication Failures</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIP Requests Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIP Requests Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Operational Commands:** RIPng
clear ripng general-statistics

Syntax
clear ripng general-statistics
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)
clear ripng general-statistics

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Clear RIP next generation (RIPng) general statistics.

Options
none—Clear RIPng general statistics.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
Level
clear

Related Documentation
• show ripng general-statistics on page 3010

List of Sample Output
clear ripng general-statistics on page 3008

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
clear ripng general-statistics

user@host> clear ripng general-statistics
clear ripng statistics

**Syntax**
```
clear ripng statistics
<instance | name>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch)**
```
clear ripng statistics
<instance | name>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Clear RIP next-generation (RIPng) statistics.

**Options**
- **none**—Reset RIPng counters for all neighbors for all routing instances.
- **instance**—(Optional) Reset RIPng counters for the specified instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **name**—(Optional) Reset RIPng counters for the specified neighbor.

**Required Privilege**
clear

**Related Documentation**
- show ripng statistics on page 3013

**List of Sample Output**
clear ripng statistics on page 3009

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear ripng statistics
```
user@host> clear ripng statistics
```
show ripng general-statistics

**Syntax**

show ripng general-statistics

<logical-system (all | logical-system-name)>

**Syntax (EX Series Switch)**

show ripng general-statistics

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display general RIP next-generation (RIPng) statistics.

**Options**

none—Display general RIPng statistics.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

view

**Related Documentation**

- clear ripng general-statistics on page 3008

**List of Sample Output**

show ripng general-statistics on page 3010

**Output Fields**

Table 373 on page 3010 lists the output fields for the `show ripng general-statistics` command. Output fields are listed in the approximate order in which they appear.

Table 373: show ripng general-statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bad msgs</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>no recv intf</td>
<td>Number of packets received with no matching interface.</td>
</tr>
<tr>
<td>curr memory</td>
<td>Amount of memory currently used by RIPng.</td>
</tr>
<tr>
<td>max memory</td>
<td>Most memory used by RIPng.</td>
</tr>
</tbody>
</table>

**Sample Output**

show ripng general-statistics

```
user@host> show ripng general-statistics
RIPng I/O info:
bad msgs      : 0
no recv intf  : 0
curr memory   : 0
max memory    : 0
```
show ripng neighbor

Syntax

show ripng neighbor
<logical-system (all | logical-system-name)>
:name>

Syntax (EX Series Switch)

show ripng neighbor
:name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display information about RIP next-generation (RIPng) neighbors.

Options

none—Display information about all RIPng neighbors.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

name—(Optional) Display detailed information about a specific RIPng neighbor.

Required Privilege Level

view

List of Sample Output

show ripng neighbor on page 3012

Output Fields

Table 374 on page 3011 lists the output fields for the show ripng neighbor command. Output fields are listed in the approximate order in which they appear.

Table 374: show ripng neighbor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Name of RIPng neighbor.</td>
</tr>
<tr>
<td>State</td>
<td>State of the connection: Up or Dn (Down).</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Destination address.</td>
</tr>
<tr>
<td>Send</td>
<td>Send options: broadcast, multicast, none, version 1, or yes.</td>
</tr>
<tr>
<td>Recv</td>
<td>Type of packets to accept: both, none, version 1, or yes.</td>
</tr>
<tr>
<td>In Met</td>
<td>Metric added to incoming routes when advertising into RIPng routes that were learned from other protocols.</td>
</tr>
</tbody>
</table>
Sample Output

show ripng neighbor

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>State</th>
<th>Source Address</th>
<th>Dest Address</th>
<th>Send</th>
<th>Recv</th>
<th>Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe-0/0/2.0</td>
<td>Up</td>
<td>fe80::290:69ff:fe68:b002</td>
<td>ff02::9</td>
<td>yes</td>
<td>yes</td>
<td>1</td>
</tr>
</tbody>
</table>
show ripng statistics

Syntax

show ripng statistics

<logical-system (all | logical-system-name) >
<name>

Syntax (EX Series Switch)

show ripng statistics

<name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display RIP next generation (RIPng) statistics about messages sent and received on an interface, as well as information received from advertisements from other routing devices.

Options

none—Display RIPng statistics for all neighbors.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

name—(Optional) Display detailed information about a specific RIPng neighbor.

Required Privilege

view

Related Documentation

• clear ripng statistics on page 3009

List of Sample Output

show ripng statistics on page 3014

Output Fields

Table 375 on page 3013 lists the output fields for the show ripng statistics command. Output fields are listed in the approximate order in which they appear.

Table 375: show ripng statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPng info</td>
<td>Information about RIPng on the specified interface:</td>
</tr>
<tr>
<td></td>
<td>• port—UDP port number used for RIPng.</td>
</tr>
<tr>
<td></td>
<td>• holddown—Hold-down interval, in seconds.</td>
</tr>
<tr>
<td></td>
<td>• rts learned—Number of routes learned through RIPng.</td>
</tr>
<tr>
<td></td>
<td>• rts held down—Number of routes held down by RIPng.</td>
</tr>
<tr>
<td></td>
<td>• rqsts dropped—Number of received request packets that were dropped.</td>
</tr>
<tr>
<td></td>
<td>• resps dropped—Number of received response packets that were dropped.</td>
</tr>
<tr>
<td></td>
<td>• restart—Graceful restart status. Displayed when RIPng is or has been in the process of graceful restart.</td>
</tr>
</tbody>
</table>
### Table 375: show ripng statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interface</strong></td>
<td>Name of the logical interface and its statistics:</td>
</tr>
<tr>
<td>routes learned</td>
<td>Number of routes learned on the logical interface.</td>
</tr>
<tr>
<td>routes advertised</td>
<td>Number of routes advertised by the logical interface.</td>
</tr>
<tr>
<td>timeout</td>
<td>Timeout interval, in seconds.</td>
</tr>
<tr>
<td>update interval</td>
<td>Interval between routing table updates, in seconds.</td>
</tr>
<tr>
<td><strong>Counter</strong></td>
<td>List of counter types:</td>
</tr>
<tr>
<td>Updates Sent</td>
<td>Number of update messages sent.</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>Number of triggered update messages sent.</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>Number of response messages sent.</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>Number of invalid messages received.</td>
</tr>
<tr>
<td>Updates Received</td>
<td>Number of RIPng update messages received.</td>
</tr>
<tr>
<td>Bad Route Entries</td>
<td>Number of RIPng invalid route entry messages received.</td>
</tr>
<tr>
<td>Updates Ignored</td>
<td>Number of RIPng update messages ignored.</td>
</tr>
<tr>
<td>RIPng Requests Received</td>
<td>Number of RIPng request messages received.</td>
</tr>
<tr>
<td>RIPng Requests Ignored</td>
<td>Number of RIPng request messages ignored.</td>
</tr>
</tbody>
</table>

| **Total** | Total number of packets for the selected counter. |
| **Last 5 min** | Number of packets for the selected counter in the most recent 5-minute period. |
| **Last minute** | Number of packets for the selected counter in the most recent 1-minute period. |

### Sample Output

```
show ripng statistics
RIPng info: port 521; holddown 120s;
                rts learned  rts held down  rqsts dropped  resps dropped
so-0/1/3.0:    0              0              0              0

so-0/1/3.0:  0 routes learned; 1 routes advertised; timeout 180s; update interval 20s

<table>
<thead>
<tr>
<th>Counter</th>
<th>Total</th>
<th>Last 5 min</th>
<th>Last minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates Sent</td>
<td>934</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Updates Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Route Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPng Requests Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPng Requests Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
PART 20

Routing Options

- Overview on page 3017
- Configuration on page 3023
- Administration on page 3133
CHAPTER 60

Overview

- Layer 3 Protocols on page 3017
- Routing Options Overview on page 3020

Layer 3 Protocols

- Layer 3 Protocols Supported on EX Series Switches on page 3017
- Layer 3 Protocols Not Supported on EX Series Switches on page 3018

Layer 3 Protocols Supported on EX Series Switches

EX Series switches support the Junos OS Layer 3 features and configuration statements listed in Table 326 on page 2553:

Table 376: Supported Junos OS Layer 3 Protocol Statements and Features

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>BFD</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>ICMP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>IGMPv1, v2, and v3</td>
<td>Fully supported.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>MLD</td>
<td>Fully supported (MLD versions 1 and 2).</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>MPLS</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS MPLS Applications Configuration Guide</td>
</tr>
<tr>
<td>OSPFv1, v2 and v3</td>
<td>Supported, with the exceptions noted in “Layer 3 Protocols Not Supported on EX Series Switches” on page 2554.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
</tbody>
</table>
### Table 376: Supported Junos OS Layer 3 Protocol Statements and Features (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Notes</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td>Fully supported on EX3200, EX3300, EX4200, EX6200, and EX8200 switches.</td>
<td>Junos OS Multicast Protocols Configuration Guide</td>
</tr>
<tr>
<td>PPM</td>
<td>Supported. See “EX Series Switch Software Features Overview” on page 27 for specific platform information.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIP</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>RIPng</td>
<td>Fully supported.</td>
<td>Junos OS Routing Protocols Configuration Guide</td>
</tr>
<tr>
<td>SNMP</td>
<td>Fully supported.</td>
<td>Junos OS Network Management Configuration Guide</td>
</tr>
<tr>
<td>VRRP</td>
<td>Fully supported.</td>
<td>See “Understanding VRRP on EX Series Switches” on page 2220. See also Junos OS High Availability Guide.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Layer 3 Protocols Not Supported on EX Series Switches on page 2554
- EX Series Switch Software Features Overview on page 27

### Layer 3 Protocols Not Supported on EX Series Switches

EX Series switches do not support the Junos OS Layer 3 protocols and features listed in Table 327 on page 2554:

### Table 377: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVMRP</td>
<td>• dvmrp and subordinate statements</td>
</tr>
<tr>
<td>Flow aggregation (cflowd)</td>
<td>• cflow and subordinate statements</td>
</tr>
<tr>
<td>IPSec</td>
<td>• [edit services] statements related to IPSec</td>
</tr>
<tr>
<td>IS-IS:</td>
<td>• cns-routing statement</td>
</tr>
<tr>
<td></td>
<td>• ipv6-multicast statement</td>
</tr>
<tr>
<td></td>
<td>• lsp-interval statement</td>
</tr>
<tr>
<td></td>
<td>• label-switched-path statement</td>
</tr>
<tr>
<td></td>
<td>• lsp-lifetime statement</td>
</tr>
<tr>
<td></td>
<td>• te-metric statement</td>
</tr>
<tr>
<td>Logical routers</td>
<td>• logical-routers and subordinate statements</td>
</tr>
</tbody>
</table>
Table 377: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MPLS:</strong></td>
<td></td>
</tr>
<tr>
<td>• Fast Reroute (FRR)</td>
<td></td>
</tr>
<tr>
<td>• Label Distribution Protocol (LDP) (except on EX8200 switches)</td>
<td></td>
</tr>
<tr>
<td>• Layer 3 VPNs (except on EX8200 switches)</td>
<td></td>
</tr>
<tr>
<td>• Multiprotocol BGP (MP-BGP) for VPN-IPv4 family</td>
<td></td>
</tr>
<tr>
<td>• Pseudowire emulation (PWE3)</td>
<td></td>
</tr>
<tr>
<td>• Routing policy statements related to Layer 3 VPNs and MPLS (except on EX8200 switches)</td>
<td></td>
</tr>
<tr>
<td>• Virtual Private LAN Service (VPLS)</td>
<td></td>
</tr>
<tr>
<td><strong>Network Address Translation (NAT)</strong></td>
<td>nat and subordinate statements</td>
</tr>
<tr>
<td><strong>OSPF</strong></td>
<td></td>
</tr>
<tr>
<td>• demand-circuit statement</td>
<td></td>
</tr>
<tr>
<td>• label-switched-path and subordinate statements</td>
<td></td>
</tr>
<tr>
<td>• neighbor statement within an OSPF area</td>
<td></td>
</tr>
<tr>
<td>• peer-interface and subordinate statements within an OSPF area</td>
<td></td>
</tr>
<tr>
<td>• sham-link statement</td>
<td></td>
</tr>
<tr>
<td>• te-metric statement</td>
<td></td>
</tr>
<tr>
<td><strong>PIM SM</strong></td>
<td>Not supported on EX2200 switches</td>
</tr>
<tr>
<td><strong>PIM SSM</strong></td>
<td>Not supported on EX2200 switches</td>
</tr>
<tr>
<td><strong>PIM DM</strong></td>
<td>Not supported on EX2200 or EX4500 switches</td>
</tr>
<tr>
<td><strong>PIM:</strong></td>
<td></td>
</tr>
<tr>
<td>• IPv6</td>
<td>inet6 family (EX2200 and EX4500 switches)</td>
</tr>
<tr>
<td><strong>PPM</strong></td>
<td>Not supported on EX2200 and EX3300 switches</td>
</tr>
<tr>
<td><strong>Routing instances:</strong></td>
<td></td>
</tr>
<tr>
<td>• Routing instance forwarding</td>
<td>i2vpn and subordinate statements (except on EX8200 switches)</td>
</tr>
<tr>
<td>• ldp and subordinate statements (except on EX8200 switches)</td>
<td></td>
</tr>
<tr>
<td>• vpls and subordinate statements</td>
<td></td>
</tr>
<tr>
<td><strong>Routed VLAN interfaces (RVIs)</strong></td>
<td>family mpls statement</td>
</tr>
</tbody>
</table>
### Table 377: Junos OS Layer 3 Protocol Statements and Features That Are Not Supported (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Configuration Statements Not Supported on EX Series Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP and SDP</td>
<td>• sap and all subordinate statements</td>
</tr>
<tr>
<td>General routing options in the <strong>routing-options</strong> hierarchy:</td>
<td>• auto-export and subordinate statements</td>
</tr>
<tr>
<td>• MPLS and label-switched-paths</td>
<td>• dynamic-tunnels and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• lsp-next-hop and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• multicast and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• p2mp-lsp-next-hop and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• route-distinguisher-id statement (except on EX8200 switches)</td>
</tr>
<tr>
<td>Traffic sampling and forwarding in the <strong>forwarding-options</strong> hierarchy</td>
<td>• accounting and subordinate statements</td>
</tr>
<tr>
<td></td>
<td>• family mpls and family multiservice under hash-key hierarchy</td>
</tr>
<tr>
<td></td>
<td>• Under monitoring group-name family inet output hierarchy:</td>
</tr>
<tr>
<td></td>
<td>• cflowd statement</td>
</tr>
<tr>
<td></td>
<td>• export-format-cflowd-version-5 statement</td>
</tr>
<tr>
<td></td>
<td>• flow-active-timeout statement</td>
</tr>
<tr>
<td></td>
<td>• flow-export-destination statement</td>
</tr>
<tr>
<td></td>
<td>• flow-inactive-timeout statement</td>
</tr>
<tr>
<td></td>
<td>• interface statement</td>
</tr>
<tr>
<td></td>
<td>• port-mirroring statement (On EX Series switches, port mirroring is implemented using the analyzer statement.)</td>
</tr>
<tr>
<td></td>
<td>• sampling and subordinate statements</td>
</tr>
</tbody>
</table>

### Related Documentation

- Layer 3 Protocols Supported on EX Series Switches on page 2553
- EX Series Switch Software Features Overview on page 27

### Routing Options Overview

- Understanding Distributed Periodic Packet Management on EX Series Switches on page 3020

### Understanding Distributed Periodic Packet Management on EX Series Switches

Periodic packet management (PPM) is responsible for processing a variety of time-sensitive periodic tasks for particular processes so that other processes on the Juniper Networks EX Series Ethernet Switch can more optimally direct their resources. PPM is responsible for the periodic transmission of packets on behalf of its various client processes, which include the processes that control the Link Aggregation Control Protocol (LACP) and Bidirectional Forwarding Detection (BFD) protocols, and also for receiving packets on behalf of these client processes. PPM also gathers some statistics and sends process-specific packets. PPM cannot be disabled and is always running on any operational switch.

The responsibility for PPM processing on the switch is distributed between the Routing Engine and either the access interfaces (on EX3200, EX4200, and EX4500 switches) or
the line cards (on EX6200 and EX8200 switches) for all protocols that use PPM by default. This distributed model provides a faster response time for protocols that use PPM than the response time provided by the nondistributed model.

If distributed PPM is disabled, the PPM process runs on the Routing Engine only.

You can disable distributed PPM for all protocols that use PPM. You can also disable distributed PPM for LACP packets only.

**BEST PRACTICE:** We recommend that, generally, you disable distributed PPM only if Juniper Networks Customer Service advises you to do so. You should disable distributed PPM only if you have a compelling reason to disable it.

**Related Documentation**
- Configuring Distributed Periodic Packet Management on an EX Series Switch (CLI Procedure) on page 3026
CHAPTER 61

Configuration

- Configuration Tasks on page 3023
- Configuration Statements on page 3028

Configuration Tasks

- Configuring Static Routing (CLI Procedure) on page 3024
- Configuring Static Routing (J-Web Procedure) on page 3024
- Configuring Distributed Periodic Packet Management on an EX Series Switch (CLI Procedure) on page 3026
Configuring Static Routing (CLI Procedure)

Static routes are routes that are manually configured and entered into the routing table. Dynamic routes, in contrast, are learned by the EX Series switch and added to the routing table using a protocol such as OSPF or RIP.

The switch uses static routes:

- When the switch does not have a route to a destination that has a better (lower) preference value. The preference is an arbitrary value in the range from 0 through 255 that the software uses to rank routes received from different protocols, interfaces, or remote systems. The routing protocol process generally determines the active route by selecting the route with the lowest preference value. In the given range, 0 is the lowest and 255 is the highest.
- When the switch cannot determine the route to a destination.
- When the switch is forwarding unroutable packets.

To configure basic static route options using the CLI:

- To configure the switch's default gateway:

  ```
  [edit]
  user@switch# set routing-options static route 0.0.0.0/0 next-hop 10.0.1.1
  ```

- To configure a static route and specify the next address to be used when routing traffic to the static route:

  ```
  [edit]
  user@switch# set routing-options static route 20.0.0.0/24 next-hop 10.0.0.2.1
  ```

- To always keep the static route in the forwarding table:

  ```
  [edit]
  user@switch# set routing-options static route 20.0.0.0/24 retain
  ```

- To prevent the static route from being readvertised:

  ```
  [edit]
  user@switch# set routing-options static route 20.0.0.0/24 no-readvertise
  ```

- To remove inactive routes from the forwarding table:

  ```
  [edit]
  user@switch# set routing-options static route 20.0.0.0/24 active
  ```

Related Documentation

- Configuring Static Routing (J-Web Procedure) on page 3024
- Monitoring Routing Information on page 3133

Configuring Static Routing (J-Web Procedure)

You can use the J-Web interface to configure static routes for EX Series switches.

To configure static routes:

1. Select **Configure > Routing > Static Routing**. The Static Routing page displays details of the configured routes.
NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

- **Add**—To configure a route. Enter information into the routing page as described in Table 378 on page 3025.

- **Edit**—To modify an existing route. Enter information into the routing page as described in Table 378 on page 3025.

- **Delete**—To delete an existing route.

### Table 378: Static Routing Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Default Route     | Specifies the default gateway for the switch. | To specify an IPv4 address:  
2. Type an IP address—for example, 10.10.10.10.  
3. Enter the subnet mask or address prefix.  
   For example, 24 bits represents 255.255.255.0.  
To specify an IPv6 address:  
2. Type an IP address—for example, 2001:ab8:85a3::8a2e:370:7334.  
3. Enter the subnet mask or address prefix.  |
| Static Routes     |                                               |                                                                             |
Table 378: Static Routing Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexthop</td>
<td>Specifies the next-hop address or addresses to be used when routing</td>
<td>To add an address:</td>
</tr>
<tr>
<td></td>
<td>traffic to the static route.</td>
<td>1. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In the IP address dialog, enter the IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If a route has multiple next-hop addresses, traffic is routed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>across each address in round-robin fashion.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a next-hop address, select it from the list and click Delete.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring Static Routing (CLI Procedure) on page 3024
- Monitoring Routing Information on page 3133
- Layer 3 Protocols Supported on EX Series Switches on page 2553

### Configuring Distributed Periodic Packet Management on an EX Series Switch (CLI Procedure)

Periodic packet management (PPM) is responsible for processing a variety of time-sensitive periodic tasks so that other processes on the EX Series switch can more optimally direct their resources.

The responsibility for PPM processing on the switch is distributed between the Routing Engine and either the access interfaces (on EX3200, EX4200, and EX4500 switches) or the line cards (on EX6200 and EX8200 switches) for all protocols that use PPM by default. This distributed model provides a faster response time for protocols that use PPM than the response time provided by the nondistributed model.

If distributed PPM is disabled, the PPM process runs on the Routing Engine only.

You can disable distributed PPM for all protocols that use PPM. You can also disable distributed PPM for LACP packets only.

**BEST PRACTICE:** We recommend that, generally, you disable distributed PPM only if Juniper Networks Customer Service advises you to do so. You should disable distributed PPM only if you have a compelling reason to disable it.

This topic describes:
- Disabling or Enabling Distributed Periodic Packet Management Globally on page 3027
- Disabling or Enabling Distributed Periodic Packet Management for LACP Packets on page 3027
Disabling or Enabling Distributed Periodic Packet Management Globally

Distributed PPM is enabled by default. Disable distributed PPM if you need to move all PPM processing to the Routing Engine. Enable distributed PPM if it was previously disabled and you need to run distributed PPM.

To disable distributed PPM:
```
[edit routing-options]
user@switch# set ppm no-delegate-processing
```

To enable distributed PPM if it was previously disabled:
```
[edit routing-options]
user@switch# delete ppm no-delegate-processing
```

Disabling or Enabling Distributed Periodic Packet Management for LACP Packets

Distributed PPM is enabled by default. Disable distributed PPM for only LACP packets if you need to move all PPM processing for LACP packets to the Routing Engine.

To disable distributed PPM for LACP packets:
```
[edit protocols]
user@switch# set lacp ppm centralized
```

To enable distributed PPM for LACP packets if it was previously disabled:
```
[edit protocols]
user@switch# delete lacp ppm centralized
```

Related Documentation

- Understanding Distributed Periodic Packet Management on EX Series Switches on page 3020
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272
Configuration Statements
Syntax (active | passive):

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-options (aggregate | generate | static) (defaults | route)],
[edit routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-optionsrib routing-table-name (aggregate | generate | static) (defaults | route)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description
Determine whether static, aggregate, or generated routes are removed from the routing and forwarding tables when they become inactive. Static routes are only removed from the routing table if the next hop becomes unreachable. This can occur if the local or neighbor interface goes down. Routes that have been configured to remain continually installed in the routing and forwarding tables are marked with reject next hops when they are inactive.

- active—Remove a route from the routing and forwarding tables when it becomes inactive.
- passive—Have a route remain continually installed in the routing and forwarding tables even when it becomes inactive.

Include the active statement when configuring an individual route in the route portion of the static statement to override a passive option specified in the defaults portion of the statement.

Default active

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
- Examples: Configuring Static Routes
- Example: Summarizing Routes Through Route Aggregation
- Example: Conditionally Generating Static Routes
aggregate (Routing)

Syntax

aggregate {
  defaults {
    ... aggregate-options ...
  }
  route destination-prefix {
    policy policy-name;
    ... aggregate-options ...
  }
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name],
[edit logical-systems logical-system-name routing-options],
[edit logical-systems logical-system-name routing-options rib routing-table-name],
[edit routing-instances routing-instance-name routing-options rib routing-table-name],
[edit routing-options rib routing-table-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Configure aggregate routes.

Options

aggregate-options—Additional information about aggregate routes that is included with the route when it is installed in the routing table. Specify zero or more of the following options in aggregate-options. Each option is explained separately.

- (active | passive);
- as-path <as-path> <origin (egp | igp | incomplete)> <atomic-aggregate> <aggregator as-number ip-address>;
- (brief | full);
- community [ community-ids ];
- discard;
- (metric | metric2 | metric3 | metric4) value <type type>;
- (preference | preference2 | color | color2) preference <type type>;
- tag string;

defaults—Specify global aggregate route options. These options only set default attributes inherited by all newly created aggregate routes. These are treated as global defaults
and apply to all the aggregate routes you configure in the `aggregate` statement. This part of the `aggregate` statement is optional.

`route destination-prefix`—Configure a nondefault aggregate route:

- `default`—For the default route to the destination. This is equivalent to specifying an IP address of 0.0.0.0/0.
- `destination-prefix/prefix-length`—`destination-prefix` is the network portion of the IP address, and `prefix-length` is the destination prefix length.

The `policy` statement is explained separately.

**Required Privilege**
- Level
  - `routing`—To view this statement in the configuration.
  - `routing-control`—To add this statement to the configuration.

**Related Documentation**
- Example: *Summarizing Routes Through Route Aggregation*
as-path (Routing Options)

Syntax
```
as-path <as-path> <aggregator as-number ip-address> <atomic-aggregate> <origin (egp | igp | incomplete)>:
```

Hierarchy Level
```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate | static) (defaults | route)],
[edit routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-options (aggregate | generate | static) (defaults | route)],
[edit routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)]
```

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description
Associate BGP autonomous system (AS) path information with a static, aggregate, or generated route.

In Junos OS Release 9.1 and later, the numeric range for the AS number is extended to provide BGP support for 4-byte AS numbers as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*. RFC 4893 introduces two new optional transitive BGP attributes, AS4 Path and AS4_AGGREGATOR. These new attributes are used to propagate 4-byte AS path information across BGP speakers that do not support 4-byte AS numbers. RFC 4893 also introduces a reserved, well-known, 2-byte AS number, AS 23456. This reserved AS number is called AS_TRANS in RFC 4893. All releases of Junos OS support 2-byte AS numbers.

In Junos OS Release 9.2 and later, you can also configure a 4-byte AS number using the AS-dot notation format of two integer values joined by a period: `<16-bit high-order value in decimal>.<16-bit low-order value in decimal>`. For example, the 4-byte AS number of 65,546 in plain-number format is represented as 1.10 in the AS-dot notation format. You can specify a value in the range from 0.0 through 65535.65535 in AS-dot notation format.

Default
No AS path information is associated with static routes.

Options
```
aggregator—(Optional) Attach the BGP aggregator path attribute to the aggregate route.

You must specify the last AS number that formed the aggregate route (encoded as two octets) for as-number, followed by the IP address of the BGP system that formed the aggregate route for ip-address.
```
**as-path**—(Optional) AS path to include with the route. It can include a combination of individual AS path numbers and AS sets. Enclose sets in brackets ([ ]). The first AS number in the path represents the AS immediately adjacent to the local AS. Each subsequent number represents an AS that is progressively farther from the local AS, heading toward the origin of the path. You cannot specify a regular expression for **as-path**. You must use a complete, valid AS path.

**atomic-aggregate**—(Optional) Attach the BGP **atomic-aggregate** path attribute to the aggregate route. This path attribute indicates that the local system selected a less specific route instead of a more specific route.

**origin egp**—(Optional) BGP origin attribute that indicates that the path information originated in another AS.

**origin igp**—(Optional) BGP origin attribute that indicates that the path information originated within the local AS.

**origin incomplete**—(Optional) BGP origin attribute that indicates that the path information was learned by some other means.

**Required Privilege**

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- *Examples: Configuring Static Routes*
- *Example: Summarizing Routes Through Route Aggregation*
- *Example: Conditionally Generating Static Routes*
- *Using 4-Byte Autonomous System Numbers in BGP Networks Technology Overview*
asm-override-ssm

Syntax
asm-override-ssm;

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name
  routing-options multicast],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options multicast]

Release Information
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description
Enable the routing device to accept any-source multicast join messages (*,G) for group addresses that are within the default or configured range of source-specific multicast groups.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Source-Specific Multicast Groups with Any-Source Override
## authentication-key-chains

### Syntax

```plaintext
authentication-key-chains {
  key-chain key-chain-name {
    description text-string;
    key key {
      algorithm (md5 | hmac-sha-1);
      options (basic | isis-enhanced);
      secret secret-data;
      start-time yyyy-mm-dd:hh:mm:ss;
    }
    tolerance seconds;
  }
}
```

### Hierarchy Level

```
[edit security]
```

### Release Information

- Statement introduced in Junos OS Release 7.6.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Support for the BFD protocol introduced in Junos OS Release 9.6.
- Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
- Support for IS-IS introduced in JUNOS OS Release 11.2.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

### Description

Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the `authentication-key-chains` statement is configured at the `[edit security]` hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the `[edit protocols]` hierarchy level or with the BFD protocol using the `bfd-liveness-detection` statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

The remaining statements are explained separately.

### Required Privilege Level

- admin—To view this statement in the configuration.
- admin-control—To add this statement to the configuration.

### Related Documentation

- **Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols**
- **Example: Configuring BFD Authentication for Static Routes**
- **Example: Configuring Hitless Authentication Key Rollover for IS-IS**

---

*Copyright © 2013, Juniper Networks, Inc.*
**autonomous-system**

**Syntax**
```autonomous-system autonomous-system <asdot-notation> <loops number> { independent-domain <no-attrset> ; }
```

**Hierarchy Level**
- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
- [edit logical-systems logical-system-name routing-options],
- [edit routing-instances routing-instance-name routing-options],
- [edit routing-options]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- asdot-notation option introduced in Junos OS Release 9.3.
- asdot-notation option introduced in Junos OS Release 9.3 for EX Series switches.
- no-attrset option introduced in Junos OS Release 10.4.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**
Specify the routing device’s AS number.

An autonomous system (AS) is a set of routing devices that are under a single technical administration and that generally use a single interior gateway protocol (IGP) and metrics to propagate routing information within the set of routing devices. An AS appears to other ASs to have a single, coherent interior routing plan and presents a consistent picture of what destinations are reachable through it. ASs are identified by a number that is assigned by the Network Information Center (NIC) in the United States ([http://www.isi.edu](http://www.isi.edu)).

If you are using BGP on the routing device, you must configure an AS number.

The AS path attribute is modified when a route is advertised to an EBGP peer. Each time a route is advertised to an EBGP peer, the local routing device prepends its AS number to the existing path attribute, and a value of 1 is added to the AS number.

In Junos OS Release 9.1 and later, the numeric range is extended to provide BGP support for 4-byte AS numbers as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*. RFC 4893 introduces two new optional transitive BGP attributes, AS4_PATH and AS4_AGGREGATOR. These new attributes are used to propagate 4-byte AS path information across BGP speakers that do not support 4-byte AS numbers. RFC 4893 also introduces a reserved, well-known, 2-byte AS number, AS 23456. This reserved AS number is called AS_TRANS in RFC 4893. All releases of Junos OS support 2-byte AS numbers.

In Junos OS Release 9.3 and later, you can also configure a 4-byte AS number using the AS-dot notation format of two integer values joined by a period: `<16-bit high-order value in decimal>.<16-bit low-order value in decimal>`. For example, the 4-byte AS number of 65,546 in plain-number format is represented as 110 in the AS-dot notation format.

**Options**
- **autonomous-system**—AS number. Use a number assigned to you by the NIC.
Range: 1 through 4,294,967,295 ($2^{32} - 1$) in plain-number format for 4-byte AS numbers

In this example, the 4-byte AS number 65,546 is represented in plain-number format:

```
[edit]
  routing-options {
    autonomous-system 65546;
  }
```

Range: 0.0 through 65535.65535 in AS-dot notation format for 4-byte numbers

In this example, 1.10 is the AS-dot notation format for 65,546:

```
[edit]
  routing-options {
    autonomous-system 1.10;
  }
```

Range: 1 through 65,535 in plain-number format for 2-byte AS numbers (this is a subset of the 4-byte range)

In this example, the 2-byte AS number 60,000 is represented in plain-number format:

```
[edit]
  routing-options {
    autonomous-system 60000;
  }
```

asdot-notation—(Optional) Display the configured 4-byte autonomous system number in the AS-dot notation format.

Default: Even if a 4-byte AS number is configured in the AS-dot notation format, the default is to display the AS number in the plain-number format.

loops number—(Optional) Specify the number of times detection of the AS number in the AS_PATH attribute causes the route to be discarded or hidden. For example, if you configure loops 1, the route is hidden if the AS number is detected in the path one or more times. This is the default behavior. If you configure loops 2, the route is hidden if the AS number is detected in the path two or more times.

Range: 1 through 10

Default: 1

NOTE: When you specify the same AS number in more than one routing instance on the local routing device, you must configure the same number of loops for the AS number in each instance. For example, if you configure a value of 3 for the loops statement in a VRF routing instance that uses the same AS number as that of the master instance, you must also configure a value of 3 loops for the AS number in the master instance.

Use the independent-domain option if the loops statement must be enabled only on a subset of routing instances.

The remaining statement is explained separately.
backup-pe-group

Syntax  
backup-pe-group group-name {
  backups [ addresses ];
  local-address address;
}

Hierarchy Level  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options multicast]

Release Information  
Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  
Configure a backup provider edge (PE) group for ingress PE redundancy when point-to-multipoint label-switched paths (LSPs) are used for multicast distribution.

Options  
backups addresses—Specify the address of backup PE routers for ingress PE redundancy when point-to-multipoint LSPs are used for multicast distribution.
local-address address—Specify the address of the local PE router for ingress PE redundancy when point-to-multipoint LSPs are used for multicast distribution.
pe-group-name—Specify the name for the group of PE routers that provide ingress PE router redundancy for point-to-multipoint LSPs.
### backups

**Syntax**

```
backups [ addresses ];
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast backup-pe-group group-name],
[edit logical-systems logical-system-name routing-options multicast backup-pe-group group-name],
[edit routing-instances routing-instance-name routing-options multicast backup-pe-group group-name],
[edit routing-options multicast backup-pe-group group-name]
```

**Release Information**

- Statement introduced in Junos OS Release 9.0.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure the addresses of backup PEs for ingress PE redundancy when point-to-multipoint label-switched paths (LSPs) are used for multicast distribution.

**Options**

- `addresses`—Addresses of other PEs in the backup group.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring Ingress PE Redundancy](#)
**bandwidth (Multicast Flow Map)**

**Syntax**  
bandwidth ( bps | adaptive );

**Hierarchy Level**  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast flow-map],  
[edit logical-systems logical-system-name routing-options multicast flow-map],  
[edit routing-instances routing-instance-name routing-options multicast flow-map],  
[edit routing-options multicast flow-map]

**Release Information**  
Statement introduced in Junos OS Release 8.3.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.  
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**  
Configure the bandwidth property for multicast flow maps.

**Options**  
adaptive—Specify that the bandwidth is measured for the flows that are matched by the flow map.

- **bps**—Bandwidth, in bits per second, for the flow map.
  
  **Range:** 0 through any amount of bandwidth
  
  **Default:** 2 Mbps

**Required Privilege Level**  
routing—To view this statement in the configuration.

- routing-control—To add this statement to the configuration.

**Related Documentation**  
- Example: Configuring a Multicast Flow Map
bdf-liveness-detection (Routing Options Static Route)

Syntax

```plaintext
bdf-liveness-detection {
    authentication {
        algorithm algorithm-name;
        key-chain key-chain-name;
        loose-check;
    }
    detection-time {
        threshold milliseconds;
    }
    hold-down-interval milliseconds;
    local-address ip-address;
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    minimum-receive-ttl number;
    multiplier number;
    neighbor address;
    no-adaptation;
    transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
    }
    version (1 | automatic);
}
```

Hierarchy Level

- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name static route destination-prefix]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name static route destination-prefix qualified-next-hop (interface-name | address)]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options static route destination-prefix]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options static route destination-prefix qualified-next-hop (interface-name | address)]`
- `[edit logical-systems logical-system-name routing-options rib routing-table-name static route destination-prefix]`
- `[edit logical-systems logical-system-name routing-options rib routing-table-name static route destination-prefix qualified-next-hop (interface-name | address)]`
- `[edit routing-instances routing-instance-name routing-options rib routing-table-name static route destination-prefix]`
- `[edit routing-instances routing-instance-name routing-options rib routing-table-name static route destination-prefix qualified-next-hop (interface-name | address)]`
- `[edit routing-instances routing-instance-name routing-options static route destination-prefix]`
- `[edit routing-instances routing-instance-name routing-options static route destination-prefix qualified-next-hop (interface-name | address)]`
- `[edit routing-options rib routing-table-name static route destination-prefix]`
- `[edit routing-options rib routing-table-name static route destination-prefix qualified-next-hop (interface-name | address)]`
- `[edit routing-options static route destination-prefix]`
[edit routing-options static route destination-prefix qualified-next-hop (interface-name | address)]

Release Information
Statement introduced before Junos OS Release 7.4.
detection-time threshold and transmit-interval threshold options introduced in Junos OS Release 8.2.
local-address statement introduced in Junos OS Release 8.2.
minimum-receive-tti statement introduced in Junos OS Release 8.2.
Support for logical routers introduced in Junos OS Release 8.3.
holddown-interval statement introduced in Junos OS Release 8.5.
no-adaptation statement introduced in Junos OS Release 9.0.
Support for IPv6 static routes introduced in Junos OS Release 9.1.
authentication algorithm, authentication key-chain, and authentication loose-check statements introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description
Configure bidirectional failure detection timers and authentication criteria for static routes.
Options

authentication algorithm algorithm-name — Configure the algorithm used to authenticate the specified BFD session: simple-password, keyed-md5, keyed-sha-1, meticulous-keyed-md5, or meticulous-keyed-sha-1.

authentication key-chain key-chain-name — Associate a security key with the specified BFD session using the name of the security keychain. The name you specify must match one of the keychains configured in the authentication-key-chains key-chain statement at the [edit security] hierarchy level.

authentication loose-check — (Optional) Configure loose authentication checking on the BFD session. Use only for transitional periods when authentication may not be configured at both ends of the BFD session.

detection-time threshold milliseconds — Configure a threshold for the adaptation of the BFD session detection time. When the detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.

holddown-interval milliseconds — Configure an interval specifying how long a BFD session must remain up before a state change notification is sent. If the BFD session goes down and then comes back up during the hold-down interval, the timer is restarted.

Range: 0 through 255,000
Default: 0

local-address ip-address — Enable a multihop BFD session and configure the source address for the BFD session.

minimum-interval milliseconds — Configure the minimum interval after which the local routing device transmits a hello packet and then expects to receive a reply from the neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum transmit and receive intervals separately using the transmit-interval minimum-interval and minimum-receive-interval statements.

Range: 1 through 255,000

minimum-receive-interval milliseconds — Configure the minimum interval after which the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum receive interval using the minimum-interval statement at the [edit routing-options static route destination-prefix bfd-liveness-detection] hierarchy level.

Range: 1 through 255,000

minimum-receive-ttl number — Configure the time to live (TTL) for the multihop BFD session.

Range: 1 through 255
Default: 255

multiplier number — Configure number of hello packets not received by the neighbor that causes the originating interface to be declared down.

Range: 1 through 255
Default: 3
neighbor address—Configure a next-hop address for the BFD session for a next hop specified as an interface name.

no-adaptation—Specify for BFD sessions not to adapt to changing network conditions. We recommend that you not disable BFD adaptation unless it is preferable not to have BFD adaptation enabled in your network.

transmit-interval threshold milliseconds—Configure the threshold for the adaptation of the BFD session transmit interval. When the transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent. The interval threshold must be greater than the minimum transmit interval.

Range: 0 through 4,294,967,295

transmit-interval minimum-interval milliseconds—Configure the minimum interval at which the routing device transmits hello packets to a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can configure the minimum transmit interval using the minimum-interval statement at the [edit routing-options static route destination-prefix bfd-liveness-detection] hierarchy level.

Range: 1 through 255,000

version—Configure the BFD version to detect: 1 (BFD version 1) or automatic (autodetect the BFD version).

Default: automatic

Required Privilege
Level routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring BFD for Static Routes
• Example: Configuring BFD Authentication for Static Routes
bgp-orf-cisco-mode

**Syntax**

```plaintext
bgp-orf-cisco-mode;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols bgp outbound-route-filter]`
- `[edit logical-systems logical-system-name protocols bgp group group-name outbound-route-filter]`
- `[edit logical-systems logical-system-name protocols bgp group group-name neighbor address outbound-route-filter]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp outbound-route-filter]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name outbound-route-filter]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols bgp group group-name neighbor address outbound-route-filter]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options outbound-route-filter]`
- `[edit logical-systems logical-system-name routing-options outbound-route-filter]`
- `[edit protocols bgp outbound-route-filter]`
- `[edit protocols bgp group group-name outbound-route-filter]`
- `[edit protocols bgp group group-name neighbor address outbound-route-filter]`
- `[edit routing-instances routing-instance-name protocols bgp outbound-route-filter]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name outbound-route-filter]`
- `[edit routing-instances routing-instance-name protocols bgp group group-name neighbor address outbound-route-filter]`
- `[edit routing-instances routing-instance-name routing-options outbound-route-filter]`
- `[edit routing-instances routing-instance-name routing-options outbound-route-filter]`
- `[edit routing-options outbound-route-filter]`

**Release Information**

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 9.2 for EX Series switches.
Support for the BGP group and neighbor hierarchy levels introduced in Junos OS Release 9.2.
Support for the BGP group and neighbor hierarchy levels introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Enable interoperability with routing devices that use the vendor-specific outbound route filter compatibility code of 130 and code type of 128.

**NOTE:** To enable interoperability for all BGP peers configured on the routing device, include the statement at the `[edit routing-options outbound-route-filter]` hierarchy level.

**Default**

Disabled

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.
Related Documentation

- Example: Configuring BGP Prefix-Based Outbound Route Filtering

**bmp**

**Syntax**

```plaintext
bmp {
  memory-limit bytes;
  station-address (ip-address | name);
  station-port port-number;
  statistics-timeout seconds;
}
```

**Hierarchy Level**

[edit routing-options]

**Release Information**

Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Configure the BGP Monitoring Protocol (BMP), which enables the routing device to collect data from the BGP Adjacency-RIB-In routing tables and periodically send that data to a monitoring station.

**Options**

- **memory-limit bytes**—(Optional) Specify a threshold at which to stop collecting BMP data if the limit is exceeded.

  **Default:** 10 MB

  **Range:** 1,048,576 through 52,428,800

- **station-address (ip-address | name)**—Specify the IP address or a valid URL for the monitoring where BMP data should be sent.

- **station-port port-number**—Specify the port number of the monitoring station to use when sending BMP data.

- **statistics-timeout seconds**—(Optional) Specify how often to send BMP data to the monitoring station.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring the BGP Monitoring Protocol
### brief

**Syntax**

(brief | full);

**Hierarchy Level**

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate) (defaults | route)],

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],

[edit logical-systems logical-system-name routing-options (aggregate | generate) (defaults | route)],

[edit logical-systems logical-system-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],

Release Information

Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Statement introduced in Junos OS Release 11.3 for the QFX Series.

Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Configure all AS numbers from all contributing paths to be included in the aggregate or generated route's path.

- **brief**—Include only the longest common leading sequences from the contributing AS paths. If this results in AS numbers being omitted from the aggregate route, the BGP ATOMIC_ATTRIBUTE path attribute is included with the aggregate route.

- **full**—Include all AS numbers from all contributing paths in the aggregate or generated route's path. Include this option when configuring an individual route in the `route` portion of the `generate` statement to override a `retain` option specified in the `defaults` portion of the statement.

**Default**

full

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Summarizing Routes Through Route Aggregation
- Example: Conditionally Generating Static Routes
  - aggregate on page 3030
  - generate on page 3062
centralized

Syntax  centralized;

Hierarchy Level  [edit protocols lACP ppm]

Release Information  Statement introduced in Junos OS Release 10.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Disable distributed periodic packet management (PPM) processing for Link Aggregation
Control Protocol (LACP) packets and run all PPM processing for LACP packets on the
Routing Engine.

This statement disables distributed PPM processing for only LACP packets. You can
disable distributed PPM processing for all packets that use PPM and run all PPM
processing on the Routing Engine by configuring the no-delegate-processing statement
in the [edit routing-options ppm] hierarchy.

BEST PRACTICE: We generally recommend that you disable distributed PPM
only if Juniper Networks Customer Service advises you to do so. You should
disable distributed PPM only if you have a compelling reason to disable it.

Default  Distributed PPM processing is enabled for all packets that use PPM.

Required Privilege  Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  • Configuring Distributed Periodic Packet Management on an EX Series Switch (CLI Procedure) on page 3026
• Configuring Aggregated Ethernet LACP (CLI Procedure) on page 2339
• Configuring Distributed Periodic Packet Management
• Configuring Link Aggregation
community (Routing Options)

Syntax  
community ([community-ids] | no-advertise | no-export | no-export-subconfed | none);

Hierarchy Level  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-options routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-optionsrib routing-table-name (aggregate | generate | static) (defaults | route)],

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  
Associate BGP community information with a static, aggregate, or generated route.

Default  
No BGP community information is associated with static routes.

Options  
community-ids—One or more community identifiers. The community-ids format varies according to the type of attribute that you use.

The BGP community attribute format is as-number:community-value:

- as-number—AS number of the community member. It can be a value from 1 through 65,535. The AS number can be a decimal or hexadecimal value.
- community-value—Identifier of the community member. It can be a number from 0 through 65,535.

For more information about BGP community attributes, see the “Configuring the Extended Communities Attribute” section in the Routing Policy Feature Guide for Routing Devices.

For specifying the BGP community attribute only, you also can specify community-ids as one of the following well-known community names defined in RFC 1997:

- no-advertise—Routes containing this community name are not advertised to other BGP peers.
- no-export—Routes containing this community name are not advertised outside a BGP confederation boundary.
- no-export-subconfed—Routes containing this community name are not advertised to external BGP peers, including peers in other members’ ASs inside a BGP confederation.
NOTE: Extended community attributes are not supported at the [edit routing-options] hierarchy level. You must configure extended communities at the [edit policy-options] hierarchy level. For information about configuring extended communities, see the Routing Policy Feature Guide for Routing Devices.

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Examples: Configuring Static Routes
- Example: Summarizing Routes Through Route Aggregation
- Example: Conditionally Generating Static Routes
- aggregate on page 3030
- generate on page 3062
- static on page 3118
### confederation

**Syntax**

```
confederation confederation-autonomous-system members [ autonomous-systems ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-options],
- [edit routing-options]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Specify the routing device's confederation AS number.

If you administer multiple ASs that contain a very large number of BGP systems, you can group them into one or more confederations. Each confederation is identified by its own AS number, which is called a confederation AS number. To external ASs, a confederation appears to be a single AS. Thus, the internal topology of the ASs making up the confederation is hidden.

The BGP path attributes `NEXT_HOP`, `LOCAL_PREF`, and `MULTI_EXIT_DISC`, which normally are restricted to a single AS, are allowed to be propagated throughout the ASs that are members of the same confederation.

Because each confederation is treated as if it were a single AS, you can apply the same routing policy to all the ASs that make up the confederation.

Grouping ASs into confederations reduces the number of BGP connections required to interconnect ASs.

If you are using BGP, you can enable the local routing device to participate as a member of an AS confederation. To do this, include the `confederation` statement.

Specify the AS confederation identifier, along with the peer AS numbers that are members of the confederation.

Note that peer adjacencies do not form if two BGP neighbors disagree about whether an adjacency falls within a particular confederation.

**Options**

- `autonomous-systems`—AS numbers of the confederation members.
  - **Range:** 1 through 65,535

- `confederation-autonomous-system`—Confederation AS number. Use one of the numbers assigned to you by the NIC.
  - **Range:** 1 through 65,535

**Required Privilege**

- **Level:**
  - `routing`—To view this statement in the configuration.
  - `routing-control`—To add this statement to the configuration.
disable (Routing Options)

Syntax  
disable;

Hierarchy Level  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options graceful-restart],  
[edit logical-systems logical-system-name routing-options graceful-restart],  
[edit routing-instances routing-instance-name routing-options graceful-restart],  
[edit routing-options graceful-restart]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  
Disable graceful restart.

Required Privilege Level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

Related Documentation  
• Junos OS High Availability Library for Routing Devices
**discard**

**Syntax**

discard;

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate) (defaults | route)],
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Do not forward packets addressed to this destination. Instead, drop the packets, do not send ICMP unreachable messages to the packets' originators, and install a reject route for this destination into the routing table.

To propagate static routes into the routing protocols, include the `discard` statement when you define the route, along with a routing policy.

**NOTE:** In other vendors' software, a common way to propagate static routes into routing protocols is to configure the routes so that the next-hop routing device is the loopback address (commonly, 127.0.0.1). However, configuring static routes in this way (by including a statement such as `route address/mask-length next-hop 127.0.0.1`) does not propagate the static routes, because the forwarding table ignores static routes whose next-hop routing device is the loopback address.

**Default**

When an aggregate route becomes active, it is installed in the routing table with a reject next hop, which means that ICMP unreachable messages are sent.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: *Summarizing Routes Through Route Aggregation*
- Example: *Conditionally Generating Static Routes*
export (Routing Options)

Syntax

```
export [ policy-name ];
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options forwarding-table],
[edit logical-systems logical-system-name routing-options forwarding-table],
[edit routing-instances routing-instance-name routing-options forwarding-table],
[edit routing-options forwarding-table]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Apply one or more policies to routes being exported from the routing table into the forwarding table.

In the `export` statement, list the name of the routing policy to be evaluated when routes are being exported from the routing table into the forwarding table. Only active routes are exported from the routing table.

You can reference the same routing policy one or more times in the same or a different `export` statement.

You can apply export policies to routes being exported from the routing table into the forwarding table for the following features:

- Per-packet load balancing
- Class of service (CoS)

Options

`policy-name`—Name of one or more policies.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Example: Load Balancing BGP Traffic
- Routing Policy Feature Guide for Routing Devices
- How a Routing Policy Is Evaluated
### export-rib

**Syntax**

```
export-rib routing-table-name;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib-groups group-name],
[edit logical-systems logical-system-name routing-options rib-groups group-name],
[edit routing-instances routing-instance-name routing-options rib-groups group-name],
[edit routing-options rib-groups group-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Specify the name of the routing table from which Junos OS should export routing information.

**Options**

`routing-table-name`—Routing table group name.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- `Example: Exporting Specific Routes from One Routing Table Into Another Routing Table`
- `import-rib on page 3065`
- `passive`
fate-sharing

Syntax
fate-sharing {  
group group-name {  
cost value;  
from address <to address>;  
}  
}  

Hierarchy Level  
[edit logical-systems logical-system-name routing-options],  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],  
[edit routing-options],  
[edit routing-instances routing-instance-name routing-options]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Specify a backup path in case the primary path becomes unusable.

You specify one or more objects with common characteristics within a group. All objects are treated as /32 host addresses. The objects can be a LAN interface, a router ID, or a point-to-point link. Sequence is insignificant.

Changing the fate-sharing database does not affect existing established LSPs until the next CSPF reoptimization. The fate-sharing database does affect fast-reroute detour path computations.

Options
cost value—Cost assigned to the group.  
Range: 1 through 65,535  
Default: 1

from address—Address of the router or address of the LAN/NBMA interface. For example, an Ethernet network with four hosts in the same fate-sharing group would require you to list all four of the separate from addresses in the group.

group group-name—Each fate-sharing group must have a name, which can have a maximum of 32 characters, including letters, numbers, periods (.), and hyphens (-). You can define up to 512 groups.

to address—(Optional) Address of egress router. For point-to-point link objects, you must specify both a from and a to address.

Required Privilege Level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

Related Documentation  
• Configuring the Ingress Router for MPLS-Signaled LSPs  
• Junos OS MPLS Applications Library for Routing Devices
flow

Syntax  flow {
    route name {
        match {
            match-conditions;
        }
        term-order (legacy | standard);
        then {
            actions;
        }
    }
    firewall-install-disable;
    term-order (legacy | standard);
    validation {
        traceoptions {
            file filename <files number> <size size> <world-readable | no-world-readable>;
            flag flag <flag-modifier> <disable>;
        }
    }
}

Hierarchy Level  [edit routing-options],
                 [edit logical-systems logical-system-name routing-options],
                 [edit routing-instances routing-instance-name routing-options],
                 [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options]

Release Information  Statement introduced before Junos OS Release 7.4.
                      Statement introduced in Junos OS Release 9.0 for EX Series switches.
                      term-order statement introduced in Junos OS Release 10.0
                      Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Configure a flow route.

Default  legacy

Options  actions—An action to take if conditions match.
          match-conditions—Match packets to these conditions.
          route name—Name of the flow route.
          standard—Specify to use version 7 or later of the flow-specification algorithm.
          term-order (legacy | standard)—Specify the version of the flow-specification algorithm.
          • legacy—Use version 6 of the flow-specification algorithm.
          • standard—Use version 7 of the flow-specification algorithm.
          then—Actions to take on matching packets.
The remaining statements are explained separately.

**Required Privilege**
- **Level**
  - *routing*—To view this statement in the configuration.
  - *routing-control*—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring Flow Routes*

---

**flow-map**

**Syntax**
```
flow-map flow-map-name {
  bandwidth (bps | adaptive);
  forwarding-cache {
    timeout (never non-discard-entry-only | minutes);
  }
  policy [ policy-names ];
  redundant-sources [ addresses ];
}
```

**Hierarchy Level**
- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast]`
- `[edit logical-systems logical-system-name routing-options multicast]`
- `[edit routing-instances routing-instance-name routing-options multicast]`
- `[edit routing-options multicast]`

**Release Information**
- Statement introduced in Junos OS Release 8.2.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Configure multicast flow maps.

**Options**
- **flow-map-name**—Name of the flow-map.

The remaining statements are explained separately.

**Required Privilege**
- **Level**
  - *routing*—To view this statement in the configuration.
  - *routing-control*—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring a Multicast Flow Map*
forwarding-cache (Flow Maps)

Syntax
forwarding-cache {
  timeout (minutes | never | non-discard-entry-only);
}

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast flow-map flow-map-name],
[edit logical-systems logical-system-name routing-options multicast flow-map flow-map-name],
[edit routing-instances routing-instance-name routing-options multicast flow-map flow-map-name],
[edit routing-options multicast flow-map flow-map-name]

Release Information
Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure multicast forwarding cache properties for the flow map.

Required Privilege
Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.
### forwarding-cache (Multicast)

**Syntax**

```plaintext
forwarding-cache {
    allow-maximum;
    family (inet | inet6) {
        threshold {
            log-warning value;
            suppress value <reuse value>;
        }
    }
    threshold {
        log-warning value;
        suppress value <reuse value>;
    }
    timeout minutes;
}
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast]`
- `[edit logical-systems logical-system-name routing-options multicast]`
- `[edit routing-instances routing-instance-name routing-options multicast]`
- `[edit routing-options multicast]`

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure multicast forwarding cache properties. These properties include threshold suppression and reuse limits, the threshold at which a warning message is logged, and timeout values.

Specify a value for the threshold at which to suppress new multicast forwarding cache entries and an optional reuse value for the threshold at which the router begins to create new multicast forwarding cache entries. The range for both is from 1 through 200,000. If configured, the reuse value should be less than the suppression threshold value. The suppression value is mandatory. If you do not specify the optional reuse value, then the number of multicast forwarding cache entries is limited to the suppression value. A new entry is created as soon as the number of multicast forwarding cache entries falls below the suppression value.

You can configure the thresholds globally for the multicast forwarding cache or individually for the IPv4 and IPv6 multicast forwarding caches. Configuring the `threshold` statement globally for the multicast forwarding cache or including the `family` statement to configure the thresholds for the IPv4 and IPv6 multicast forwarding caches are mutually exclusive.

**Default**

By default, there are no limits on the number of multicast forwarding cache entries.

**Options**

- `family (inet | inet6)`—(Optional) Apply the configured thresholds to either IPv4 or IPv6 multicast forwarding cache entries.

**Default**

By default, the configured thresholds are applied to both IPv4 and IPv6 multicast forwarding cache entries.
The remaining statements are explained separately.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>routing-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Example: Configuring the Multicast Forwarding Cache

### forwarding-table

**Syntax**

```plaintext
forwarding-table {
    chained-composite-next-hop {
        ingress {
            l3vpn {
                extended-space;
            }
        }
    }
    export [policy-name];
    indexed-next-hop;
    (indirect-next-hop | no-indirect-next-hop);
    (indirect-next-hop-change-acknowledgements | no-indirect-next-hop-change-acknowledgements);
    krt-nexthop-ack-timeout interval;
    unicast-reverse-path (active-paths | feasible-paths);
}
```

**Hierarchy Level**

[edit logical-systems logical-system-name routing-options],
[edit routing-options]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure information about the routing device's forwarding table.

The remaining statements are explained separately.

**Required Privilege**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing</td>
<td>To view this statement in the configuration.</td>
</tr>
<tr>
<td>routing-control</td>
<td>To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- Example: Load Balancing BGP Traffic
**generate**

Syntax

generate {
    defaults {
        generate-options;
    }
    route destination-prefix {
        policy policy-name;
        generate-options;
    }
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name],
[edit routing-options],
[edit routing-options rib routing-table-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure generated routes, which are used as routes of last resort.

Options

**defaults**—(Optional) Specify global generated route options. These options only set default attributes inherited by all newly created generated routes. These are treated as global defaults and apply to all the generated routes you configure in the `generate` statement.

**generate-options**—Additional information about generated routes, which is included with the route when it is installed in the routing table. Specify zero or more of the following options in **generate-options**. Each option is explained separately.

- (active | passive);
- as-path <as-path> <origin (egp | igp | incomplete)> <atomic-aggregate> <aggregator as-number in-address>;
- (brief | full);
- community [ community-ids ];
- discard;
- (metric | metric2 | metric3 | metric4) value <type type>;
- (preference | preference2 | color | color2) preference <type type>;
- tag string;

**route destination-prefix**—Configure a non-default generated route:

- default—For the default route to the destination. This is equivalent to specifying an IP address of 0.0.0.0/0.
- **destination-prefix/prefix-length**—/destination-prefix is the network portion of the IP address, and **prefix-length** is the destination prefix length.

The **policy** statement is explained separately.

**Required Privilege**

**Level** routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Conditionally Generating Static Routes

---

**import (Routing Options)**

**Syntax**

```import [ policy-names ];```

**Hierarchy Level**

```[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options resolution rib],
[edit logical-systems logical-system-name routing-options resolution rib],
[edit routing-instances routing-instance-name routing-options resolution rib],
[edit routing-options resolution rib]```  

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Specify one or more import policies to use for route resolution.

**Options**

**policy-names**—Name of one or more import policies.

**Required Privilege**

**Level** routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Route Resolution on PE Routers
import-policy

Syntax  
```
import-policy [ policy-names ];
```

Hierarchy Level  
```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib-groups group-name],
[edit logical-systems logical-system-name routing-options rib-groups group-name],
[edit routing-instances routing-instance-name routing-options rib-groups group-name],
[edit routing-options rib-groups group-name]
```

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Apply one or more policies to routes imported into the routing table group. The `import-policy` statement complements the `import-rib` statement and cannot be used unless you first specify the routing tables to which routes are being imported.

NOTE: On EX Series switches, only dynamically learned routes can be imported from one routing table group to another.

Options  
- `policy-names`—Name of one or more policies.

Required Privilege
- Level  
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

Related Documentation
- `Example: Exporting Specific Routes from One Routing Table Into Another Routing Table`
- `export-rib on page 3055`
- `passive`
import-rib

**Syntax**

import-rib [ **routing-table-names** ];

**Hierarchy Level**

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib-groups group-name],
[edit logical-systems logical-system-name routing-options rib-groups group-name],
[edit routing-instances routing-instance-name routing-options rib-groups group-name],
[edit routing-options rib-groups group-name]

**Release Information**

Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Specify the name of the routing table into which Junos OS should import routing information. The first routing table name you enter is the primary routing table. Any additional names you enter identify secondary routing tables. When a protocol imports routes, it imports them into the primary and any secondary routing tables. If the primary route is deleted, the secondary route also is deleted. For IPv4 import routing tables, the primary routing table must be inet.0 or **routing-instance-name.inet.0**. For IPv6 import routing tables, the primary routing table must be inet6.0.

In Junos OS Release 9.5 and later, you can configure an IPv4 import routing table that includes both IPv4 and IPv6 routing tables. Including both types of routing tables permits you, for example, to populate an IPv6 routing table with IPv6 addresses that are compatible with IPv4. In releases prior to Junos OS Release 9.5, you could configure an import routing table with only either IPv4 or IPv6 routing tables.

---

**NOTE:** On EX Series switches, only dynamically learned routes can be imported from one routing table group to another.

---

**Options**

**routing-table-names**—Name of one or more routing tables.

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Exporting Specific Routes from One Routing Table Into Another Routing Table
- export-rib on page 3055
- passive
indirect-next-hop

**Syntax**
(indirect-next-hop | no-indirect-next-hop);

**Hierarchy Level**
[edit logical-systems logical-system-name routing-options forwarding-table],
[edit routing-options forwarding-table]

**Release Information**
Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Enable indirectly connected next hops for route convergence. This statement is implemented on the Packet Forward Engine to speed up forwarding information base (FIB) updates. Configuring this statement significantly speeds convergence times. The only downside of configuring this statement is that some additional FIB memory overhead is required. Unless routes have an extremely high number of next hops, this increased memory usage should not be noticeable.

**NOTE:**
- When virtual private LAN service (VPLS) is configured on the routing device, the indirect-next-hop statement is configurable at the [edit routing-options forwarding-table] hierarchy level. However, this configuration is not applicable to indirect nexthops specific to VPLS routing instances.
- By default, the Junos Trio Modular Port Concentrator (MPC) chipset on MX Series routers is enabled with indirectly connected next hops, and this cannot be disabled using the no-indirect-next-hop statement.

**Default**
Disabled.

**Options**
indirect-next-hop—Enable indirectly connected next hops.

no-indirect-next-hop—Explicitly disable indirect next hops.

**Required Privilege Level**
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

**Related Documentation**
- Example: Optimizing Route Reconvergence by Enabling Indirect Next Hops on the Packet Forwarding Engine
install (Routing Options)

Syntax  (install | no-install);

Hierarchy Level  [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options static (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name static (defaults | route)],
[edit logical-systems logical-system-name routing-options rib routing-table-name static (defaults | route)],
[edit logical-systems logical-system-name routing-options static (defaults | route)],
[edit routing-instances routing-instance-name routing-options rib routing-table-name static (defaults | route)],
[edit routing-instances routing-instance-name routing-options static (defaults | route)],
[edit routing-options static (defaults | route)]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Configure whether Junos OS installs all static routes into the forwarding table. Even if you configure a route so it is not installed in the forwarding table, the route is still eligible to be exported from the routing table to other protocols.

Options  install—Explicitly install all static routes into the forwarding table. Include this statement when configuring an individual route in the route portion of the static statement to override a no-install option specified in the defaults portion of the statement.

no-install—Do not install the route into the forwarding table, even if it is the route with the lowest preference.

Default: install

Required Privilege Level  routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation  • Examples: Configuring Static Routes
• static on page 3118
instance-export

Syntax
instance-export [policy-names];

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information
Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Apply one or more policies to routes being exported from a routing instance.

Options
policy-names—Name of one or more export policies.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related
Documentation
• Routing Policy Feature Guide for Routing Devices

instance-import

Syntax
instance-import [policy-names];

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information
Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Apply one or more policies to routes being imported into a routing instance.

Options
policy-names—Name of one or more import policies.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related
Documentation
• Routing Policy Feature Guide for Routing Devices
interface (Multicast Static Routes)

Syntax

```
interface interface-names {
    disable;
    maximum-bandwidth bps;
    no-qos-adjust;
    reverse-oif-mapping {
        no-qos-adjust;
    }
    subscriber-leave-timer seconds;
}
```

Hierarchy Level

- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast]`
- `[edit logical-systems logical-system-name routing-options multicast]`
- `[edit routing-instances routing-instance-name routing-options multicast]`
- `[edit routing-options multicast]`

Release Information

Statement introduced in Junos OS Release 8.1.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable multicast traffic on an interface.

By default, multicast packets are forwarded by enabling Protocol Independent Multicast (PIM) on an interface. PIM adds multicast routes into the routing table.

You can also configure multicast packets to be forwarded over a static route, such as a static route associated with an LSP next hop. Multicast packets are accepted on an interface and forwarded over a static route in the forwarding table. This is useful when you want to enable multicast traffic on a specific interface without configuring PIM on the interface.

You cannot enable multicast traffic on an interface and configure PIM on the same interface simultaneously.

Static routes must be configured before you can enable multicast on an interface. Configuring the `interface` statement alone does not install any routes into the routing table. This feature relies on the static route configuration.

Options

- `interface-names`—Name of one or more interfaces on which to enable multicast traffic.

The remaining statements are explained separately.

Required Privilege Level

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation

- *Example: Defining Interface Bandwidth Maximums*
- *Example: Configuring Multicast with Subscriber VLANs*
interface (Routing Options)

Syntax

interface interface-names {
  maximum-bandwidth bps;
  no-qos-adjust;
  reverse-oif-mapping {
    no-qos-adjust;
  }
  subscriber-leave-timer seconds;
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options multicast]

Release Information

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable multicast traffic on an interface.

⚠️ TIP: You cannot enable multicast traffic on an interface by using the routing-options multicast interface statement and configure PIM on the interface.

Options

- **interface-name**—Names of the physical or logical interface.

  The remaining statements are explained separately.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Defining Interface Bandwidth Maximums*
- *Example: Configuring Multicast with Subscriber VLANs*
interface-routes

Syntax

interface-routes {
  family (inet | inet6) {
    export {
      lan;
      point-to-point;
    }
  }
  rib-group group-name;
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

NOTE: On EX Series switches, only dynamically learned routes can be imported from one routing table group to another.

Description

Associate a routing table group with the routing device’s interfaces, and specify routing table groups into which interface routes are imported.

By default, IPv4 interface routes (also called direct routes) are imported into routing table inet.0, and IPv6 interface routes are imported into routing table inet6.0. If you are configuring alternate routing tables for use by some routing protocols, it might be necessary to import the interface routes into the alternate routing tables. To define the routing tables into which interface routes are imported, you create a routing table group and associate it with the routing device’s interfaces.

To create the routing table groups, include the passive statement at the [edit routing-options] hierarchy level.

If you have configured a routing table, configure the OSPF primary instance at the [edit protocols ospf] hierarchy level with the statements needed for your network so that routes are installed in inet.0 and in the forwarding table. Make sure to include the routing table group.

To export local routes, include the export statement.

To export LAN routes, include the lan option. To export point-to-point routes, include the point-to-point option.
Only local routes on point-to-point interfaces configured with a destination address are exportable.

**Options**
- **inet**—Specify the IPv4 address family.
- **inet6**—Specify the IPv6 address family.
- **lan**—Export LAN routes.
- **point-to-point**—Export point-to-point routes.

The remaining statements are explained separately.

**Required Privilege**
- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Importing Direct and Static Routes Into a Routing Instance
- Example: Configuring Multiple Routing Instances of OSPF
- passive

---

**local-address (Routing Options)**

**Syntax**
```
local-address address;
```

**Hierarchy Level**
- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast backup-pe-group group-name],
- [edit logical-systems logical-system-name routing-options multicast backup-pe-group group-name],
- [edit routing-instances routing-instance-name routing-options multicast backup-pe-group group-name],
- [edit routing-options multicast backup-pe-group group-name]

**Release Information**
- Statement introduced in Junos OS Release 9.0.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Configure the address of the local PE for ingress PE redundancy when point-to-multipoint LSPs are used for multicast distribution.

**Options**
- **address**—Address of local PEs in the backup group.

**Required Privilege**
- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring Ingress PE Redundancy
**martians**

**Syntax**

```bash
martians {
  destination-prefix match-type <allow>;
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name],
[edit logical-systems logical-system-name routing-options],
[edit logical-systems logical-system-name routing-options rib routing-table-name],
[edit routing-instances routing-instance-name routing-options rib routing-table-name],
[edit routing-options],
[edit routing-options rib routing-table-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure martian addresses.

**Options**

- `allow`—(Optional) Explicitly allow a subset of a range of addresses that has been disallowed. The `allow` option is the only supported action.

- `destination-prefix`—Destination route you are configuring:
  - `destination-prefix/prefix-length`—`destination-prefix` is the network portion of the IP address, and `prefix-length` is the destination prefix length.
  - `default`—Default route to use when routing packets do not match a network or host in the routing table. This is equivalent to specifying the IP address `0.0.0.0/0`.

- `match-type`—Criteria that the destination must match:
  - `exact`—Exactly match the route’s mask length.
  - `longer`—The route’s mask length is greater than the specified mask length.
  - `orlonger`—The route’s mask length is equal to or greater than the specified mask length.
  - `through destination-prefix`—The route matches the first prefix, the route matches the second prefix for the number of bits in the route, and the number of bits in the route is less than or equal to the number of bits in the second prefix.
  - `upto prefix-length`—The route’s mask length falls between the two destination prefix lengths, inclusive.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.
maximum-bandwidth (Routing Options)

**Syntax**

```plaintext
maximum-bandwidth bps;
```

**Hierarchy Level**

```
[edit dynamic-profiles profile-name routing-instances instance-name routing-options multicast interface interface-name],
[edit dynamic-profiles profile-name routing-options multicast interface interface-name]
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit logical-systems logical-system-name routing-options multicast interface interface-name],
[edit routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit routing-options multicast interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
**dynamic-profiles** hierarchy level added in Junos OS Release 11.2.

**Description**

Configure the multicast bandwidth for the interface.

**Options**

- **bps**—Bandwidth rate, in bits per second, for the multicast interface.

**Range:** 0 through any amount of bandwidth

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring Martian Addresses*

- *Example: Defining Interface Bandwidth Maximums*
maximum-paths

Syntax

maximum-paths path-limit <log-interval seconds> <log-only | threshold value>;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure a limit for the number of routes installed in a routing table based upon the route path.

NOTE: The maximum-paths statement is similar to the maximum-prefixes statement. The maximum-prefixes statement limits the number of unique destinations in a routing instance. For example, suppose a routing instance has the following routes:

OSPF 10.10.10.0/24
ISIS 10.10.10.0/24

These are two routes, but only one destination (prefix). The maximum-paths limit applies the total number of routes (two). The maximum-prefixes limit applies to the total number of unique prefixes (one).

Options

log-interval seconds—(Optional) Minimum time interval (in seconds) between log messages.
Range: 5 through 86,400

log-only—(Optional) Sets the route limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected.

path-limit—Maximum number of routes. If this limit is reached, a warning is triggered and additional routes are rejected.
Range: 1 through 4,294,967,295 (2^{32} – 1)
Default: No default

threshold value—(Optional) Percentage of the maximum number of routes that starts triggering a warning. You can configure a percentage of the path-limit value that starts triggering the warnings.
Range: 1 through 100
NOTE: When the number of routes reaches the threshold value, routes are still installed into the routing table while warning messages are sent. When the number of routes reaches the path-limit value, then additional routes are rejected.

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Limiting the Number of Paths and Prefixes Accepted from CE Routers in Layer 3 VPNs
maximum-prefixes

Syntax
maximum-prefixes prefix-limit <log-interval seconds> <log-only | threshold percentage>;

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information
Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure a limit for the number of routes installed in a routing table based upon the route prefix.

Using a prefix limit, you can curtail the number of prefixes received from a CE router in a VPN. Prefix limits apply only to dynamic routing protocols and are not applicable to static or interface routes.

NOTE: The maximum-prefixes statement is similar to the maximum-paths statement. The maximum-prefixes statement limits the number of unique destinations in a routing instance. For example, suppose a routing instance has the following routes:

OSPF 10.10.10.0/24
ISIS 10.10.10.0/24

These are two routes, but only one destination (prefix). The maximum-paths limit applies the total number of routes (two). The maximum-prefixes limit applies to the total number of unique prefixes (one).

Options
log-interval seconds—(Optional) Minimum time interval (in seconds) between log messages.
Range: 5 through 86,400

log-only—(Optional) Sets the prefix limit as an advisory limit. An advisory limit triggers only a warning, and additional routes are not rejected.

prefix-limit—Maximum number of route prefixes. If this limit is reached, a warning is triggered and any additional routes are rejected.
Range: 1 through 4,294,967,295
Default: No default

threshold value—(Optional) Percentage of the maximum number of prefixes that starts triggering a warning. You can configure a percentage of the prefix-limit value that starts triggering the warnings.
Range: 1 through 100

NOTE: When the number of routes reaches the threshold value, routes are still installed into the routing table while warning messages are sent. When the number of routes reaches the prefix-limit value, then additional routes are rejected.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Limiting the Number of Paths and Prefixes Accepted from CE Routers in Layer 3 VPNs

med-igp-update-interval

Syntax med-igp-update-interval minutes;

Hierarchy Level [edit routing-options]

Release Information Statement introduced in Junos OS Release 9.0
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Configure a timer for how long to delay updates for the multiple exit discriminator (MED) path attribute for BGP groups and peers configured with the metric-out igp offset delay-med-update statement. The timer delays MED updates for the interval configured unless the MED is lower than the previously advertised attribute or another attribute associated with the route has changed or if the BGP peer is responding to a refresh route request.

Options minutes—Interval to delay MED updates.
Range: 10 through 600
Default: 10 minutes

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Associating the MED Path Attribute with the IGP Metric and Delaying MED Updates
• metric-out on page 2618
**metric (Aggregate, Generated, or Static Route)**

**Syntax**

```
(metric | metric2 | metric3 | metric4) metric <type type>;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-options (aggregate | generate | static) 
 (defaults | route )],
[edit routing-options (aggregate | generate | static) (defaults | route )]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Specify the metric value for an aggregate, generated, or static route. You can specify up to four metric values, starting with `metric` (for the first metric value) and continuing with `metric2`, `metric3`, and `metric4`.

**Options**

- `metric`—Metric value.
  
  **Range:** 0 through 4,294,967,295 ($2^{32} – 1$)

- `type type`—(Optional) Type of route.

  When routes are exported to OSPF, type 1 routes are advertised in type 1 externals, and routes of any other type are advertised in type 2 externals. Note that if a qualified-next-hop metric value is configured, this value overrides the route metric.

  **Range:** 1 through 16

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Summarizing Static Routes Through Route Aggregation*
- *Example: Conditionally Generating Static Routes*
  
  - aggregate on page 3030
  - generate on page 3062
  - static on page 3118
**multicast (Routing Options)**

**Syntax**

```plaintext
multicast {
    forwarding-cache {
        threshold suppress value <reuse value>;
    }
    interface interface-name {
        enable;
    }
    scope scope-name {
        interface [ interface-names ];
        prefix destination-prefix;
    }
    ssm-groups {
        address;
    }
}
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
- [edit logical-systems logical-system-name routing-options],
- [edit routing-instances routing-instance-name routing-options],
- [edit routing-options]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Configure generic multicast properties.

---

**NOTE:** You cannot apply a scoping policy to a specific routing instance. All scoping policies are applied to all routing instances. However, you can apply the scope statement to a specific routing instance.

---

The remaining statements are explained separately.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- *Examples: Configuring Administrative Scoping*
- *Example: Configuring Source-Specific Multicast Groups with Any-Source Override*
- *Examples: Configuring the Multicast Forwarding Cache*
- *Multicast Protocols Feature Guide for Routing Devices*
- *(indirect-next-hop on page 3066 | no-indirect-next-hop)*
no-qos-adjust

Syntax  no-qos-adjust;

Hierarchy Level  [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast interface interface-name reverse-oif-mapping],
[edit logical-systems logical-system-name routing-options multicast interface interface-name],
[edit logical-systems logical-system-name routing-options multicast interface interface-name reverse-oif-mapping],
[edit routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit routing-instances routing-instance-name routing-options multicast interface interface-name reverse-oif-mapping],
[edit routing-options multicast interface interface-name],
[edit routing-options multicast interface interface-name reverse-oif-mapping]

Release Information  Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  Disable hierarchical bandwidth adjustment for all subscriber interfaces that are identified by their MLD or IGMP request from a specific multicast interface.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  •  Example: Configuring Multicast with Subscriber VLANs
options (Routing Options)

Syntax

```plaintext
options {
    syslog (level level | upto level level);
}
```

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Configure the types of system logging messages sent about the routing protocols process to the system message logging file. These messages are also displayed on the system console. You can log messages at a particular level, or up to and including a particular level.

Options

- `level level`—Severity of the message. It can be one or more of the following levels, in order of decreasing urgency:
  - `alert`—Conditions that should be corrected immediately, such as a corrupted system database.
  - `critical`—Critical conditions, such as hard drive errors.
  - `debug`—Software debugging messages.
  - `emergency`—Panic or other conditions that cause the system to become unusable.
  - `error`—Standard error conditions.
  - `info`—Informational messages.
  - `notice`—Conditions that are not error conditions, but might warrant special handling.
  - `warning`—System warning messages.
  - `upto level level`—Log all messages up to a particular level.

Required Privilege Level

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation

- `syslog` in the Junos OS Administration Library for Routing Devices
pim-to-igmp-proxy

Syntax

pim-to-igmp-proxy {
  upstream-interface [interface-names ];
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options multicast]

Release Information

Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Configure the rendezvous point (RP) routing device that resides between a customer edge-facing Protocol Independent Multicast (PIM) domain and a core-facing PIM domain to translate PIM join or prune messages into corresponding Internet Group Management Protocol (IGMP) report or leave messages. The routing device then transmits the report or leave messages by proxying them to one or two upstream interfaces that you configure on the RP routing device. Including the pim-to-igmp-proxy statement enables you to use IGMP to forward IPv4 multicast traffic across the PIM sparse mode domains.

The remaining statement is explained separately.

Required Privilege

Level

routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation

• Configuring PIM-to-IGMP Message Translation
### pim-to-mld-proxy

**Syntax**
```
pim-to-mld-proxy {
  upstream-interface [interface-names ];
}
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options multicast]
```

**Release Information**
Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**
Configure the rendezvous point (RP) routing device that resides between a customer edge–facing Protocol Independent Multicast (PIM) domain and a core-facing PIM domain to translate PIM join or prune messages into corresponding Multicast Listener Discovery (MLD) report or leave messages. The routing device then transmits the report or leave messages by proxying them to one or two upstream interfaces that you configure on the RP routing device. Including the `pim-to-mld-proxy` statement enables you to use MLD to forward IPv6 multicast traffic across the PIM sparse mode domains.

The remaining statement is explained separately.

**Required Privilege**
- **Level**
  - routing—to view this statement in the configuration.
  - routing-control—to add this statement to the configuration.

**Related Documentation**
- Configuring PIM-to-MLD Message Translation
policy (Aggregate and Generated Routes)

Syntax

```
policy policy-name;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate) (defaults | route)],
[edit logical-systems logical-system-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],
[edit routing-instances routing-instance-name routing-options (aggregate | generate) (defaults | route)],
[edit routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate) (defaults | route)],
[edit routing-options (aggregate | generate) (defaults | route)],
[edit routing-options rib routing-table-name (aggregate | generate) (defaults | route)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Associate a routing policy when configuring an aggregate or generated route's destination prefix in the `routes` part of the `aggregate` or `generate` statement. This provides the equivalent of an import routing policy filter for the destination prefix. That is, each potential contributor to an aggregate route, along with any aggregate options, is passed through the policy filter. The policy then can accept or reject the route as a contributor to the aggregate route.

If the contributor is accepted, the policy can modify the default preferences. The contributor with the numerically smallest prefix becomes the most preferred, or `primary`, contributor. A rejected contributor still can contribute to a less specific aggregate route.

If you do not specify a policy filter, all candidate routes contribute to an aggregate route.

The following algorithm is used to compare two generated contributing routes in order to determine which one is the primary or preferred contributor:

1. Compare the protocol's `preference` of the contributing routes. The lower the preference, the better the route. This is similar to the comparison that is done while determining the best route for the routing table.
2. Compare the protocol's `preference2` of the contributing routes. The lower `preference2` value is better. If only one route has `preference2`, then this route is preferred.
3. The preference values are the same. Proceed with a numerical comparison of the prefixes' values.
   a. The primary contributor is the numerically smallest prefix value.
   b. If the two prefixes are numerically equal, the primary contributor is the route that has the smallest prefix length value.
At this point, the two routes are the same. The primary contributor does not change. An additional next hop is available for the existing primary contributor.

A rejected contributor still can contribute to less specific generated route. If you do not specify a policy filter, all candidate routes contribute to a generated route.

**Options**

- **policy-name**—Name of a routing policy.

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- Example: Summarizing Routes Through Route Aggregation
- Example: Conditionally Generating Static Routes
  - aggregate on page 3030
  - generate on page 3062

---

**policy (Flow Maps)**

**Syntax**

```bash
policy [ policy-names ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast flow-map flow-map-name],
- [edit logical-systems logical-system-name routing-options multicast flow-map flow-map-name],
- [edit routing-instances routing-instance-name routing-options multicast flow-map flow-map-name],
- [edit routing-options multicast flow-map flow-map-name]

**Release Information**

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Configure a flow map policy.

**Options**

- **policy-names**—Name of one or more policies for flow mapping.

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
**policy (SSM Maps)**

**Syntax**

```
policy [policy-names];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast ssm-map ssm-map-name]
- [edit logical-systems logical-system-name routing-options multicast ssm-map ssm-map-name]
- [edit routing-instances routing-instance-name routing-options multicast ssm-map ssm-map-name]
- [edit routing-options multicast ssm-map ssm-map-name]

**Release Information**

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Apply one or more policies to an SSM map.

**Options**

`policy-names`—Name of one or more policies for SSM mapping.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To view this statement in the configuration.

**Related Documentation**

- Example: Configuring SSM Mapping
ppm

Syntax  ppm {
  no-delegate-processing;
}

Hierarchy Level  [edit logical-systems logical-system-name routing-options],
                 [edit routing-options]

                     Statement introduced in Junos OS Release 10.2 for EX Series switches.
                     Statement introduced in Junos OS Release 11.3 for the QFX Series.
                     Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  (M120, M320, MX Series, T Series, TX Matrix routers, M7i and M10i routers with Enhanced
             CFEB [CFEB-E], EX Series switches, and QFX Series only) Disable distributed periodic
             packet management (PPM) to the Packet Forwarding Engine (on routers), to access
             ports (on EX3200 and EX4200 switches, and QFX Series), or to line cards (on EX6200
             and EX8200 switches).

             After you disable PPM, PPM processing continues to run on the Routing Engine.

             In Junos OS Release 8.2, PPM was moved from the Routing Engine to the Packet
             Forwarding Engine, access ports, or line cards. The no-delegate-processing statement
             disables the default behavior and restores the legacy behavior.

Default  Distributed PPM processing is enabled for all protocols that use PPM.

Options  no-delegate-processing—Disable PPM to the Packet Forwarding Engine, access ports, or
         line cards. Distributed PPM is enabled by default.

Required Privilege Level  routing—To view this statement in the configuration.
                          routing-control—To add this statement to the configuration.

Related Documentation  • Configuring Distributed Periodic Packet Management on an EX Series Switch (CLI
                        Procedure) on page 3026
                      • Configuring Distributed Periodic Packet Management
### ppm (Ethernet Switching)

**Syntax**

```plaintext
ppm {
    centralized;
}
```

**Hierarchy Level**

```
[edit protocols lacp]
```

**Release Information**

- Statement introduced in Junos OS Release 10.2 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- Statement introduced in Junos OS Release 12.1 for T Series devices.

**Description**

Configure PPM processing options for Link Aggregation Control Protocol (LACP) packets.

This command configures the PPM processing options for LACP packets only. You can disable distributed PPM processing for all packets that use PPM and run all PPM processing on the Routing Engine by configuring the `no-delegate-processing` configuration statement in the `[edit routing-options ppm]` configuration hierarchy.

**Default**

Distributed PPM processing is enabled for all packets that use PPM.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring Distributed Periodic Packet Management on an EX Series Switch (CLI Procedure) on page 3026
- Configuring Distributed Periodic Packet Management
**preference (Routing Options)**

**Syntax**

```
(preference | preference2 | color | color2) preference <type type>;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-optionsrib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit logical-systems routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems routing-instance-name routing-optionsrib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit routing-instances routing-instance-name routing-optionsrib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit routing-options (aggregate | generate | static) (defaults | route)],
[edit routing-optionsrib routing-table-name (aggregate | generate | static) (defaults | route)],
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Preference value for a static, aggregate, or generated route. You also can specify a secondary preference value (`preference2`), as well as colors, which are even finer-grained preference values (`color` and `color2`).

If the Junos OS routing table contains a dynamic route to a destination that has a better (lower) preference value than the static, aggregate, or generated route, the dynamic route is chosen as the active route and is installed in the forwarding table.

**Options**

`preference`—Preference value. A lower number indicates a more preferred route.

- **Range**: 0 through 4,294,967,295 (2^{32} – 1)
- **Default**: 5 (for static routes), 130 (for aggregate and generated routes)

`type type`—(Optional) Type of route.

- **Range**: 1 through 16

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- Examples: Configuring Static Routes
- Example: Summarizing Routes Through Route Aggregation
- Example: Conditionally Generating Static Routes
  - aggregate on page 3030
  - generate on page 3062
  - static on page 3118
**prefix**

**Syntax**

`prefix destination-prefix;`

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast scope scope-name],
[edit logical-systems logical-system-name routing-options multicast scope scope-name],
[edit routing-instances routing-instance-name routing-options multicast scope scope-name],
[edit routing-options multicast scope scope-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Configure the prefix for multicast scopes.

**Options**

`destination-prefix`—Address range for the multicast scope.

**Required Privilege**

Level:
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- *Examples: Configuring Administrative Scoping*
- *Example: Creating a Named Scope for Multicast Scoping*
- `multicast`
qualified-next-hop (Static Routes)

Syntax

qualified-next-hop (address | interface-name) {
  bfd-liveness-detection {
    authentication {
      algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 | meticulous-keyed-sha-1 | simple-password);
      key-chain key-chain-name;
      loose-check;
    }
    detection-time {
      threshold milliseconds;
    }
    holddown-interval milliseconds;
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    version (1 | automatic);
  }
  interface interface-name;
  metric metric;
  preference preference;
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options static route destination-prefix],
[edit logical-systems logical-system-name routing-options rib inet6.0 static route destination-prefix],
[edit logical-systems logical-system-name routing-options static route destination-prefix],
[edit routing-instances routing-instance-name routing-options static route destination-prefix],
[edit routing-options rib inet6.0 static route destination-prefix],
[edit routing-options static route destination-prefix]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Configure a static route with multiple possible next hops, each of which can have its own preference value, IGP metric that is used when the route is exported into an IGP, and Bidirectional Forwarding Detection (BFD) settings. If multiple links are operational, the one with the most preferred next hop is used. The most preferred next hop is the one with the lowest preference value.

Options

address—IPv4, IPv6, or ISO network address of the next hop.

interface-name—Name of the interface on which to configure an independent metric or preference for a static route. To configure an unnumbered interface as the next-hop..
interface for a static route, specify qualified-next-hop interface-name, where
interface-name is the name of the IPv4 or IPv6 unnumbered interface.

NOTE: For an Ethernet interface to be configured as the qualified next hop
for a static route, it must be an unnumbered interface.

To configure an Ethernet interface as an unnumbered interface, configure
the unnumbered-address <interface-name> statement at the [edit interfaces
<interface-name> unit <logical-unit-number> family <family-name>] hierarchy
level as described in Configuring an Unnumbered Interface.

The remaining statements are explained separately.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Static Route Preferences and Qualified Next Hops
• Example: Enabling BFD on Qualified Next Hops in Static Routes
readvertise

Syntax
(readvertise | no-readvertise);

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name
  routing-options rib routing-table-name static (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  routing-options static (defaults | route)],
[edit logical-systems logical-system-name routing-optionsrib routing-table-name static
  (defaults | route)],
[edit logical-systems logical-system-name routing-options static (defaults | route)],
[edit routing-instances routing-instance-name routing-options rib routing-table-name static
  (defaults | route)],
[edit routing-instances routing-instance-name routing-options static (defaults | route)],
[edit routing-optionsrib routing-table-name static (defaults | route)],
[edit routing-options static (defaults | route)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description
Configure whether static routes are eligible to be readvertised by routing protocols:

Default
Static routes are eligible to be readvertised (that is, exported from the routing table into
dynamic routing protocols) if a policy to do so is configured. To mark an IPv4 static route
as being ineligible for readvertisement, include the no-readvertise statement.

Options
readvertise—Readvertise static routes. Include the readvertise statement when configuring
an individual route in the route portion of the static statement to override a
no-readvertise option specified in the defaults portion of the statement.

no-readvertise—Mark a static route as being ineligible for readvertisement. Include the
no-readvertise option when configuring the route.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Controlling Static Routes in Routing and Forwarding Tables
• static on page 3118
### redundant-sources

**Syntax**

```plaintext
redundant-sources [ addresses ];
```

**Hierarchy Level**

- `edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast flow-map flow-map-name`
- `edit logical-systems logical-system-name routing-options multicast flow-map flow-map-name`
- `edit routing-instances routing-instance-name routing-options multicast flow-map flow-map-name`
- `edit routing-options multicast flow-map flow-map-name`

**Release Information**

- Statement introduced in Junos OS Release 8.3.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure a list of redundant sources for multicast flows defined by a flow map.

**Options**

- **addresses**—List of IPv4 or IPv6 addresses for use as redundant (backup) sources for multicast flows defined by a flow map.

**Required Privilege**

- **Level**
  - **rout**ing—To view this statement in the configuration.
  - **route**ing-control—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring a Multicast Flow Map*
resolution

Syntax  
resolution {
rib routing-table-name {
import [policy-names ];
resolution-ribs [routing-table-names ];
}
}

Hierarchy Level  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Configure the router to perform custom route resolution on protocol next hops of routes in a certain routing table. The protocol next hop is used to determine the forwarding next-hop.

For example, you might want to direct inet.2 route resolution to use topology routing tables :red.inet.0 and :blue.inet.0 for protocol next-hop IP address lookups. Or you might want to direct bgp.l3vpn.0 to use the information in inet.0 to resolve routes, thus overriding the default behavior, which is to use inet.3.

You can specify up to two routing tables in the resolution-ribs statement. The route resolution scheme first checks the first-listed routing table for the protocol next-hop address. If the address is found, it uses this entry. If it is not found, the resolution scheme checks second-listed routing table. Hence, only one routing table is used for each protocol nexthop address. For example, if you configure resolutionribbgp.l3vpn.0 resolution-ribs [inet.0 inet.3], inet.0 is checked first and then inet.3 is checked.

NOTE: Customizing route resolution might cause the routing protocol process (rpd) to consume more memory resources than it ordinarily would. When you customize route resolution, we recommend that you check the memory resources by running the show system processes and the show task memory commands. For more information, see Routing Protocol Process Memory FAQs.

The remaining statements are explained separately.

Required Privilege Level  
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
resolution-ribs

Syntax  resolution-ribs [ routing-table-names ];

Hierarchy Level  [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options resolution rib],
[edit logical-systems logical-system-name routing-options resolution rib],
[edit routing-instances routing-instance-name routing-options resolution rib],
[edit routing-options resolution rib]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Specify one or more routing tables to use for route resolution.

This statement enables you to override the default routing tables that Junos OS uses for route resolution. For example, suppose that the resolution routing table is inet.3, but you want to allow fallback resolution through inet.0. One example use case is overriding the bgp.rtarget.0 (family route-target) routing table resolution from using only inet.3 to using both inet.3 and inet.0.

Options  routing-table-names—Name of one or more routing tables.

Required Privilege Level  routing—To view this statement in the configuration.
route-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring Route Resolution on PE Routers
• Example: Configuring Multitopology Routing Based on a Multicast Source
** resolve **

**Syntax**  
resolve;

**Hierarchy Level**
- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name static (defaults | route)],
- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options static (defaults | route)],
- [edit logical-systems logical-system-name routing-options rib routing-table-name static (defaults | route)],
- [edit logical-systems logical-system-name routing-options static (defaults | route)],
- [edit routing-instances routing-instance-name routing-options rib routing-table-name static (defaults | route)],
- [edit routing-instances routing-instance-name routing-options static (defaults | route)],
- [edit routing-options rib routing-table-name static (defaults | route)],
- [edit routing-options static (defaults | route)]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Statically configure routes to be resolved to a next hop that is not directly connected. The route is resolved through the inet.0 and inet.3 routing tables.

**Default**
Static routes can point only to a directly connected next hop.

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- static on page 3118
restart-duration (Routing Options)

Syntax     restart-duration seconds;

Hierarchy Level  [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options graceful-restart],
                  [edit logical-systems logical-system-name routing-options graceful-restart],
                  [edit routing-instances routing-instance-name routing-options graceful-restart],
                  [edit routing-options graceful-restart]

Release Information  Statement introduced before Junos OS Release 7.4.
                       Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure the restart timer for graceful restart.

Options  
seconds—Configure the time period for the restart to last.

Range:  120 through 900 seconds
Default:  300 seconds

Required Privilege Level  routing—To view this statement in the configuration.
                          routing-control—To add this statement to the configuration.

Related Documentation  •  Junos OS High Availability Library for Routing Devices
**retain**

Syntax  
(no-retain | retain);

Hierarchy Level  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name static (defaults | route)],  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options static (defaults | route)],  
[edit logical-systems logical-system-name routing-options static (defaults | route)],  
[edit logical-systems routing-optionsrib routing-table-name static (defaults | route)],  
[edit routing-instances routing-instance-name routing-optionsrib routing-table-name static (defaults | route)],  
[edit routing-instances routing-instance-name routing-options static (defaults | route)],  
[edit routing-optionsrib routing-table-name static (defaults | route)],  
[edit routing-options static (defaults | route)]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Configure statically configured routes to be deleted from or retained in the forwarding table when the routing protocol process shuts down normally:

Default  
Statically configured routes are deleted from the forwarding table when the routing protocol process shuts down normally. Doing this greatly reduces the time required to restart a system that has a large number of routes in its routing table.

Options  
no-retain—Delete statically configured routes from the forwarding table when the routing protocol process shuts down normally. To explicitly specify that routes be deleted from the forwarding table, include the no-retain statement. Include this statement when configuring an individual route in the route portion of the static statement to override a retain option specified in the defaults portion of the statement.

retain—Have a static route remain in the forwarding table when the routing protocol process shuts down normally. Doing this greatly reduces the time required to restart a system that has a large number of routes in its routing table.

Required Privilege Level  
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation  
- Examples: Configuring Static Routes
- static on page 3118
reverse-oif-mapping

Syntax

reverse-oif-mapping {
   no-qos-adjust;
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit logical-systems logical-system-name routing-options multicast interface interface-name],
[edit routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit routing-options multicast interface interface-name]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 9.2 for EX Series switches.
The no-qos-adjust statement added in Junos OS Release 9.5.
The no-qos-adjust statement introduced in Junos OS Release 9.5 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable the routing device to identify a subscriber VLAN or interface based on an IGMP or MLD request it receives over the multicast VLAN.

The remaining statement is explained separately.

Required Privilege

Level: routing—to view this statement in the configuration.
Level: routing-control—to add this statement to the configuration.

Related Documentation

• Example: Configuring Multicast with Subscriber VLANs
## rpf-check-policy (Routing Options RPF)

**Syntax**

```
rfp-check-policy [ policy-names ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast]
- [edit logical-systems logical-system-name routing-options multicast]
- [edit routing-instances routing-instance-name routing-options multicast]
- [edit routing-options multicast]

**Release Information**

- Statement introduced in Junos OS Release 8.1.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Apply policies for disabling RPF checks on arriving multicast packets. The policies must be correctly configured.

**Options**

- **policy-names**—Name of one or more multicast RPF check policies.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring RPF Policies
rib (General)

Syntax

```
rib routing-table-name {
  aggregate {
    defaults {
      ... aggregate-options ...
    }
    route destination-prefix {
      policy policy-name;
      ... aggregate-options ...
    }
  }
  generate {
    defaults {
      generate-options;
    }
    route destination-prefix {
      policy policy-name;
      generate-options;
    }
  }
  martians {
    destination-prefix match-type <allow>;
  }
  static {
    defaults {
      static-options;
    }
    rib-group group-name;
    route destination-prefix {
      next-hop;
      static-options;
    }
  }
}
```

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Create a routing table.

Explicitly creating a routing table with `routing-table-name` is optional if you are not adding any static, martian, aggregate, or generated routes to the routing table and if you also are creating a routing table group.
NOTE: The IPv4 multicast routing table (inet.1) and the IPv6 multicast routing table (inet6.1) are not supported for this statement.

**Default**
If you do not specify a routing table name with the `routing-table-name` option, the software uses the default routing tables, which are `inet.0` for unicast routes and `inet.1` for the multicast cache.

**Options**
`routing-table-name`—Name of the routing table, in the following format:

```
protocol [ identifier ]
```

In a routing instance, the routing table name must include the routing instance name.
For example, if the routing instance name is `link0`, the routing table name might be `link0.inet6.0`.

- `protocol` is the protocol family. It can be `inet6` for the IPv6 family, `inet` for the IPv4 family, `iso` for the ISO protocol family, or `instance-name.iso.0` for an ISO routing instance.
- `identifier` is a positive integer that specifies the instance of the routing table.

**Default:** `inet.0`

The remaining statements are explained separately.

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- `Example: Creating Routing Tables`
- `passive`
rib (Route Resolution)

Syntax

rib routing-table-name {
  import [policy-names ];
  resolution-ribs [routing-table-names ];
}

Hierarchy Level
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options resolution ],
[edit logical-systems logical-system-name routing-options resolution ],
[edit routing-instances routing-instance-name routing-options resolution ],
[edit routing-options resolution ]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Specify a routing table name for route resolution.

The remaining statements are explained separately.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Route Resolution on PE Routers
### rib-group (Routing Options)

**Syntax**

```
rib-group group-name;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options interface-routes]`
- `[edit logical-systems logical-system-name routing-options interface-routes]`
- `[edit logical-systems logical-system-name routing-options rib routing-table-name static]`
- `[edit logical-systems logical-system-name routing-options static]`
- `[edit routing-instances routing-instance-name routing-options interface-routes]`
- `[edit routing-options interface-routes]`
- `[edit routing-options rib routing-table-name static]`
- `[edit routing-options static]`

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure which routing table groups interface routes are imported into.

**Options**

`group-name`—Name of the routing table group. The name must start with a letter and can include letters, numbers, and hyphens. It generally does not make sense to specify more than a single routing table group.

**Required Privilege Level**

- Routing—to view this statement in the configuration.
- Routing-control—to add this statement to the configuration.

**Related Documentation**

- `Example: Importing Direct and Static Routes Into a Routing Instance`
- `Example: Exporting Specific Routes from One Routing Table Into Another Routing Table`
- `interface-routes on page 3071`
- `rib-groups on page 3107`
ribbon

Syntax

```
rib-groups {
  group-name {
    export-rib group-name;
    import-policy [ policy-names ];
    import-rib [ group-names ];
  }
}
```

Hierarchy Level

[edit logical-systems logical-system-name routing-options],
[edit routing-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Group one or more routing tables to form a routing table group. A routing protocol can import routes into all the routing tables in the group and can export routes from a single routing table.

Each routing table group must contain one or more routing tables that Junos OS uses when importing routes (specified in the `import-rib` statement) and optionally can contain one routing table group that Junos OS uses when exporting routes to the routing protocols (specified in the `export-rib` statement).

The first routing table you specify is the primary routing table, and any additional routing tables are the secondary routing tables.

The primary routing table determines the address family of the routing table group. To configure an IP version 4 (IPv4) routing table group, specify `inet.0` as the primary routing table. To configure an IP version 6 (IPv6) routing table group, specify `inet6.0` as the primary routing table. If you configure an IPv6 routing table group, the primary and all secondary routing tables must be IPv6 routing tables (`inet6.x`).

In Junos OS Release 9.5 and later, you can include both IPv4 and IPv6 routing tables in an IPv4 import routing table group using the `import-rib` statement. In releases prior to Junos OS Release 9.5, you can only include either IPv4 or IPv6 routing tables in the same `import-rib` statement. The ability to configure an import routing table group with both IPv4 and IPv6 routing tables enables you, for example, to populate the `inet6.3` routing table with IPv6 addresses that are compatible with IPv4. Specify `inet.0` as the primary routing table, and specify `inet6.3` as a secondary routing table.

**NOTE:** On EX Series switches, only dynamically learned routes can be imported from one routing table group to another.
NOTE: If you configure an import routing table group that includes both IPv4 and IPv6 routing tables, any corresponding export routing table group must include only IPv4 routing tables.

If you have configured a routing table, configure the OSPF primary instance at the [edit protocols ospf] hierarchy level with the statements needed for your network so that routes are installed in inet.0 and in the forwarding table. Make sure to include the routing table group. For more information, see Example: Configuring Multiple Routing Instances of OSPF.

After specifying the routing table from which to import routes, you can apply one or more policies to control which routes are installed in the routing table group. To apply a policy to routes being imported into the routing table group, include the import-policy statement.

Options

**group-name**—Name of the routing table group. The name must start with a letter and can include letters, numbers, and hyphens.

The remaining statements are explained separately.

Required Privilege

Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation

- Example: Exporting Specific Routes from One Routing Table Into Another Routing Table
- rib-group on page 3106
route-distinguisher-id

Syntax    
route-distinguisher-id ip-address;

Hierarchy Level    
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information    
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description    
Automatically assign a route distinguisher to the routing instance.

If you configure the route-distinguisher statement in addition to the route-distinguisher-id statement, the value configured for route-distinguisher supersedes the value generated from route-distinguisher-id.

NOTE: To avoid a conflict in the two route distinguisher values, it is recommended to ensure that the first half of the route distinguisher obtained by configuring the route-distinguisher statement is different from the first half of the route distinguisher obtained by configuring the route-distinguisher-id statement.

Options    
ip-address—Address for routing instance.

Required Privilege Level    
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation    
• Example: Configuring BGP Route Target Filtering for VPNs
• Configuring Routing Instances on PE Routers in VPNs
route-record

Syntax       route-record;

Hierarchy Level       [edit logical-systems logical-system-name routing-options],
                      [edit routing-options]

Release Information  Statement introduced before Junos OS Release 7.4.
                      Statement introduced in Junos OS Release 9.0 for EX Series switches.
                      Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Export the AS path and routing information to the traffic sampling process.

Before you can perform flow aggregation, the routing protocol process must export the
AS path and routing information to the sampling process.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Enabling Flow Aggregation
• Junos OS Services Interfaces Library for Routing Devices
router-id

Syntax

router-id address;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit logical-systems logical-system-name routing-options],
[edit routing-instances routing-instance-name routing-options],
[edit routing-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Specify the routing device’s IP address.

The router identifier is used by BGP and OSPF to identify the routing device from which a packet originated. The router identifier usually is the IP address of the local routing device. If you do not configure a router identifier, the IP address of the first interface to come online is used. This is usually the loopback interface. Otherwise, the first hardware interface with an IP address is used.

NOTE: We strongly recommend that you configure the router identifier under the [edit routing-options] hierarchy level to avoid unpredictable behavior if the interface address on a loopback interface changes.

For more information about the router identifier in OSPF, see Example: Configuring an OSPF Router Identifier.

Options

address—IP address of the routing device.

Default: Address of the first interface encountered by Junos OS

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Examples: Configuring External BGP Peering
• Examples: Configuring Internal BGP Peering
routing-options

Syntax  routing-options { ... }

Hierarchy Level  [edit],
[edit logical-systems logical-system-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name],
[edit routing-instances routing-instance-name]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure protocol-independent routing properties.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.


scope

Syntax  scope scope-name {
    interface [ interface-names ];
    prefix destination-prefix;
}

Hierarchy Level  [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options multicast]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  Configure multicast scoping.

Options  scope-name—Name of the multicast scope.

The remaining statements are explained separately.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  • Example: Creating a Named Scope for Multicast Scoping
### scope-policy

**Syntax**

```
scope-policy [ policy-names ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name routing-options multicast],
- [edit routing-options multicast]

**NOTE:** You can configure a scope policy at these two hierarchy levels only. You cannot apply a scope policy to a specific routing instance, because all scoping policies are applied to all routing instances. However, you can apply the scope statement to a specific routing instance at the [edit routing-instances routing-instance-name routing-options multicast] or [edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast] hierarchy level.

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Apply policies for scoping. The policy must be correctly configured at the edit policy-options policy-statement hierarchy level.

**Options**

- `policy-names`—Name of one or more multicast scope policies.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- scope on page 3112
- Example: Using a Scope Policy for Multicast Scoping
source (Source-Specific Multicast)

**Syntax**

```
source [ addresses ];
```

**Hierarchy Level**
```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast ssm-map ssm-map-name], [edit logical-systems logical-system-name routing-options multicast ssm-map ssm-map-name], [edit routing-instances routing-instance-name routing-options multicast ssm-map ssm-map-name], [edit routing-options multicast ssm-map ssm-map-name]
```

**Release Information**
Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**
Specify IPv4 or IPv6 source addresses for an SSM map.

**Options**
```
addresses—IPv4 or IPv6 source addresses.
```

**Required Privilege**
```
routing—to view this statement in the configuration.
routing-control—to view this statement in the configuration.
```

**Related Documentation**
- Example: Configuring SSM Mapping
source-routing

| Syntax          | source-routing [ (ip | ipv6) ] |
|-----------------|---------------------------------|
| Hierarchy Level | [edit routing-options]          |
| Description     | Enable source routing. Source routing allows a sender of a packet to partially or completely specify the route the packet takes through the network. In contrast, in non-source routing protocols, routers in the network determine the path based on the packet’s destination. |
| Default         | Disabled                        |
| Required Privilege Level | routing—To view this statement in the configuration. routing-control—To add this statement to the configuration. |
| Related Documentation | • Example: Configuring Filter-Based Forwarding on the Source Address |
# ssm-groups

**Syntax**

```bash
ssm-groups [ ip-addresses ];
```

**Hierarchy Level**

- `edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast`
- `edit logical-systems logical-system-name routing-options multicast`
- `edit routing-instances routing-instance-name routing-options multicast`
- `edit routing-options multicast`

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.
- Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Configure source-specific multicast (SSM) groups.

By default, the SSM group multicast address is limited to the IP address range from 232.0.0.0 through 232.255.255.255. However, you can extend SSM operations into another Class D range by including the `ssm-groups` statement in the configuration. The default SSM address range from 232.0.0.0 through 232.255.255.255 cannot be used in the `ssm-groups` statement. This statement is for adding other multicast addresses to the default SSM group addresses. This statement does not override the default SSM group address range.

IGMPv3 supports SSM groups. By utilizing inclusion lists, only sources that are specified send to the SSM group.

**Options**

`ip-addresses`—List of one or more additional SSM group addresses separated by a space.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring Source-Specific Multicast Groups with Any-Source Override](#)
ssm-map (Routing Options Multicast)

Syntax

ssm-map ssm-map-name {
    policy [ policy-names ];
    source [ addresses ];
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options multicast]

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Configure SSM mapping.

Options

ssm-map-name—Name of the SSM map.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring SSM Mapping
static (Routing Options)

Syntax

```
static {
  defaults {
    static-options;
  }
  rib-group group-name;
  route destination-prefix {
    bfd-liveness-detection {
      authentication {
        algorithm algorithm-name;
        key-chain key-chain-name;
        loose-check;
      }
      detection-time {
        threshold milliseconds;
      }
      local-address ip-address;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      minimum-receive-ttl number;
      multiplier number;
      neighbor address;
      no-adaptation;
      transmit-interval {
        threshold milliseconds;
        minimum-interval milliseconds;
      }
      version (1 | automatic);
    }
    next-hop address;
    next-hop options;
    qualified-next-hop address {
      bfd-liveness-detection {
        authentication {
          algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
                      meticulous-keyed-sha-1 | simple-password);
          key-chain key-chain-name;
          loose-check;
        }
        detection-time {
          threshold milliseconds;
        }
        holddown-interval milliseconds;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        version (1 | automatic);
      }
    }
  }
}
```
Configure static routes to be installed in the routing table. You can specify any number of routes within a single static statement, and you can specify any number of static options in the configuration.
**Options**

**defaults**—(Optional) Specify global static route options. These options only set default attributes inherited by all newly created static routes. These are treated as global defaults and apply to all the static routes you configure in the `static` statement.

---

**NOTE:** Specifying the global static route options does not create default routes. These options only set default attributes inherited by all newly created static routes.

---

**route**—Configure individual static routes. In this part of the `static` statement, you optionally can configure static route options. These options apply to the individual destination only and override any options you configured in the `defaults` part of the `static` statement.

- **destination-prefix/prefix-length**—`destination-prefix` is the network portion of the IP address, and `prefix-length` is the destination prefix length.

When you configure an individual static route in the `route` part of the `static` statement, specify the destination of the route (in `route destination-prefix`) in one of the following ways:

- **network/mask-length**, where `network` is the network portion of the IP address and `mask-length` is the destination prefix length.
- **default** if this is the default route to the destination. This is equivalent to specifying an IP address of 0.0.0.0/0.

---

**NOTE:** IPv4 packets with a destination of 0.0.0.0 (the obsoleted limited broadcast address) and IPv6 packets with a destination of 0:0 are discarded by default. To forward traffic destined to these addresses, you can add a static route to 0.0.0.0/32 for IPv4 or 0::/128 for IPv6.

---

- **nsap-prefix**—`nsap-prefix` is the network service access point (NSAP) address for ISO.
- **next-hop address**—Reach the next-hop routing device by specifying an IP address, an interface name, or an ISO network entity title (NET).

IPv4 or IPv6 address of the next hop to the destination, specified as:

- IPv4 or IPv6 address of the next hop
- Interface name (for point-to-point interfaces only)
- `address` or `interface-name` to specify an IP address of a multipoint interface or an interface name of a point-to-point interface.

---

**NOTE:** If an interface becomes unavailable, all configured static routes on that interface are withdrawn from the routing table.
NOTE: Load balancing is not supported on management and internal Ethernet (fxo) interfaces because this type of interface cannot handle the routing process. On fxp interfaces, you cannot configure multiple next hops and enable load balancing.

**next-hop options**—Additional information for how to manage forwarding of packets to the next hop.

- **discard**—Do not forward packets addressed to this destination. Instead, drop the packets, do not send ICMP (or ICMPv6) unreachable messages to the packets’ originators, and install a reject route for this destination into the routing table.

- **iso-net**—Reach the next-hop routing device by specifying an ISO NSAP.
- **next-table routing-table-name**—Name of the next routing table to the destination.

If you use the `next-table` action, the configuration must include a term qualifier that specifies a different table than the one specified in the `next-table` action. In other words, the term qualifier in the `from` statement must exclude the table in the `next-table` action. In the following example, the first term contains `rib vrf-customer2.inet.0` as a matching condition. The action specifies a next-hop in a different routing table, `vrf-customer1.inet.0`. The second term does the opposite by using `rib vrf-customer1.inet.0` in the match condition and `vrf-customer2.inet.0` in the `next-table` action.

```plaintext
term1 {
  from {
    protocol bgp;
    rib vrf-customer2.inet.0;
    community customer;
  }
  then {
    next-hop next-table vrf-customer1.inet.0;
  }
}
term2 {
  from {
    protocol bgp;
    rib vrf-customer1.inet.0;
    community customer;
  }
  then {
    next-hop next-table vrf-customer2.inet.0;
  }
}
```

**NOTE:** Within a routing instance, you cannot configure a static route with the `next-table inet.0` statement if any static route in the main routing instance is already configured with the `next-table` statement to point to the `inet.0` routing table of the routing instance. For example, if you configure on the main routing instance a static route 192.168.88.88/32 with the `next-table test.inet.0` statement and the routing instance test is also configured with a static route 192.168.88.88/32 with the `next-table inet.0` statement, the commit operation fails. Instead, you must configure a routing table group both on the main instance and on the routing instance, which enables you to install the static route into both routing tables.
• **receive**—Install a route for this next-hop destination into the routing table.

The **receive** option forces the packet to be sent to the Routing Engine.

The **receive** option can be useful in the following cases:

  • For receiving MPLS packets destined to a VRF instance's loopback address
  • For receiving packets on a link's subnet address, with zeros in the host portion of the address

• **reject**—Do not forward packets addressed to this destination. Instead, drop the packets, send ICMP (or ICMPv6) unreachable messages to the packets' originators, and install a reject route for this destination into the routing table.

**static-options**—(Optional under **route**) Additional information about static routes, which is included with the route when it is installed in the routing table.

You can specify one or more of the following in **static-options**. Each of the options is explained separately.

  • **(active | passive):**
  • **as-path** `<as-path> <origin (egp | igp | incomplete)> <atomic-aggregate> <aggregator as-number in-address>**;
  • **community [ community-ids ];**
  • **(install | no-install);**
  • **(metric | metric2 | metric3 | metric4) value <type type>;**
  • **(preference | preference2 | color | color2) preference <type type>;**
  • **(readvertise | no-readvertise);**
  • **(resolve | no-resolve);**
  • **(retain | no-retain);**
  • **tag string;**

The remaining statements are explained separately.

**Required Privilege**

- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- **Examples: Configuring Static Routes**
subscriber-leave-timer

Syntax

subscriber-leave-timer seconds;

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit logical-systems logical-system-name routing-options multicast interface interface-name],
[edit routing-instances routing-instance-name routing-options multicast interface interface-name],
[edit routing-options multicast interface interface-name]

Release Information

Statement introduced in Junos OS Release 9.2.
Statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Length of time before the multicast VLAN updates QoS data (for example, available bandwidth) for subscriber interfaces after it receives an IGMP leave message.

Options

seconds—Length of time before the multicast VLAN updates QoS data (for example, available bandwidth) for subscriber interfaces after it receives an IGMP leave message. Specifying a value of 0 results in an immediate update. This is the same as if the statement were not configured.

Range: 0 through 30
Default: 0 seconds

Required Privilege

Level

routing—To view this statement in the configuration.
Routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring Multicast with Subscriber VLANs
tag (Routing Options)

Syntax  
tag string;

Hierarchy Level  
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-options (aggregate | generate | static) (defaults | route)],
[edit logical-systems logical-system-name routing-options rib routing-table-name (aggregate | generate | static) (defaults | route)],

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  
Associate an OSPF tag with a static, aggregate, or generated route.

Default  
No OSPF tag strings are associated with static routes.

Options  
string—OSPF tag string.

Required Privilege Level  
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  
• Examples: Configuring Static Routes
  • Example: Summarizing Routes Through Route Aggregation
  • Example: Conditionally Generating Static Routes
  • aggregate on page 3030
  • generate on page 3062
  • static on page 3118
threshold (Multicast Forwarding Cache)

Syntax

```
threshold {
  log-warning value;
  suppress value <reuse value>;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast forwarding-cache],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast forwarding-cache family (inet | inet6)],
[edit logical-systems logical-system-name routing-options multicast forwarding-cache],
[edit logical-systems logical-system-name routing-options multicast forwarding-cache family (inet | inet6)],
[edit routing-instances routing-instance-name routing-options multicast forwarding-cache],
[edit routing-instances routing-instance-name routing-options multicast forwarding-cache (inet | inet6)],
[edit routing-options multicast forwarding-cache],
[edit routing-options multicast forwarding-cache family (inet | inet6)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Configure the global suppression, reuse, and warning log message thresholds for multicast forwarding cache limits. You can configure the thresholds globally for the multicast forwarding cache or individually for the IPv4 and IPv6 multicast forwarding caches. Configuring the `threshold` statement globally for the multicast forwarding cache or including the `family` statement to configure the thresholds for the IPv4 and IPv6 multicast forwarding caches are mutually exclusive.

To confirm the configured threshold values, use the `show multicast forwarding-cache statistics` command.

Options

- `reuse value`—(Optional) Value at which to begin creating new multicast forwarding cache entries. If configured, this number should be less than the `suppress` value.
  
  **Range:** 1 through 200,000

- `suppress value`—Value at which to begin suppressing new multicast forwarding cache entries. This value is mandatory. This number should be greater than the `reuse` value.
  
  **Range:** 1 through 200,000

The remaining statement is explained separately.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Examples: Configuring the Multicast Forwarding Cache
timeout (Flow Maps)

Syntax  
```
timeout (never non-discard-entry-only | minutes);
```

Hierarchy Level  
```
[edit logical-systems logical-system-name routing-instances routing-instance-name
 routing-options multicast flow-map flow-map-name],
[edit logical-systems logical-system-name routing-options multicast flow-map
 flow-map-name],
[edit routing-instances routing-instance-name routing-options multicast flow-map
 flow-map-name],
[edit routing-options multicast flow-map flow-map-name]
```

Release Information  
Statement introduced in Junos OS Release 8.2.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.  
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  
Configure the timeout value for multicast forwarding cache entries associated with the flow map.

Options  
- `minutes`—Length of time that the forwarding cache entry remains active.  
  Range: 1 through 720
- `never non-discard-entry-only`—Specify that the forwarding cache entry always remain active. If you omit the `non-discard-entry-only` option, all multicast forwarding entries, including those in forwarding and pruned states, are kept forever. If you include the `non-discard-entry-only` option, entries with forwarding states are kept forever, and entries with pruned states time out.

Required Privilege  
- **Level**
  - routing—To view this statement in the configuration.  
  - routing-control—To add this statement to the configuration.
timeout (Multicast)

Syntax  
timeout minutes <family (inet | inet6)>

Hierarchy Level  
[edit logical-systems logical-system-name routing-instances routing-instance-name 
  routing-options multicast forwarding-cache], 
[edit logical-systems logical-system-name routing-options multicast forwarding-cache], 
[edit routing-instances routing-instance-name routing-options multicast forwarding-cache], 
[edit routing-options multicast forwarding-cache]

Release Information  
Statement introduced in Junos OS Release 8.2.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.3 for the QFX Series.  
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description  
Configure the timeout value for multicast forwarding cache entries.

Options  
minutes—Length of time that the forwarding cache limit remains active.  
Range: 1 through 720

family (inet | inet6)—(Optional) Apply the configured timeout to either IPv4 or IPv6 multicast forwarding cache entries. Configuring the timeout statement globally for the multicast forwarding cache or including the family statement to configure the timeout value for the IPv4 and IPv6 multicast forwarding caches are mutually exclusive.

Default:  By default, the configured timeout applies to both IPv4 and IPv6 multicast forwarding cache entries.

Required Privilege Level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

Related Documentation  
• Example: Configuring the Multicast Forwarding Cache
traceoptions (Routing Options)

Syntax

traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <disable>;
}

Hierarchy Level

[edit logical-systems logical-system-name routing-instances routing-instance-name
  routing-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  routing-options multicast],
[edit logical-systems logical-system-name routing-options],
[edit logical-systems logical-system-name routing-options multicast],
[edit routing-instances routing-instance-name routing-options],
[edit routing-instances routing-instance-name routing-options multicast],
[edit routing-options],
[edit routing-options flow],
[edit routing-options multicast]

Release Information

Statement introduced before Junos OS Release 7.4.
nsr-synchronization flag for BGP, IS-IS, LDP, and OSPF added in Junos OS Release 8.4.
nsr-synchronization and nsr-packet flags for BFD sessions added in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
nsr-synchronization flag for RIP and RIPng added in Junos OS Release 9.0.
nsr-synchronization flag for Layer 2 VPNs and VPLS added in Junos OS Release 9.1.
nsr-synchronization flag for PIM added in Junos OS Release 9.3.
nsr-synchronization flag for MPLS added in Junos OS Release 10.1.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
nsr-synchronization flag for MSDP added in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Define tracing operations that track all routing protocol functionality in the routing device.
To specify more than one tracing operation, include multiple flag statements.

Default

If you do not include this statement, no global tracing operations are performed.

Options

Values:

disable—(Optional) Disable the tracing operation. You can use this option to disable a
  single operation when you have defined a broad group of tracing operations, such
  as all.

file filename—Name of the file to receive the output of the tracing operation. Enclose the
  name within quotation marks. All files are placed in the directory /var/log. We
  recommend that you place global routing protocol tracing output in the file
  routing-log.

files number—(Optional) Maximum number of trace files. When a trace file named
  trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and
so on, until the maximum number of trace files is reached. Then, the oldest trace file
is overwritten. Note that if you specify a maximum number of files, you also must
specify a maximum file size with the size option.

**Range:** 2 through 1000 files

**Default:** 10 files

flag — Tracing operation to perform. To specify more than one tracing operation,
include multiple flag statements. These are the global routing protocol tracing
options:

- **all** — All tracing operations
- **condition-manager** — Condition-manager events
- **config-internal** — Configuration internals
- **general** — All normal operations and routing table changes (a combination of the normal
  and route trace operations)
- **graceful-restart** — Graceful restart operations
- **normal** — All normal operations
- **nsr-packet** — Detailed trace information for BFD nonstop active routing only
- **nsr-synchronization** — Tracing operations for nonstop active routing
- **nsr-synchronization-detail** — (MPLS only) Tracing operations for nonstop active routing
  in detail
- **parse** — Configuration parsing
- **policy** — Routing policy operations and actions
- **regex-parse** — Regular-expression parsing
- **route** — Routing table changes
- **state** — State transitions
- **task** — Interface transactions and processing
- **timer** — Timer usage

no-world-readable — (Optional) Prevent any user from reading the log file.

size size — (Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB),
or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed
trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed
trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues
until the maximum number of trace files is reached. Then, the oldest trace file is
overwritten. Note that if you specify a maximum file size, you also must specify a
maximum number of trace files with the files option.

**Syntax:** xk to specify KB, xm to specify MB, or xg to specify GB

**Range:** 10 KB through the maximum file size supported on your system

**Default:** 128 KB
**world-readable**—(Optional) Allow any user to read the log file.

**Required Privilege Level**
- routing and trace—To view this statement in the configuration.
- routing-control and trace-control—To add this statement to the configuration.

**Related Documentation**
- Example: *Tracing Global Routing Protocol Operations*
- *Tracing Nonstop Active Routing Synchronization Events*
**upstream-interface**

**Syntax**

```
upstream-interface [ interface-names ];
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast pim-to-igmp-proxy],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options multicast pim-to-mld-proxy],
[edit logical-systems logical-system-name routing-options multicast pim-to-igmp-proxy],
[edit logical-systems logical-system-name routing-options multicast pim-to-mld-proxy],
[edit routing-instances routing-instance-name routing-options multicast pim-to-igmp-proxy],
[edit routing-instances routing-instance-name routing-options multicast pim-to-mld-proxy],
[edit routing-options multicast pim-to-igmp-proxy],
[edit routing-options multicast pim-to-mld-proxy]
```

**Release Information**

Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

**Description**

Configure at least one, but not more than two, upstream interfaces on the rendezvous point (RP) routing device that resides between a customer edge–facing Protocol Independent Multicast (PIM) domain and a core-facing PIM domain. The RP routing device translates PIM join or prune messages into corresponding IGMP report or leave messages (if you include the `pim-to-igmp-proxy` statement), or into corresponding MLD report or leave messages (if you include the `pim-to-mld-proxy` statement). The routing device then proxies the IGMP or MLD report or leave messages to one or both upstream interfaces to forward IPv4 multicast traffic (for IGMP) or IPv6 multicast traffic (for MLD) across the PIM domains.

**Options**

`interface-names`—Names of one or two upstream interfaces to which the RP routing device proxies IGMP or MLD report or leave messages for transmission of multicast traffic across PIM domains. You can specify a maximum of two upstream interfaces on the RP routing device. To configure a set of two upstream interfaces, specify the full interface names, including all physical and logical address components, within square brackets (`[]`).

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring PIM-to-IGMP Message Translation](#)
- [Configuring PIM-to-MLD Message Translation](#)
CHAPTER 62

Administration

• Routine Monitoring on page 3133
• Operational Commands on page 3135

Routine Monitoring

• Monitoring Routing Information on page 3133

Monitoring Routing Information

**Purpose**  Use the monitoring functionality to view the inet.0 routing table on the routing device.

**Action**  To view the routing tables in the J-Web interface, select Monitor > Routing > Route Information. Apply a filter or a combination of filters to view messages. You can use filters to display relevant events.

To view the routing table in the CLI, enter the following commands in the CLI interface:

- `show route terse`
- `show route detail`

**Meaning**  Table 379 on page 3133 describes the different filters, their functions, and the associated actions.

Table 380 on page 3134 summarizes key output fields in the routing information display.

<table>
<thead>
<tr>
<th>Table 379: Filtering Route Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Destination Address</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Next hop address</td>
</tr>
</tbody>
</table>
### Table 379: Filtering Route Messages (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive protocol</td>
<td>Specifies the dynamic routing protocol using which the routing information was received through a particular neighbor.</td>
<td>Enter the routing protocol.</td>
</tr>
<tr>
<td>Best route</td>
<td>Specifies only the best route available.</td>
<td>Select the view details of the best route.</td>
</tr>
<tr>
<td>Inactive routes</td>
<td>Specifies the inactive routes.</td>
<td>Select the view details of inactive routes.</td>
</tr>
<tr>
<td>Exact route</td>
<td>Specifies the exact route.</td>
<td>Select the view details of the exact route.</td>
</tr>
<tr>
<td>Hidden routes</td>
<td>Specifies the hidden routes.</td>
<td>Select the view details of hidden routes.</td>
</tr>
<tr>
<td>Search</td>
<td>Applies the specified filter and displays the matching messages.</td>
<td>To apply the filter and display messages, click Search.</td>
</tr>
</tbody>
</table>

### Table 380: Summary of Key Routing Information Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Route Addresses</td>
<td>The list of static route addresses.</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol from which the route was learned: Static, Direct, Local, or the name of a particular protocol.</td>
<td></td>
</tr>
<tr>
<td>Preference</td>
<td>The preference is the individual preference value for the route.</td>
<td>The route preference is used as one of the route selection criteria.</td>
</tr>
<tr>
<td>Next-Hop</td>
<td>Network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.</td>
<td>If a next hop is listed as Discard, all traffic with that destination address is discarded rather than routed. This value generally means that the route is a static route for which the discard attribute has been set. If a next hop is listed as Reject, all traffic with that destination address is rejected. This value generally means that the address is unreachable. For example, if the address is a configured interface address and the interface is unavailable, traffic bound for that address is rejected. If a next hop is listed as Local, the destination is an address on the host (either the loopback address or Ethernet management port 0 address, for example).</td>
</tr>
<tr>
<td>Age</td>
<td>How long the route has been active.</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Flags for this route.</td>
<td>There are many possible flags.</td>
</tr>
</tbody>
</table>
Table 380: Summary of Key Routing Information Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Path</td>
<td>AS path through which the route was learned. The letters of the AS path indicate the path origin:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete. Typically, the AS path was aggregated.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring Static Routing (J-Web Procedure) on page 3024
- Configuring Static Routing (CLI Procedure) on page 3024
- Layer 3 Protocols Supported on EX Series Switches on page 2553

**Operational Commands**
clear ipv6 neighbors

Syntax

```
clear ipv6 neighbors
<all | host hostname>
```

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.3 for EX Series switches.
- Command introduced in Junos OS Release 12.2 for the QFX Series.

Description

Clear IPv6 neighbor cache information.

Options

- **none**—Clear all IPv6 neighbor cache information.
- **all**—(Optional) Clear all IPv6 neighbor cache information.
- **host hostname**—(Optional) Clear the information for the specified IPv6 neighbors.

Required Privilege

- **Level** view

Related Documentation

- [show ipv6 neighbors on page 3145](#)

List of Sample Output

- **clear ipv6 neighbors on page 3136**

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear ipv6 neighbors
```

```
user@host> clear ipv6 neighbors
```
### show as-path

#### Syntax

```
show as-path
<brief | detail>
<logical-system (all | logical-system-name)>
```

#### Syntax (EX Series Switches)

```
show as-path
<brief | detail>
```

#### Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

#### Description

Display the distribution of autonomous system (AS) paths that the local routing device is using (usually through the routing table). Use this command to debug problems for AS paths and to understand how AS paths have been manipulated through a policy (through the `as-path-prepend` action) or through aggregation.

AS paths are stored in a hash table. A hash table is one method for fast lookup. Each entry in the table is called a bucket. Junos OS computes a hash value that indicates in which bucket the AS path is stored. The AS paths are dispersed among the hash buckets so that a manageable number of AS paths is stored in each bucket. Only unique AS paths are stored. Duplicate AS paths increase a reference count, but do not increase the number of AS paths stored in the hash table.

#### Options

- **none**—Display basic information about AS paths that the local routing device is using (same as brief).
- **brief | detail**—(Optional) Display the specified level of output.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

#### Required Privilege

- **Level**
  - view

#### Related Documentation

- `show as-path summary on page 3143`

#### List of Sample Output

- `show as-path on page 3138`
- `show as-path detail on page 3139`

#### Output Fields

Table 381 on page 3137 lists the output fields for the `show as-path` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total AS paths</td>
<td>Total number of AS paths.</td>
<td>brief none</td>
</tr>
<tr>
<td>Bucket</td>
<td>Bucket number.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

---

Copyright © 2013, Juniper Networks, Inc.
### Table 381: show as-path Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Count</strong></td>
<td>Number of AS path entries in this bucket.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>AS path</strong></td>
<td>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete; typically, the AS path was aggregated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Atomic—Route is an aggregate of several route prefixes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Aggregator—Routing device has summarized a range of prefixes.</td>
<td></td>
</tr>
<tr>
<td><strong>domain</strong></td>
<td>Number of independent AS domains. The AS paths of an independent AS domain are not shared with the AS paths and AS path attributes of other domains, including the master routing instance domain.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>neighbor as</strong></td>
<td>AS peer address.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>length</strong></td>
<td>Length of the AS path.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>segments</strong></td>
<td>Length of the AS segment descriptor.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>references</strong></td>
<td>Path reference count.</td>
<td>detail</td>
</tr>
</tbody>
</table>

### Sample Output

```
show as-path
Total AS paths: 30382
Bucket 0 Count: 36
I
14203 2914 174 31752 I
14203 2914 701 21512 I
14203 2914 1239 26632 I
14203 2914 1239 29704 I
14203 2914 4323 10248 I
14203 2914 4766 23560 I
14203 2914 6395 32776 I
14203 2914 7911 11272 I
14203 2914 12180 18440 I
14203 2914 17408 17416 I
14203 2914 701 702 24586 I
14203 2914 1239 4657 9226 I
14203 2914 1239 7132 16394 I
14203 2914 1299 8308 34826 I
14203 2914 3320 5603 28682 I
14203 2914 3491 1680 33802 I
14203 2914 3549 7908 27658 I
14203 2914 3549 20804 30730 I
14203 2914 7018 2687 9226 I
14203 2914 174 9318 9318 23564 I
```

**user@host>**
<table>
<thead>
<tr>
<th>AS Path</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>14203 2914 701 3786 3786 23564</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 701 4761 4795 9228</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 1239 7132 5673 18444</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 3491 20485 24588 24588</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 5511 2200 1945 2060</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 7911 14325 14325 14348</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 701 4637 9230 9230 9230</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 6395 14 14 14 14</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 9299 6163 6163 6163 9232</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 3356 3356 3356 3356 11955 21522</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 5511 2200 1945 2060</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 7911 14325 14325 14348</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 701 4637 9230 9230 9230</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 6395 14 14 14 14</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 9299 6163 6163 6163 9232</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 3356 3356 3356 3356 11955 21522</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 9299 6163 6163 6163 9232</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 174 30209 30222 30222 30222</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 1299 5377</td>
<td>(Atomic) Aggregator: 5377 193.219.192.22</td>
</tr>
<tr>
<td>14203 2914 4323 36097</td>
<td>(Atomic) Aggregator: 36097 216.69.252.254</td>
</tr>
<tr>
<td>14203 2914 209 2516 17676 23813</td>
<td>(Atomic) Aggregator: 23813 219.127.233.66</td>
</tr>
</tbody>
</table>

Bucket 1 Count: 28

<table>
<thead>
<tr>
<th>AS Path</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>14203 2914 35847</td>
<td>I</td>
</tr>
<tr>
<td>14203 2914 174</td>
<td>19465 I</td>
</tr>
<tr>
<td>14203 2914 174</td>
<td>35849 I</td>
</tr>
<tr>
<td>14203 2914 2828</td>
<td>32777 I</td>
</tr>
<tr>
<td>14203 2914 4323</td>
<td>14345 I</td>
</tr>
<tr>
<td>14203 2914 4323</td>
<td>29705 I</td>
</tr>
<tr>
<td>14203 2914 6395</td>
<td>32777 I</td>
</tr>
</tbody>
</table>

...
AS path: 14203 2914 3320 5603 28682 I
domain 1, neighbor as: 14203, length 5, segments 1, references 2
AS path: 14203 2914 3491 1680 33802 I
domain 1, neighbor as: 14203, length 5, segments 1, references 2
AS path: 14203 2914 3549 7908 27658 I
domain 1, neighbor as: 14203, length 5, segments 1, references 2
AS path: 14203 2914 3549 20804 30730 I
domain 1, neighbor as: 14203, length 5, segments 1, references 2
AS path: 14203 2914 7018 2687 9226 I
domain 1, neighbor as: 14203, length 5, segments 1, references 2
AS path: 14203 2914 701 3786 3786 23564 I
domain 1, neighbor as: 14203, length 6, segments 1, references 2
AS path: 14203 2914 174 9318 9318 23564 I
domain 1, neighbor as: 14203, length 6, segments 1, references 3
AS path: 14203 2914 701 4761 4795 9228 I
domain 1, neighbor as: 14203, length 6, segments 1, references 14
AS path: 14203 2914 1239 7132 5673 18444 I
domain 1, neighbor as: 14203, length 6, segments 1, references 2
AS path: 14203 2914 3491 20485 24588 24588 I
domain 1, neighbor as: 14203, length 6, segments 1, references 4
AS path: 14203 2914 5511 2200 1945 2060 I
domain 1, neighbor as: 14203, length 6, segments 1, references 2
AS path: 14203 2914 7911 14325 14325 14348 I
domain 1, neighbor as: 14203, length 6, segments 1, references 2
AS path: 14203 2914 701 4637 9230 9230 9230 I
domain 1, neighbor as: 14203, length 7, segments 1, references 3
AS path: 14203 2914 6395 14 14 14 14 I
domain 1, neighbor as: 14203, length 7, segments 1, references 10
show as-path domain

Syntax

show as-path domain
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show as-path domain

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display autonomous system (AS) path domain information.

Options

none—(Optional) Display AS path domain information for all routing instances.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

Level view

List of Sample Output

show as-path domain on page 3142

Output Fields

Table 382 on page 3141 lists the output fields for the show as-path domain command. Output fields are listed in the approximate order in which they appear.

Table 382: show as-path domain Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Number of independent AS domains. The AS paths of an independent AS domain are not shared with the AS paths and AS path attributes of other domains, including the master routing instance domain.</td>
</tr>
<tr>
<td>Primary</td>
<td>Primary AS number.</td>
</tr>
<tr>
<td>References</td>
<td>Path reference count.</td>
</tr>
<tr>
<td>Number Paths</td>
<td>Number of known AS paths.</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the AS path:</td>
</tr>
<tr>
<td></td>
<td>• ASLoop—Path contains an AS loop.</td>
</tr>
<tr>
<td></td>
<td>• Atomic—Path includes the ATOMIC_AGGREGATE path attribute.</td>
</tr>
<tr>
<td></td>
<td>• Local—Path was created by local aggregation.</td>
</tr>
<tr>
<td></td>
<td>• Master—Path was created by the master routing instance.</td>
</tr>
<tr>
<td>Local AS</td>
<td>AS number of the local routing device.</td>
</tr>
<tr>
<td>Loops</td>
<td>How many times this AS number can appear in an AS path.</td>
</tr>
</tbody>
</table>
Sample Output

```
user@host> show as-path domain
Domain: 1       Primary: 10458
    References:      3       Paths:     30383
    Flags: Master
    Local AS: 10458   Loops: 1
```
show as-path summary

Syntax

show as-path summary
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show as-path summary

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display autonomous system (AS) path summary information.

AS paths are stored in a hash table. A hash table is one method for fast lookup. Each entry in the table is called a bucket. Junos OS computes a hash value that indicates in which bucket the AS path is stored. The AS paths are dispersed among the hash buckets so that a manageable number of AS paths is stored in each bucket. Only unique AS paths are stored. Duplicate AS paths increase a reference count, but do not increase the number of AS paths stored in the hash table.

Options

none—(Optional) Display AS path summary information for all routing instances.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

Related Documentation

• show as-path on page 3137

List of Sample Output

show as-path summary on page 3144

Output Fields

Table 383 on page 3143 lists the output fields for the show as-path summary command. Output fields are listed in the approximate order in which they appear.

Table 383: show as-path summary Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Paths</td>
<td>Number of AS paths.</td>
</tr>
<tr>
<td>Buckets</td>
<td>Number of hash buckets in use.</td>
</tr>
<tr>
<td>Max</td>
<td>Maximum number of AS path entries per bucket.</td>
</tr>
<tr>
<td>Min</td>
<td>Minimum number of AS path entries per bucket.</td>
</tr>
<tr>
<td>Avg</td>
<td>Average number of AS path entries per bucket.</td>
</tr>
<tr>
<td>Std deviation</td>
<td>Standard deviation of AS path entries per bucket.</td>
</tr>
</tbody>
</table>
## Sample Output

show as-path summary

```bash
classic@host> show as-path summary
AS Paths | Buckets | Max | Min | Avg | Std deviation
---------|--------|-----|-----|-----|------------------
30425    | 1024   | 95  | 12  | 29  | 6.481419
```

Copyright © 2013, Juniper Networks, Inc.
show ipv6 neighbors

Syntax

show ipv6 neighbors

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.3 for EX Series switches.
Command introduced in Junos OS Release 12.2 for the QFX Series.

Description

Display information about the IPv6 neighbor cache.

Options

This command has no options.

Required Privilege Level

view

Related Documentation

• clear ipv6 neighbors on page 3136

List of Sample Output

show ipv6 neighbors on page 3145

Output Fields

Table 384 on page 3145 describes the output fields for the show ipv6 neighbors command. Output fields are listed in the approximate order in which they appear.

Table 384: show ipv6 neighbors Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>Name of the IPv6 interface.</td>
</tr>
<tr>
<td>Linklayer Address</td>
<td>Link-layer address.</td>
</tr>
<tr>
<td>State</td>
<td>State of the link: up, down, incomplete, reachable, stale, or unreachable.</td>
</tr>
<tr>
<td>Exp</td>
<td>Number of seconds until the entry expires.</td>
</tr>
<tr>
<td>Rtr</td>
<td>Whether the neighbor is a routing device: yes or no.</td>
</tr>
<tr>
<td>Secure</td>
<td>Whether this entry was created using the Secure Neighbor Discovery (SEND) protocol: yes or no.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
</tbody>
</table>

Sample Output

show ipv6 neighbors

user@host> show ipv6 neighbors
IPv6 Address      Linklayer Address  State     Exp  Rtr  Secure
Interface
2001:db8:0:1:2a0:a514:0:24c  00:05:85:8f:c8:bd stale  546 yes no
fe-1/2/0.1

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>State</th>
<th>Age</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:a514:0:24c</td>
<td>00:05:85:8f:c8:bd</td>
<td>stale</td>
<td>258</td>
<td>yes</td>
</tr>
<tr>
<td>fe-1/2/0.1</td>
<td></td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>fe80::2a0:a514:0:64c</td>
<td>00:05:85:8f:c8:bd</td>
<td>stale</td>
<td>111</td>
<td>yes</td>
</tr>
<tr>
<td>fe-1/2/1.5</td>
<td></td>
<td></td>
<td></td>
<td>no</td>
</tr>
<tr>
<td>fe80::2a0:a514:0:a4c</td>
<td>00:05:85:8f:c8:bd</td>
<td>stale</td>
<td>327</td>
<td>yes</td>
</tr>
<tr>
<td>fe-1/2/2.9</td>
<td></td>
<td></td>
<td></td>
<td>no</td>
</tr>
</tbody>
</table>
show route

Syntax

show route
<all>
<destination-prefix>
logical-system (all | logical-system-name)>
<private>

Syntax (EX Series Switches)

show route
<all>
<destination-prefix>
<private>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option private introduced in Junos OS Release 9.5.
Option private introduced in Junos OS Release 9.5 for EX Series switches.

Description
Display the active entries in the routing tables.

Options

none—Display brief information about all active entries in the routing tables.

all—(Optional) Display information about all routing tables, including private, or internal, routing tables.

destination-prefix—(Optional) Display active entries for the specified address or range of addresses.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

private—(Optional) Display information only about all private, or internal, routing tables.

Required Privilege

Level view

Related Documentation

- Example: Configuring RIP
- Example: Configuring RIPng
- Example: Configuring IS-ISIS
- Examples: Configuring Internal BGP Peering
- Examples: Configuring External BGP Peering
- Examples: Configuring OSPF Routing Policy

List of Sample Output

show route on page 3150
show route on page 3150
show route destination-prefix on page 3151
show route extensive on page 3151
Output Fields  Table 385 on page 3148 describes the output fields for the \texttt{show route} command. Output fields are listed in the approximate order in which they appear.

Table 385: show route Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{routing-table-name}</td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td>\texttt{number destinations}</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td>\texttt{number routes}</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>\begin{itemize} \item active (routes that are active). \item holddown (routes that are in the pending state before being declared inactive). A holddown route was once the active route and is no longer the active route. The route is in the holddown state because a protocol still has interest in the route, meaning that the interest bit is set. A protocol might have its interest bit set on the previously active route because the protocol is still advertising the route. The route will be deleted after all protocols withdraw their advertisement of the route and remove their interest bit. A persistent holddown state often means that the interested protocol is not releasing its interest bit properly. However, if you have configured advertisement of multiple routes (with the \texttt{add-path} or \texttt{advertise-inactive} statement), the holddown bit is most likely set because BGP is advertising the route as an active route. In this case, you can ignore the holddown state because nothing is wrong. \item hidden (routes that are not used because of a routing policy). \end{itemize}</td>
</tr>
<tr>
<td>\texttt{destination-prefix}</td>
<td>Route destination (for example:10.0.0.1/24). Sometimes the route information is presented in another format, such as:</td>
</tr>
<tr>
<td></td>
<td>\begin{itemize} \item \texttt{MPLS-label} (for example, 80001). \item \texttt{interface-name} (for example, ge-1/0/2). \item \texttt{neighbor-address}:\texttt{control-word-status}:\texttt{encapsulation type}:\texttt{vc-id}:\texttt{source} (Layer 2 circuit only. For example, 10.1.1.195:NoCtrlWord:1:1:Local/96): \begin{itemize} \item \texttt{neighbor-address}—Address of the neighbor. \item \texttt{control-word-status}—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord. \item \texttt{encapsulation type}—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport. \item \texttt{vc-id}—Virtual circuit identifier. \item \texttt{source}—Source of the advertisement: Local or Remote. \end{itemize} \end{itemize}</td>
</tr>
<tr>
<td>\texttt{protocol, preference}</td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td>\begin{itemize} \item +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table. \item -—A hyphen indicates the last active route. \item *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route. \end{itemize}</td>
</tr>
</tbody>
</table>

In every routing metric except for the BGP \texttt{LocalPref} attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the \texttt{1}'s complement of the \texttt{LocalPref} value in the \texttt{Preference2} field. For example, if the \texttt{LocalPref} value for Route 1 is 100, the \texttt{Preference2} value is -101. If the \texttt{LocalPref} value for Route 2 is 155, the \texttt{Preference2} value is -156. Route 2 is preferred because it has a higher \texttt{LocalPref} value and a lower \texttt{Preference2} value.
### Table 385: show route Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>weeks:days hours:minutes:seconds</code></td>
<td>How long the route been known (for example, <code>2w4d13:11:14</code>, or 2 weeks, 4 days, 13 hours, 11 minutes, and 14 seconds).</td>
</tr>
<tr>
<td>metric</td>
<td>Cost value of the indicated route. For routes within an AS, the cost is determined by the IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.</td>
</tr>
<tr>
<td>localpref</td>
<td>Local preference value included in the route.</td>
</tr>
<tr>
<td>from</td>
<td>Interface from which the route was received.</td>
</tr>
</tbody>
</table>
| AS path               | AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:  
  - I—IGP.  
  - E—EGP.  
  - ?—Incomplete; typically, the AS path was aggregated.  
  When AS path numbers are included in the route, the format is as follows:  
    - `[ ]`—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured.  
    - `{ }`—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.  
    - `( )`—Parentheses enclose a confederation.  
    - `(()`—Parentheses and brackets enclose a confederation set.  
  **NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance. |
| validation-state      | (BGP-learned routes) Validation status of the route:  
  - **Invalid**—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database.  
  - **Unknown**—Indicates that the prefix is not among the prefixes or prefix ranges in the database.  
  - **Valid**—Indicates that the prefix and autonomous system pair are found in the database. |
| to                    | Next hop to the destination. An angle bracket (>) indicates that the route is the selected route. If the destination is **Discard**, traffic is dropped.                                                                 |
Table 385: show route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>via</td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word Selected. This field can also contain the following information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Weight</strong>—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Balance</strong>—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.</td>
</tr>
<tr>
<td></td>
<td>• <strong>lsp-path-name</strong>—Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td></td>
<td>• <strong>label-action</strong>—MPLS label and operation occurring at the next hop. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label). For VPNs, expect to see multiple push operations, corresponding to the inner and outer labels required for VPN routes (in the case of a direct PE-to-PE connection, the VPN route would have the inner label push only).</td>
</tr>
</tbody>
</table>

Sample Output

```
user@host> show route
inet.0: 11 destinations, 12 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1:65500:1:10.0.0.20/240
   *[MVPN/70] 19:53:41, metric2 1
      Indirect
1:65500:1:10.0.0.40/240
   *[BGP/170] 19:53:29, localpref 100, from 10.0.0.30
      AS path: I
         > to 10.0.24.4 via lt-0/3/0.24, label-switched-path toD
   *[BGP/170] 19:53:29, localpref 100, from 10.0.0.33
      AS path: I
         > to 10.0.24.4 via lt-0/3/0.24, label-switched-path toD

1:65500:1:10.0.0.60/240
   *[BGP/170] 19:53:29, localpref 100, from 10.0.0.30
      AS path: I
         > to 10.0.28.8 via lt-0/3/0.28, label-switched-path toD
   *[BGP/170] 19:53:25, localpref 100, from 10.0.0.33
      AS path: I
         > to 10.0.28.8 via lt-0/3/0.28, label-switched-path toD
```

show route

The following sample output shows a VPN route with composite next hops enabled. The first **Push** operation corresponds to the outer label. The second **Push** operation corresponds to the inner label.

```
user@host> show route 70.0.0.0

13979:665001.inet.0: 871 destinations, 3556 routes (871 active, 0 holddown, 0 hidden)
```
show route destination-prefix

user@host> show route 172.16.0.0/12
inet.0: 10 destinations, 10 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.0.0/12 *[Static/5] 2w4d 12:54:27
> to 192.168.167.254 via fxp0.0

show route extensive

user@host> show route extensive
v1.mvpn.0: 5 destinations, 8 routes (5 active, 1 holddown, 0 hidden)
1:65500:1:10.0.0.40/240 (1 entry, 1 announced)
*BGP Preference: 170/-101
PMSI: Flags 0x0: Label[0:0:0]: PIM-SM: Sender 10.0.0.40 Group 225.1.1.1

Next hop type: Indirect
Address: 0x92455b8
Next-hop reference count: 2
Source: 10.0.0.30
Protocol next hop: 10.0.0.40
Indirect next hop: 2 no-forward
State: <Active Int Ext>
Local AS: 65500 Peer AS: 65500
Age: 3 Metric2: 1
Task: BGP_65500.10.0.0.30+179
Announcement bits (2): 0-PIM.v1 1-mvpn global task
AS path: I (Originator) Cluster list: 10.0.0.30
AS path: Originator ID: 10.0.0.40
Communities: target:65520:100
Import Accepted
Localpref: 100
Router ID: 10.0.0.30
Primary Routing Table bgp.mvpn.0
Indirect next hops: 1
Protocol next hop: 10.0.0.40 Metric: 1
Indirect next hop: 2 no-forward
Indirect path forwarding next hops: 1
Next hop type: Router
Next hop: 10.0.24.4 via lt-0/3/0.24 weight 0x1
10.0.0.40/32 Originating RIB: inet.3
Metric: 1 Node path count: 1
Forwarding nexthops: 1
Nexthop: 10.0.24.4 via lt-0/3/0.24
**show route active-path**

**Syntax**

```
show route active-path
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**

```
show route active-path
<brief | detail | extensive | terse>
```

**Release Information**

Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display all active routes for destinations. An active route is a route that is selected as the best path.Inactive routes are not displayed.

**Options**

- `none`—Display all active routes.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to `brief`.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

`view`

**List of Sample Output**

- show route active-path on page 3152
- show route active-path brief on page 3153
- show route active-path detail on page 3153
- show route active-path extensive on page 3154
- show route active-path terse on page 3156

**Output Fields**

For information about output fields, see the output field tables for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

**Sample Output**

```
user@host> show route active-path

inet.0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.70.19/32   *[Direct/0] 21:33:52
   > via lo0.0
10.255.71.50/32   *[IS-IS/15] 00:18:13, metric 10
   > to 100.1.2.1 via so-2/1/3.0
100.1.2.0/24      *[Direct/0] 00:18:36
   > via so-2/1/3.0
100.1.2.2/32      *[Local/0] 00:18:41
   Local via so-2/1/3.0
192.168.64.0/21   *[Direct/0] 21:33:52
```
show route active-path brief

The output for the `show route active-path brief` command is identical to that for the `show route active-path` command. For sample output, see `show route active-path on page 3152`.

show route active-path detail

```
user@host> show route active-path detail

inet.0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)

10.255.70.19/32 (1 entry, 1 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 3
  Next hop: via lo0.0, selected
  State: <Active Int>
  Local AS: 200
  Age: 21:37:10
  Task: IF
  Announcement bits (3): 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3
  AS path: I

10.255.71.50/32 (1 entry, 1 announced)
  *IS-IS Preference: 15
  Level: 1
  Next hop type: Router, Next hop index: 397
  Next-hop reference count: 4
  Next hop: 100.1.2.1 via so-2/1/3.0, selected
  State: <Active Int>
  Local AS: 200
  Age: 21:31 Metric: 10
  Task: IS-IS
  Announcement bits (4): 0-KRT 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3
  AS path: I

100.1.2.0/24 (1 entry, 1 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 3
  Next hop: via so-2/1/3.0, selected
  State: <Active Int>
  Local AS: 200
  Age: 21:54
  Task: IF
  Announcement bits (3): 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3
  AS path: I

100.1.2.2/32 (1 entry, 1 announced)
  *Local Preference: 0
  Next hop type: Local
  Next-hop reference count: 11
  Interface: so-2/1/3.0
  State: <Active NoReadvrt Int>
```
Local AS: 200
Age: 21:59
Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I

192.168.64.0/21 (1 entry, 1 announced)
*Direct Preference: 0
Next hop type: Interface
Next-hop reference count: 3
Next hop: via fxp0.0, selected
State: <Active Int>
Local AS: 200
Age: 21:37:10
Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I

192.168.70.19/32 (1 entry, 1 announced)
*Local Preference: 0
Next hop type: Local
Next-hop reference count: 11
Interface: fxp0.0
State: <Active NoReadvrt Int>
Local AS: 200
Age: 21:37:10
Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I

show route active-path extensive

user@host> show route active-path extensive

inet.0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)
10.255.70.19/32 (1 entry, 1 announced)
TSI:
IS-IS level 1, LSP fragment 0
IS-IS level 2, LSP fragment 0
*Direct Preference: 0
Next hop type: Interface
Next-hop reference count: 3
Next hop: via lo0.0, selected
State: <Active Int>
Local AS: 200
Age: 21:39:47
Task: IF
Announcement bits (3): 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3
AS path: I

10.255.71.50/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.255.71.50/32 -> {100.1.2.1}
IS-IS level 2, LSP fragment 0
*IS-IS Preference: 15
Level: 1
Next hop type: Router, Next hop index: 397
Next-hop reference count: 4
Next hop: 100.1.2.1 via so-2/1/3.0, selected
State: <Active Int>
Local AS: 200
Age: 24:08 Metric: 10
Task: IS-IS
Announcement bits (4): 0-KRT 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3
AS path: I

100.1.2.0/24 (1 entry, 1 announced)
TSI:
IS-IS level 1, LSP fragment 0
IS-IS level 2, LSP fragment 0
*Direct Preference: 0
Next hop type: Interface
Next-hop reference count: 3
Next hop: via so-2/1/3.0, selected
State: <Active Int>
Local AS: 200
Age: 24:31
Task: IF
Announcement bits (3): 2-IS-IS 5-Resolve tree 2 6-Resolve tree 3
AS path: I

100.1.2.2/32 (1 entry, 1 announced)
*Local Preference: 0
Next hop type: Local
Next-hop reference count: 11
Interface: so-2/1/3.0
State: <Active NoReadvrt Int>
Local AS: 200
Age: 24:36
Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I

192.168.64.0/21 (1 entry, 1 announced)
*Direct Preference: 0
Next hop type: Interface
Next-hop reference count: 3
Next hop: via fxp0.0, selected
State: <Active Int>
Local AS: 200
Age: 21:39:47
Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I

192.168.70.19/32 (1 entry, 1 announced)
*Local Preference: 0
Next hop type: Local
Next-hop reference count: 11
Interface: fxp0.0
State: <Active NoReadvrt Int>
Local AS: 200
Age: 21:39:47
Task: IF
Announcement bits (2): 5-Resolve tree 2 6-Resolve tree 3
AS path: I
show route active-path terse

user@host> show route active-path terse

inet.0: 7 destinations, 7 routes (6 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.255.70.19/32</td>
<td>D</td>
<td>0</td>
<td></td>
<td>&gt;lo0.0</td>
<td></td>
</tr>
<tr>
<td>* 10.255.71.50/32</td>
<td>I</td>
<td>15</td>
<td>10</td>
<td>&gt;100.1.2.1</td>
<td></td>
</tr>
<tr>
<td>* 100.1.2.0/24</td>
<td>D</td>
<td>0</td>
<td></td>
<td>&gt;so-2/1/3.0</td>
<td></td>
</tr>
<tr>
<td>* 100.1.2.2/32</td>
<td>L</td>
<td>0</td>
<td></td>
<td>Local</td>
<td></td>
</tr>
<tr>
<td>* 192.168.64.0/21</td>
<td>D</td>
<td>0</td>
<td></td>
<td>&gt;fxp0.0</td>
<td></td>
</tr>
<tr>
<td>* 192.168.70.19/32</td>
<td>L</td>
<td>0</td>
<td></td>
<td>Local</td>
<td></td>
</tr>
</tbody>
</table>
show route all

Syntax

show route all
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show route all

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display information about all routes in all routing tables, including private, or internal, tables.

Options

none—Display information about all routes in all routing tables, including private, or internal, tables.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

List of Sample Output

show route all on page 3157

Output Fields

In Junos OS Release 9.5 and later, only the output fields for the show route all command display all routing tables, including private, or hidden, routing tables. The output field table of the show route command does not display entries for private, or hidden, routing tables in Junos OS Release 9.5 and later.

Sample Output

The following example displays a snippet of output from the show route command and then displays the same snippet of output from the show route all command:

user@host> show route
mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
0 *[MPLS/0] 2d 02:24:39, metric 1
  Receive
1 *[MPLS/0] 2d 02:24:39, metric 1
  Receive
2 *[MPLS/0] 2d 02:24:39, metric 1
  Receive
800017 *[VPLS/7] 1d 14:00:16
  > via vt-3/2/0.32769, Pop
800018 *[VPLS/7] 1d 14:00:26
  > via vt-3/2/0.32772, Pop

user@host> show route all
mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete
<table>
<thead>
<tr>
<th>Route</th>
<th>Interface</th>
<th>Type</th>
<th>Age</th>
<th>Metric</th>
<th>Active Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>[MPLS/0]</td>
<td>2d</td>
<td>02:19:12</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>1</td>
<td>[MPLS/0]</td>
<td>2d</td>
<td>02:19:12</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>2</td>
<td>[MPLS/0]</td>
<td>2d</td>
<td>02:19:12</td>
<td>1</td>
<td>*</td>
</tr>
<tr>
<td>800017</td>
<td>[VPLS/7]</td>
<td>1d</td>
<td>13:54:49</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>800018</td>
<td>[VPLS/7]</td>
<td>1d</td>
<td>13:54:59</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>vt-3/2/0.32769</td>
<td>[VPLS/7]</td>
<td>1d</td>
<td>13:54:49</td>
<td></td>
<td>Unusable</td>
</tr>
<tr>
<td>vt-3/2/0.32772</td>
<td>[VPLS/7]</td>
<td>1d</td>
<td>13:54:59</td>
<td></td>
<td>Unusable</td>
</tr>
</tbody>
</table>

* = Both
+ = Active Route, - = Last Active

Copyright © 2013, Juniper Networks, Inc.
### show route aspath-regex

| Syntax | show route aspath-regex regular-expression <logical-system (all | logical-system-name)> |
|--------|-----------------------------------------------------------------------------------|
| Syntax (EX Series Switches) | show route aspath-regex regular-expression |

**Release Information**
Command introduced before Junos OS Release 7.4. 
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display the entries in the routing table that match the specified autonomous system (AS) path regular expression.

**Options**
- **regular-expression**—Regular expression that matches an entire AS path. 
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**
You can specify a regular expression as:

- An individual AS number
- A period wildcard used in place of an AS number
- An AS path regular expression that is enclosed in parentheses

You also can include the operators described in the table of AS path regular expression operators in the *Junos Policy Framework Configuration Guide*. The following list summarizes these operators:

- **{m,n}**—At least $m$ and at most $n$ repetitions of the AS path term.
- **{m}**—Exactly $m$ repetitions of the AS path term.
- **{m,}**—$m$ or more repetitions of the AS path term.
- **\*\**—Zero or more repetitions of an AS path term.
- **\+\**—One or more repetitions of an AS path term.
- **?\**—Zero or one repetition of an AS path term.
- **aspath_term | aspath_term**—Match one of the two AS path terms.

When you specify more than one AS number or path term, or when you include an operator in the regular expression, enclose the entire regular expression in quotation marks. For example, to match any path that contains AS number 234, specify the following command:

```
show route aspath-regex ".*234.*"
```

**Required Privilege**
- **view**

---

Copyright © 2013, Juniper Networks, Inc.
Related Documentation

Example: Using AS Path Regular Expressions

List of Sample Output

show route aspath-regex (Matching a Specific AS Number) on page 3160
show route aspath-regex (Matching Any Path with Two AS Numbers) on page 3160

Output Fields

For information about output fields, see the output field table for the show route command.

Sample Output

show route aspath-regex (Matching a Specific AS Number)

```
user@host> show route aspath-regex 65477
inet.0: 46411 destinations, 46411 routes (46409 active, 0 holddown, 2 hidden)
+ = Active Route, - = Last Active, * = Both

111.222.1.0/25   *[BGP/170] 00:08:48, localpref 100, from 111.222.2.24
    AS Path: [65477] ({65488 65535}) IGP
    to 111.222.18.225 via fpa0.0(111.222.18.233)

111.222.1.128/25  *[IS-IS/15] 09:15:37, metric 37, tag 1
  to 111.222.18.225 via fpa0.0(111.222.18.233)
    [BGP/170] 00:08:48, localpref 100, from 111.222.2.24
    AS Path: [65477] ({65488 65535}) IGP
    to 111.222.18.225 via fpa0.0(111.222.18.233)

...
```

show route aspath-regex (Matching Any Path with Two AS Numbers)

```
user@host> show route aspath-regex ?.*2343561.*?
inet.0: 46351 destinations, 46351 routes (46349 active, 0 holddown, 2 hidden)
+ = Active Route, - = Last Active, * = Both

9.20.0.0/17     *[BGP/170] 01:35:00, localpref 100, from 131.103.20.49
    AS Path: [666] 234 3561 2685 2686 Incomplete
    to 192.156.169.1 via 192.156.169.14(so-0/0/0)

12.10.231.0/24  *[BGP/170] 01:35:00, localpref 100, from 131.103.20.49
    AS Path: [666] 234 3561 5696 7369 IGP
    to 192.156.169.1 via 192.156.169.14(so-0/0/0)

24.64.32.0/19   *[BGP/170] 01:34:59, localpref 100, from 131.103.20.49
    AS Path: [666] 234 3561 6327 IGP
    to 192.156.169.1 via 192.156.169.14(so-0/0/0)

...
```
show route best

Syntax

show route best destination-prefix
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show route best destination-prefix
<brief | detail | extensive | terse>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the route in the routing table that is the best route to the specified address or range of addresses. The best route is the longest matching route.

Options

brief | detail | extensive | terse—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.

destination-prefix—Address or range of addresses.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

List of Sample Output

show route best on page 3161
show route best detail on page 3162
show route best extensive on page 3163
show route best terse on page 3163

Output Fields

For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output

show route best

user@host> show route best 10.255.70.103
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.255.70.103/32 *[OSPF/10] 1d 13:19:20, metric 2
> to 10.31.1.6 via ge-3/1/0.0
via so-0/3/0.0

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.255.70.103/32 *[RSVP/7] 1d 13:20:13, metric 2
> via so-0/3/0.0, label-switched-path green-r1-r3

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
show route best detail

user@host> show route best 10.255.70.103 detail
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
      Restart Complete
      10.255.70.103/32 (1 entry, 1 announced)
            *OSPF   Preference: 10
            Next-hop reference count: 9
            Next hop: 10.31.1.6 via ge-3/1/0.0, selected
            Next hop: via so-0/3/0.0
            State: <Active Int>
            Local AS:    69
            Age: 1d 13:20:06        Metric: 2
            Area: 0.0.0.0
            Task: OSPF
            Announcement bits (2): 0-KRT 3-Resolve tree 2
            AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
      Restart Complete
      10.255.70.103/32 (1 entry, 1 announced)
            *RSVP   Preference: 7
            Next-hop reference count: 5
            Next hop: via so-0/3/0.0 weight 0x1, selected
            Label-switched-path green-r1-r3
            Label operation: Push 100016
            State: <Active Int>
            Local AS:    69
            Age: 1d 13:20:59        Metric: 2
            Task: RSVP
            Announcement bits (1): 1-Resolve tree 2
            AS path: I

private1__inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
      10.0.0.0/8 (2 entries, 0 announced)
            *Direct Preference: 0
            Next hop type: Interface
            Next-hop reference count: 1
            Next hop: via fxp2.0, selected
            State: <Active Int>
            Age: 2d 1:44:20
            Task: IF
            AS path: I

Direct Preference: 0
      Next hop type: Interface
      Next-hop reference count: 1
      Next hop: via fxp1.0, selected
      State: <NotBest Int>
      Inactive reason: No difference
      Age: 2d 1:44:20
      Task: IF
      AS path: I
show route best extensive

The output for the show route best extensive command is identical to that for the show route best detail command. For sample output, see show route best detail on page 3162.

show route best terse

user@host> show route best 10.255.70.103 terse
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
* 10.255.70.103/32   O  10          2            >10.31.1.6
so-0/3/0.0

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
* 10.255.70.103/32   R   7          2            >so-0/3/0.0

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
* 10.0.0.0/8         D   0                       >fxp2.0
* 10.0.0.0/8         D   0                       >fxp1.0
show route brief

Syntax
show route brief
<destination-prefix>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)
show route brief
<destination-prefix>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display brief information about the active entries in the routing tables.

Options
none—Display all active entries in the routing table.

destination-prefix—(Optional) Display active entries for the specified address or range of addresses.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

List of Sample Output
show route brief on page 3164

Output Fields
For information about output fields, see the Output Field table of the show route command.

Sample Output

user@host> show route brief
inet.0: 10 destinations, 10 routes (9 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0 *[Static/5] 1w5d 20:30:29
  Discard
10.255.245.51/32 *[Direct/0] 2w4d 13:11:14
  > via lo0.0
172.16.0.0/12 *[Static/5] 2w4d 13:11:14
  > to 192.168.167.254 via fxp0.0
192.168.0.0/18 *[Static/5] 1w5d 20:30:29
  > to 192.168.167.254 via fxp0.0
192.168.40.0/22 *[Static/5] 2w4d 13:11:14
  > to 192.168.167.254 via fxp0.0
192.168.64.0/18 *[Static/5] 2w4d 13:11:14
  > to 192.168.167.254 via fxp0.0
192.168.164.0/22 *[Direct/0] 2w4d 13:11:14
  > via fxp0.0
192.168.164.51/32 *[Local/0] 2w4d 13:11:14
  Local via fxp0.0
207.17.136.192/32 *[Static/5] 2w4d 13:11:14
green.inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
100.101.0.0/16   *[Direct/0] 1w5d 20:30:28
   > via fe-0/0/3.0
100.101.2.3/32   *[Local/0] 1w5d 20:30:28
   Local via fe-0/0/3.0
224.0.0.5/32     *[OSPF/10] 1w5d 20:30:29, metric 1
   MultiRecv
**show route community**

**Syntax**
```
show route community as-number:community-value
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route community as-number:community-value
<brief | detail | extensive | terse>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display the route entries in each routing table that are members of a Border Gateway Protocol (BGP) community.

**Options**
- **as-number:community-value**—One or more community identifiers. **as-number** is the AS number, and **community-value** is the community identifier. When you specify more than one community identifier, enclose the identifiers in double quotation marks. Community identifiers can include wildcards.
- **brief | detail | extensive | terse**—(Optional) Display the specified level of output.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**
Specifying the community option displays all routes matching the community found within the routing table. The community option does not limit the output to only the routes being advertised to the neighbor after any egress routing policy.

**Required Privilege**
view

**Related Documentation**
- show route detail on page 3175
- show route community on page 3166

**List of Sample Output**
show route community on page 3166

**Output Fields**
For information about output fields, see the output field tables for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

**Sample Output**

```
user@host> show route community 234:80
inet.0: 46511 destinations, 46511 routes (46509 active, 0 holddown, 2 hidden)
+ = Active Route, - = Last Active, * = Both

4.0.0.0/8     *[BGP/170] 03:33:07, localpref 100, from 131.103.20.49
  AS Path: (666) 234 2548 1 IGP
to 192.156.169.1 via 192.156.169.14(so-0/0/0)
6.0.0.0/8     *[BGP/170] 03:33:07, localpref 100, from 131.103.20.49
```
AS Path: {666} 234 2548 568 721 Incomplete to 192.156.169.1 via 192.156.169.14 (so-0/0/0)

9.2.0.0/16

*[BGP/170] 03:33:06, localpref 100, from 131.103.20.49
AS Path: {666} 234 2548 1673 1675 1747 IGP
to 192.156.169.1 via 192.156.169.14 (so-0/0/0)
show route community-name

Syntax
show route community-name community-name
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)
show route community-name community-name
  <brief | detail | extensive | terse>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display the route entries in each routing table that are members of a Border Gateway Protocol (BGP) community, specified by a community name.

Options
community-name—Name of the community.
brief | detail | extensive | terse—(Optional) Display the specified level of output.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

List of Sample Output
show route community-name on page 3168

Output Fields
For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output
show route community-name

user@host> show route community-name red-com
inet.0: 17 destinations, 17 routes (16 active, 0 holddown, 1 hidden)
  inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  instance1.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
  red.inet.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

  10.255.245.212/32  *[BGP/170] 00:04:40, localpref 100, from 10.255.245.204
  AS path: 300 I
    > to 100.1.2.2 via ge-1/1/0.0, label-switched-path to_fix
  20.20.20.20/32  *[BGP/170] 00:04:40, localpref 100, from 10.255.245.204
  AS path: I
    > to 100.1.2.2 via ge-1/1/0.0, label-switched-path to_fix
  100.1.4.0/24  *[BGP/170] 00:04:40, localpref 100, from 10.255.245.204
  AS path: I
    > to 100.1.2.2 via ge-1/1/0.0, label-switched-path to_fix
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

bgp.l3vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.245.204:10:10.255.245.212/32
* [BGP/170] 00:06:40, localpref 100, from 10.255.245.204
  AS path: 300 I
  > to 100.1.2.2 via ge-1/1/0.0, label-switched-path to_fix

10.255.245.204:10:20.20.20.20/32
* [BGP/170] 00:36:02, localpref 100, from 10.255.245.204
  AS path: I
  > to 100.1.2.2 via ge-1/1/0.0, label-switched-path to_fix

10.255.245.204:10:100.1.4.0/24
* [BGP/170] 00:36:02, localpref 100, from 10.255.245.204
  AS path: I
  > to 100.1.2.2 via ge-1/1/0.0, label-switched-path to_fix

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

instance1.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
show route damping

**Syntax**

```
show route damping (decayed | history | suppressed)
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and QFX Series)**

```
show route damping (decayed | history | suppressed)
<brief | detail | extensive | terse>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display the BGP routes for which updates might have been reduced because of route flap damping.

**Options**

- **brief | detail | extensive | terse**—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.
  - **decayed**—Display route damping entries that might no longer be valid, but are not suppressed.
  - **history**—Display entries that have already been withdrawn, but have been logged.
  - **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
  - **suppressed**—Display entries that have been suppressed and are no longer being installed into the forwarding table or exported by routing protocols.

**Required Privilege**

- **view**

**Related Documentation**

- clear bgp damping on page 2652
- show policy damping on page 2685

**List of Sample Output**

- show route damping decayed detail on page 3173
- show route damping history on page 3174
- show route damping history detail on page 3174

**Output Fields**

Table 386 on page 3170 lists the output fields for the `show route damping` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table—for example, inet.0.</td>
<td>All levels</td>
</tr>
<tr>
<td>destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 386: show route damping Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• holdown (routes that are in a pending state before being declared inactive)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hidden (the routes are not used because of a routing policy)</td>
<td></td>
</tr>
<tr>
<td>destination-prefix</td>
<td>Destination prefix. The <strong>entry</strong> value is the number of routes for this destination, and the <strong>announced</strong> value is the number of routes being announced for this destination.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>(entry, announced)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[protocol, preference]</td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• −—A hyphen indicates the last active route.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In every routing metric except for the BGP LocalPref attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the LocalPref value in the Preference2 field. For example, if the LocalPref value for Route 1 is 100, the Preference2 value is -101. If the LocalPref value for Route 2 is 155, the Preference2 value is -156. Route 2 is preferred because it has a higher LocalPref value and a lower Preference2 value.</td>
<td></td>
</tr>
<tr>
<td>Next-hop reference count</td>
<td>Number of references made to the next hop.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>Source</td>
<td>IP address of the route source.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>Next hop</td>
<td>Network layer address of the directly reachable neighboring system.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>via</td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word Selected.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>Protocol next hop</td>
<td>Network layer address of the remote routing device that advertised the prefix.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>This address is used to derive a forwarding next hop.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indirect next hop</td>
<td>Index designation used to specify the mapping between protocol next hops, tags, kernel export policy, and the forwarding next hops.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>State</td>
<td>Flags for this route. For a description of possible values for this field, see the output field table for the <code>show route detail</code> command.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>Local AS</td>
<td>AS number of the local routing device.</td>
<td>Detail extensive</td>
</tr>
<tr>
<td>Peer AS</td>
<td>AS number of the peer routing device.</td>
<td>Detail extensive</td>
</tr>
</tbody>
</table>
### Table 386: show route damping Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Age</strong></td>
<td>How long the route has been known.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Metric for the route.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Task</strong></td>
<td>Name of the protocol that has added the route.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Announcement bits</strong></td>
<td>List of protocols that announce this route. <strong>n-Resolve inet</strong> indicates that the route is used for route resolution for next hops found in the routing table. <strong>n</strong> is an index used by Juniper Networks customer support only.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
| **AS path** | AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:  
- I—IGP.  
- E—EGP.  
- ?—Incomplete; typically, the AS path was aggregated.  
When AS path numbers are included in the route, the format is as follows:  
- [ ]—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device or if AS path prepending is configured.  
- { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.  
- ()—Parentheses enclose a confederation.  
- ([ ])—Parentheses and brackets enclose a confederation set.  
**NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance. | All levels |
| **to**      | Next hop to the destination. An angle bracket (>) indicates that the route is the selected route. | brief none |
| **via**     | Interface used to reach the next hop. If there is more than one interface available to the next hop, the interface that is actually used is followed by the word Selected. | brief none |
| **Communities** | Community path attribute for the route. See the output field table for the show route detail command. | detail extensive |
| **Localpref** | Local preference value included in the route.                                      | All levels |
| **Router ID** | BGP router ID as advertised by the neighbor in the open message.                   | detail extensive |
| **Merit (last update/now)** | Last updated and current figure-of-merit value. | detail extensive |
Table 386: show route damping Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>damping-parameters</td>
<td>Name that identifies the damping parameters used, which is defined in the</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>damping statement at the [edit policy-options] hierarchy level.</td>
<td></td>
</tr>
<tr>
<td>Last update</td>
<td>Time of most recent change in path attributes.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>First update</td>
<td>Time of first change in path attributes, which started the route damping process.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Flaps</td>
<td>Number of times the route has gone up or down or its path attributes have</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>changed.</td>
<td></td>
</tr>
<tr>
<td>Suppressed</td>
<td>(suppressed keyword only) This route is currently suppressed. A suppressed</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>route does not appear in the forwarding table and routing protocols do not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>export it.</td>
<td></td>
</tr>
<tr>
<td>Reusable in</td>
<td>(suppressed keyword only) Time when a suppressed route will again be available.</td>
<td>All levels</td>
</tr>
<tr>
<td>Preference will be</td>
<td>(suppressed keyword only) Preference value that will be applied to the route</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>when it is again active.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show route damping decayed detail

user@host> show route damping decayed detail
inet.0: 173319 destinations, 1533668 routes (172625 active, 4 holddown, 108083 hidden)
10.0.111.0/24 (7 entries, 1 announced)
*BGP    Preference: 170/-101
Next-hop reference count: 151973
Source: 172.23.2.129
Next hop: via so-1/2/0.0
Next hop: via so-5/1/0.0, selected
Next hop: via so-6/0/0.0
Protocol next hop: 172.23.2.129
Indirect next hop: 89a1a00 264185
State: <Active Ext>
Local AS: 65000 Peer AS:   65490
Age: 3:28       Metric2: 0
Task: BGP_65490.172.23.2.129+179
Announcement bits (6): 0-KRT 1-RT 4-KRT 5-BGP.0.0.0.0+179
6-Resolve tree 2 7-Resolve tree 3
AS path: 65490 65520 65525 65525 65525 65525 1 ()
Localpref: 100
Router ID: 172.23.2.129
Merit (last update/now): 1934/1790
damping-parameters: damping-high
Last update:       00:03:28 First update:       00:06:40
Flaps: 2
show route damping history

user@host> show route damping history
inet.0: 173320 destinations, 1533529 routes (172624 active, 6 holddown, 108122 hidden)
+ = Active Route, - = Last Active, * = Both

10.108.0.0/15       [BGP ] 2d 22:47:58, localpref 100
                      AS path: 65220 65501 65502 I
                      > to 192.168.60.85 via so-3/1/0.0

show route damping history detail

user@host> show route damping history detail
inet.0: 173319 destinations, 1533435 routes (172627 active, 2 holddown, 108105 hidden)

10.108.0.0/15 (3 entries, 1 announced)
                      BGP
                      /-101
                      Next-hop reference count: 69058
                      Source: 192.168.60.85
                      Next hop: 192.168.60.85 via so-3/1/0.0, selected
                      State: <Hidden Ext>
                      Inactive reason: Unusable path
                      Local AS: 65000 Peer AS: 65220
                      Age: 2d 22:48:10
                      Task: BGP_65220.192.168.60.85+179
                      AS path: 65220 65501 65502 I ()
                      Communities: 65501:390 65501:2000 65501:3000 65504:3561
                      Localpref: 100
                      Router ID: 192.168.80.25
                      Merit (last update/now): 1000/932
                      damping-parameters: set-normal
                      Last update: 00:01:05 First update: 00:01:05
                      Flaps: 1
show route detail

Syntax
show route detail
<destination-prefix>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)
show route detail
<destination-prefix>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display detailed information about the active entries in the routing tables.

Options
none—Display all active entries in the routing table on all systems.

<destination-prefix>—(Optional) Display active entries for the specified address or range of addresses.

<logical-system (all | logical-system-name)>—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

List of Sample Output
- show route detail on page 3183
- show route detail (with BGP Multipath) on page 3189
- show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 3189

Output Fields
Table 387 on page 3175 describes the output fields for the show route detail command. Output fields are listed in the approximate order in which they appear.

Table 387: show route detail Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>• active (routes that are active)</td>
</tr>
<tr>
<td></td>
<td>• holdown (routes that are in the pending state before being declared inactive)</td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy)</td>
</tr>
</tbody>
</table>
Table 387: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>route-destination</strong></td>
<td>Route destination (for example:10.0.0.1/24). The entry value is the number of routes for this destination, and the announced value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:</td>
</tr>
<tr>
<td></td>
<td>• <strong>MPLS-label</strong> (for example, 80001).</td>
</tr>
<tr>
<td></td>
<td>• <strong>interface-name</strong> (for example, ge-1/0/2).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address:control-word-status:encapsulation type:vc-id:source</strong> (Layer 2 circuit only; for example, 10.1.1.195:NoCtrlWord:1:1:Local/96).</td>
</tr>
<tr>
<td></td>
<td>- <strong>neighbor-address</strong>—Address of the neighbor.</td>
</tr>
<tr>
<td></td>
<td>- <strong>control-word-status</strong>—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord.</td>
</tr>
<tr>
<td></td>
<td>- <strong>encapsulation type</strong>—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.</td>
</tr>
<tr>
<td></td>
<td>- <strong>vc-id</strong>—Virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td>- <strong>source</strong>—Source of the advertisement: Local or Remote.</td>
</tr>
<tr>
<td><strong>label stacking</strong></td>
<td>(Next-to-the-last-hop routing device for MPLS only) Depth of the MPLS label stack, where the label-popping operation is needed to remove one or more labels from the top of the stack. A pair of routes is displayed, because the pop operation is performed only when the stack depth is two or more labels.</td>
</tr>
<tr>
<td></td>
<td>• S=0 route indicates that a packet with an incoming label stack depth of 2 or more exits this routing device with one fewer label (the label-popping operation is performed).</td>
</tr>
<tr>
<td></td>
<td>• If there is no S= information, the route is a normal MPLS route, which has a stack depth of 1 (the label-popping operation is not performed).</td>
</tr>
<tr>
<td><strong>[protocol, preference]</strong></td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td>- +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>- -—A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>- *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route.</td>
</tr>
<tr>
<td></td>
<td>In every routing metric except for the BGP LocalPref attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the LocalPref value in the Preference2 field. For example, if the LocalPref value for Route 1 is 100, the Preference2 value is -101.</td>
</tr>
<tr>
<td></td>
<td>If the LocalPref value for Route 2 is 155, the Preference2 value is -156. Route 2 is preferred because it has a higher LocalPref value and a lower Preference2 value.</td>
</tr>
<tr>
<td><strong>Level</strong></td>
<td>(IS-IS only). In IS-IS, a single AS can be divided into smaller groups called areas. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area. When the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs.</td>
</tr>
<tr>
<td><strong>Route Distinguisher</strong></td>
<td>IP subnet augmented with a 64-bit prefix.</td>
</tr>
<tr>
<td><strong>Next-hop type</strong></td>
<td>Type of next hop. For a description of possible values for this field, see Table 388 on page 3179.</td>
</tr>
</tbody>
</table>
Table 387: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next-hop reference count</strong></td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td><strong>Flood nexthop branches exceed maximum message</strong></td>
<td>Indicates that the number of flood next-hop branches exceeded the system limit of 32 branches, and only a subset of the flood next-hop branches were installed in the kernel.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>IP address of the route source.</td>
</tr>
<tr>
<td><strong>Next hop</strong></td>
<td>Network layer address of the directly reachable neighboring system.</td>
</tr>
<tr>
<td><strong>via</strong></td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word <strong>Selected</strong>. This field can also contain the following information:</td>
</tr>
<tr>
<td></td>
<td>• Weight—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.</td>
</tr>
<tr>
<td></td>
<td>• Balance—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.</td>
</tr>
<tr>
<td><strong>Label-switched-path lsp-path-name</strong></td>
<td>Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td><strong>Label operation</strong></td>
<td>MPLS label and operation occurring at this routing device. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label).</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>(Local only) Local interface name.</td>
</tr>
<tr>
<td><strong>Protocol next hop</strong></td>
<td>Network layer address of the remote routing device that advertised the prefix. This address is used to derive a forwarding next hop.</td>
</tr>
<tr>
<td><strong>Indirect next hop</strong></td>
<td>Index designation used to specify the mapping between protocol next hops, tags, kernel export policy, and the forwarding next hops.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>State of the route (a route can be in more than one state). See Table 389 on page 3181.</td>
</tr>
<tr>
<td><strong>Local AS</strong></td>
<td>AS number of the local routing device.</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>How long the route has been known.</td>
</tr>
<tr>
<td><strong>AIGP</strong></td>
<td>Accumulated interior gateway protocol (AIGP) BGP attribute.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Cost value of the indicated route. For routes within an AS, the cost is determined by IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.</td>
</tr>
</tbody>
</table>
### Table 387: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MED-plus-IGP</td>
<td>Metric value for BGP path selection to which the IGP cost to the next-hop destination has been added.</td>
</tr>
<tr>
<td>TTL-Action</td>
<td>For MPLS LSPs, state of the TTL propagation attribute. Can be enabled or disabled for all RSVP-signaled and LDP-signaled LSPs or for specific VRF routing instances. For sample output, see show route table.</td>
</tr>
<tr>
<td>Task</td>
<td>Name of the protocol that has added the route.</td>
</tr>
<tr>
<td>Announcement bits</td>
<td>List of protocols that announce this route. (n)-Resolve inet indicates that the route is used for route resolution for next hops found in the routing table. (n) is an index used by Juniper Networks customer support only.</td>
</tr>
</tbody>
</table>
| AS path          | AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:  

- I—IGP.
- E—EGP.
- Recorded—The AS path is recorded by the sample process (sampled).
- ?—Incomplete; typically, the AS path was aggregated.

When AS path numbers are included in the route, the format is as follows:

- []—Brackets enclose the number that precedes the AS path. This number represents the number of ASs present in the AS path, when calculated as defined in RFC 4271. This value is used in the AS-path merge process, as defined in RFC 4893.
- []—If more than one AS number is configured on the routing device, or if AS path prepending is configured, brackets enclose the local AS number associated with the AS path.
- {}—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.
- ()—Parentheses enclose a confederation.
- ([ ])—Parentheses and brackets enclose a confederation set.

**NOTE:** In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.

<table>
<thead>
<tr>
<th>FECs bound to route</th>
<th>Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC Label</td>
<td>MPLS label assigned to the Layer 2 circuit virtual connection.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) of the Layer 2 circuit.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN identifier of the Layer 2 circuit.</td>
</tr>
<tr>
<td>Prefixes bound to route</td>
<td>Forwarding equivalent class (FEC) bound to this route. Applicable only to routes installed by LDP.</td>
</tr>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See Table 390 on page 3183 for all possible values for this field.</td>
</tr>
</tbody>
</table>
Table 387: show route detail Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2-info: encaps</td>
<td>Layer 2 encapsulation (for example, VPLS).</td>
</tr>
<tr>
<td>control flags</td>
<td>Control flags: none or Site Down.</td>
</tr>
<tr>
<td>mtu</td>
<td>Maximum transmission unit (MTU) information.</td>
</tr>
<tr>
<td>Label-Base, range</td>
<td>First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.</td>
</tr>
<tr>
<td>status vector</td>
<td>Layer 2 VPN and VPLS network layer reachability information (NLRI).</td>
</tr>
<tr>
<td>Accepted Multipath</td>
<td>Current active path when BGP multipath is configured.</td>
</tr>
<tr>
<td>Accepted MultipathContrib</td>
<td>Path currently contributing to BGP multipath.</td>
</tr>
<tr>
<td>Localpref</td>
<td>Local preference value included in the route.</td>
</tr>
<tr>
<td>Router ID</td>
<td>BGP router ID as advertised by the neighbor in the open message.</td>
</tr>
<tr>
<td>Primary Routing Table</td>
<td>In a routing table group, the name of the primary routing table in which the route resides.</td>
</tr>
<tr>
<td>Secondary Tables</td>
<td>In a routing table group, the name of one or more secondary tables in which the route resides.</td>
</tr>
</tbody>
</table>

Table 388 on page 3179 describes all possible values for the Next-hop Types output field.

Table 388: Next-hop Types Output Field Values

<table>
<thead>
<tr>
<th>Next-Hop Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast (bcast)</td>
<td>Broadcast next hop.</td>
</tr>
<tr>
<td>Deny</td>
<td>Deny next hop.</td>
</tr>
<tr>
<td>Discard</td>
<td>Discard next hop.</td>
</tr>
<tr>
<td>Flood</td>
<td>Flood next hop. Consists of components called branches, up to a maximum of 32 branches. Each flood next-hop branch sends a copy of the traffic to the forwarding interface. Used by point-to-multipoint RSVP, point-to-multipoint LDP, point-to-multipoint CCC, and multicast.</td>
</tr>
<tr>
<td>Hold</td>
<td>Next hop is waiting to be resolved into a unicast or multicast type.</td>
</tr>
<tr>
<td>Indexed (idxd)</td>
<td>Indexed next hop.</td>
</tr>
<tr>
<td>Next-Hop Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indirect (indr)</td>
<td>Used with applications that have a protocol next hop address that is remote. You are likely to see this next-hop type for internal BGP (iBGP) routes when the BGP next hop is a BGP neighbor that is not directly connected.</td>
</tr>
<tr>
<td>Interface</td>
<td>Used for a network address assigned to an interface. Unlike the router next hop, the interface next hop does not reference any specific node on the network.</td>
</tr>
<tr>
<td>Local (locl)</td>
<td>Local address on an interface. This next-hop type causes packets with this destination address to be received locally.</td>
</tr>
<tr>
<td>Multicast (mcst)</td>
<td>Wire multicast next hop (limited to the LAN).</td>
</tr>
<tr>
<td>Multicast discard (mdsc)</td>
<td>Multicast discard.</td>
</tr>
<tr>
<td>Multicast group (mgrp)</td>
<td>Multicast group member.</td>
</tr>
<tr>
<td>Receive (recv)</td>
<td>Receive.</td>
</tr>
<tr>
<td>Reject (rjct)</td>
<td>Discard. An ICMP unreachable message was sent.</td>
</tr>
<tr>
<td>Resolve (rslv)</td>
<td>Resolving next hop.</td>
</tr>
<tr>
<td>Routed multicast (mcrt)</td>
<td>Regular multicast next hop.</td>
</tr>
<tr>
<td>Router</td>
<td>A specific node or set of nodes to which the routing device forwards packets that match the route prefix. To qualify as next-hop type router, the route must meet the following criteria:</td>
</tr>
<tr>
<td></td>
<td>• Must not be a direct or local subnet for the routing device.</td>
</tr>
<tr>
<td></td>
<td>• Must have a next hop that is directly connected to the routing device.</td>
</tr>
<tr>
<td>Table</td>
<td>Routing table next hop.</td>
</tr>
<tr>
<td>Unicast (ucst)</td>
<td>Unicast.</td>
</tr>
<tr>
<td>Unilist (ulst)</td>
<td>List of unicast next hops. A packet sent to this next hop goes to any next hop in the list.</td>
</tr>
</tbody>
</table>

Table 389 on page 3181 describes all possible values for the State output field. A route can be in more than one state (for example, <Active NoReadvt Int Ext>).
### Table 389: State Output Field Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
<td>Route needs accounting.</td>
</tr>
<tr>
<td>Active</td>
<td>Route is active.</td>
</tr>
<tr>
<td>Always Compare MED</td>
<td>Path with a lower multiple exit discriminator (MED) is available.</td>
</tr>
<tr>
<td>AS path</td>
<td>Shorter AS path is available.</td>
</tr>
<tr>
<td>Cisco Non-deterministic MED selection</td>
<td>Cisco nondeterministic MED is enabled, and a path with a lower MED is available.</td>
</tr>
<tr>
<td>Clone</td>
<td>Route is a clone.</td>
</tr>
<tr>
<td>Cluster list length</td>
<td>Length of cluster list sent by the route reflector.</td>
</tr>
<tr>
<td>Delete</td>
<td>Route has been deleted.</td>
</tr>
<tr>
<td>Ex</td>
<td>Exterior route.</td>
</tr>
<tr>
<td>Ext</td>
<td>BGP route received from an external BGP neighbor.</td>
</tr>
<tr>
<td>FlashAll</td>
<td>Forces all protocols to be notified of a change to any route, active or inactive, for a prefix. When not set, protocols are informed of a prefix only when the active route changes.</td>
</tr>
<tr>
<td>Hidden</td>
<td>Route not used because of routing policy.</td>
</tr>
<tr>
<td>IfCheck</td>
<td>Route needs forwarding RPF check.</td>
</tr>
<tr>
<td>IGP metric</td>
<td>Path through next hop with lower IGP metric is available.</td>
</tr>
<tr>
<td>Inactive reason</td>
<td>Flags for this route, which was not selected as best for a particular destination.</td>
</tr>
<tr>
<td>Initial</td>
<td>Route being added.</td>
</tr>
<tr>
<td>Int</td>
<td>Interior route.</td>
</tr>
<tr>
<td>Int Ext</td>
<td>BGP route received from an internal BGP peer or a BGP confederation peer.</td>
</tr>
<tr>
<td>Interior &gt; Exterior &gt; Exterior via Interior</td>
<td>Direct, static, IGP, or EBGP path is available.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>Path with a higher local preference value is available.</td>
</tr>
<tr>
<td>Martian</td>
<td>Route is a martian (ignored because it is obviously invalid).</td>
</tr>
</tbody>
</table>
Table 389: State Output Field Values (continued)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MartianOK</td>
<td>Route exempt from martian filtering.</td>
</tr>
<tr>
<td>Next hop address</td>
<td>Path with lower metric next hop is available.</td>
</tr>
<tr>
<td>No difference</td>
<td>Path from neighbor with lower IP address is available.</td>
</tr>
<tr>
<td>NoReadvrt</td>
<td>Route not to be advertised.</td>
</tr>
<tr>
<td>NotBest</td>
<td>Route not chosen because it does not have the lowest MED.</td>
</tr>
<tr>
<td>Not Best in its group</td>
<td>Incoming BGP AS is not the best of a group (only one AS can be the best).</td>
</tr>
<tr>
<td>NotInstall</td>
<td>Route not to be installed in the forwarding table.</td>
</tr>
<tr>
<td>Number of gateways</td>
<td>Path with a greater number of next hops is available.</td>
</tr>
<tr>
<td>Origin</td>
<td>Path with a lower origin code is available.</td>
</tr>
<tr>
<td>Pending</td>
<td>Route pending because of a hold-down configured on another route.</td>
</tr>
<tr>
<td>Release</td>
<td>Route scheduled for release.</td>
</tr>
<tr>
<td>RIB preference</td>
<td>Route from a higher-numbered routing table is available.</td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>64-bit prefix added to IP subnets to make them unique.</td>
</tr>
<tr>
<td>Route Metric or MED comparison</td>
<td>Route with a lower metric or MED is available.</td>
</tr>
<tr>
<td>Route Preference</td>
<td>Route with lower preference value is available</td>
</tr>
<tr>
<td>Router ID</td>
<td>Path through a neighbor with lower ID is available.</td>
</tr>
<tr>
<td>Secondary</td>
<td>Route not a primary route.</td>
</tr>
<tr>
<td>Unusable path</td>
<td>Path is not usable because of one of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• The route is damped.</td>
</tr>
<tr>
<td></td>
<td>• The route is rejected by an import policy.</td>
</tr>
<tr>
<td></td>
<td>• The route is unresolved.</td>
</tr>
<tr>
<td>Update source</td>
<td>Last tiebreaker is the lowest IP address value.</td>
</tr>
</tbody>
</table>

Table 390 on page 3183 describes the possible values for the Communities output field.
### Table 390: Communities Output Field Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>area-number</em></td>
<td>4 bytes, encoding a 32-bit area number. For AS-external routes, the value is 0. A nonzero value identifies the route as internal to the OSPF domain, and as within the identified area. Area numbers are relative to a particular OSPF domain.</td>
</tr>
<tr>
<td><em>bandwidth:</em> <em>local AS number:</em> <em>link-bandwidth-number</em></td>
<td>Link-bandwidth community value used for unequal-cost load balancing. When BGP has several candidate paths available for multipath purposes, it does not perform unequal-cost load balancing according to the link-bandwidth community unless all candidate paths have this attribute.</td>
</tr>
<tr>
<td><em>domain-id</em></td>
<td>Unique configurable number that identifies the OSPF domain.</td>
</tr>
<tr>
<td><em>domain-id-vendor</em></td>
<td>Unique configurable number that further identifies the OSPF domain.</td>
</tr>
<tr>
<td><em>link-bandwidth-number</em></td>
<td>Link-bandwidth number: from 0 through 4,294,967,295 (bytes per second).</td>
</tr>
<tr>
<td><em>local AS number</em></td>
<td>Local AS number: from 1 through 65,535.</td>
</tr>
<tr>
<td><em>options</em></td>
<td>1 byte. Currently this is only used if the route type is 5 or 7. Setting the least significant bit in the field indicates that the route carries a type 2 metric.</td>
</tr>
<tr>
<td><em>origin</em></td>
<td>(Used with VPNs) Identifies where the route came from.</td>
</tr>
<tr>
<td><em>ospf-route-type</em></td>
<td>1 byte, encoded as 1 or 2 for intra-area routes (depending on whether the route came from a type 1 or a type 2 LSA); 3 for summary routes; 5 for external routes (area number must be 0); 7 for NSSA routes; or 129 for sham link endpoint addresses.</td>
</tr>
<tr>
<td><em>route-type-vendor</em></td>
<td>Displays the area number, OSPF route type, and option of the route. This is configured using the BGP extended community attribute 0x8000. The format is <em>area-number:</em> <em>ospf-route-type:</em> <em>options</em>.</td>
</tr>
<tr>
<td><em>rte-type</em></td>
<td>Displays the area number, OSPF route type, and option of the route. This is configured using the BGP extended community attribute 0x0306. The format is <em>area-number:</em> <em>ospf-route-type:</em> <em>options</em>.</td>
</tr>
<tr>
<td><em>target</em></td>
<td>Defines which VPN the route participates in; <em>target</em> has the format 32-bit <em>IP address</em>:16-bit <em>number</em>. For example, 10.19.0.0:100.</td>
</tr>
<tr>
<td><em>unknown IANA</em></td>
<td>Incoming IANA codes with a value between 0x1 and 0x7fff. This code of the BGP extended community attribute is accepted, but it is not recognized.</td>
</tr>
<tr>
<td><em>unknown OSPF vendor community</em></td>
<td>Incoming IANA codes with a value above 0x8000. This code of the BGP extended community attribute is accepted, but it is not recognized.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show route detail

user@host>  show route detail

inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
```
10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 29
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 1:31:43
  Task: RT
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

10.31.1.0/30 (2 entries, 1 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 2
  Next hop: via so-0/3/0.0, selected
  State: <Active Int>
  Local AS: 69
  Age: 1:30:17
  Task: IF
  Announcement bits (1): 3-Resolve tree 2
  AS path: I
  OSPF Preference: 10
  Next-hop reference count: 1
  Next hop: via so-0/3/0.0, selected
  State: <Int>
  Inactive reason: Route Preference
  Local AS: 69
  Age: 1:30:17    Metric: 1
  Area: 0.0.0.0
  Task: OSPF
  AS path: I

10.31.1.32 (1 entry, 1 announced)
  *Local Preference: 0
  Next hop type: Local
  Next-hop reference count: 7
  Interface: so-0/3/0.0
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:30:20
  Task: IF
  Announcement bits (1): 3-Resolve tree 2
  AS path: I

...
224.0.0.2/32 (1 entry, 1 announced)
  *PIM  Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS:    69
  Age: 1:31:45
  Task: PIM Recv
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

...  

224.0.0.22/32 (1 entry, 1 announced)
  *IGMP  Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS:    69
  Age: 1:31:43
  Task: IGMP
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.255.70.103/32 (1 entry, 1 announced)
  State: <FlashAll>
  *RSVP  Preference: 7
  Next-hop reference count: 6
  Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
  Label-switched-path green-r1-r3
  Label operation: Push 100096
  State: <Active Int>
  Local AS:    69
  Age: 1:25:49    Metric: 2
  Task: RSVP
  Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
  AS path: I

10.255.71.238/32 (1 entry, 1 announced)
  State: <FlashAll>
  *RSVP  Preference: 7
  Next-hop reference count: 6
  Next hop: via so-0/3/0.0 weight 0x1, selected
  Label-switched-path green-r1-r2
  State: <Active Int>
  Local AS:    69
  Age: 1:25:49    Metric: 1
  Task: RSVP
  Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
  AS path: I

private__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

47.0005.80ff.f800.0000.0108.0001.0102.5507.1052/152 (1 entry, 0 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
State: <Active Int>
Local AS: 69
Age: 1:31:44
Task: IF
AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
0 (1 entry, 1 announced)
  *MPLS Preference: 0
    Next hop type: Receive
    Next-hop reference count: 6
    State: <Active Int>
    Local AS: 69
    Age: 1:31:45
    Metric: 1
    Task: MPLS
    Announcement bits (1): 0-KRT
    AS path: I

... 

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
299776 (1 entry, 1 announced)
  TSI:
    KRT in-kernel 299776 /52 -> {Flood}
    *RSVP Preference: 7
    Next hop type: Flood
    Next-hop reference count: 130
    Flood nexthop branches exceed maximum
    Address: 0x8ea65d0

... 

800010 (1 entry, 1 announced)
  *VPLS Preference: 7
  Next-hop reference count: 2
  Next hop: via vt-3/2/0.32769, selected
  Label operation: Pop
  State: <Active Int>
  Age: 1:29:30
  Task: Common L2 VC
  Announcement bits (1): 0-KRT
  AS path: I

vt-3/2/0.32769 (1 entry, 1 announced)
  *VPLS Preference: 7
  Next-hop reference count: 2
  Next hop: 10.31.1.6 via ge-3/1/0 weight 0x1, selected
  Label-switched-path green-r1-r3
  Label operation: Push 800012, Push 100096(top)
  Protocol next hop: 10.255.70.103
  Push 800012
  Indirect next hop: 87272e4 1048574
  State: <Active Int>
  Age: 1:29:30
  Metric2: 2
  Task: Common L2 VC
  Announcement bits (2): 0-KRT 1-Common L2 VC
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS,
  control flags:, mtu: 0

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
abcd::10:255:71:52/128 (1 entry, 0 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
  State: <Active Int>
  Local AS: 69
  Age: 1:31:44
  Task: IF
  AS path: I

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:31:44
  Task: IF
  AS path: I

ff02::2/128 (1 entry, 1 announced)
  *PIM Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:31:45
  Task: PIM Recv6
  Announcement bits (1): 0-KRT
  AS path: I

ff02::d/128 (1 entry, 1 announced)
  *PIM Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:31:45
  Task: PIM Recv6
  Announcement bits (1): 0-KRT
  AS path: I

ff02::16/128 (1 entry, 1 announced)
  *MLD Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:31:43
  Task: MLD
  Announcement bits (1): 0-KRT
  AS path: I

private.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.16385, selected
  State: <Active NoReadvrt Int>
  Age: 1:31:44
Task: IF
AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
   *BGP    Preference: 170/-101
     Route Distinguisher: 10.255.70.103
     Next-hop reference count: 7
     Source: 10.255.70.103
     Protocol next hop: 10.255.70.103
     Indirect next hop: 2 no-forward
     State: <Secondary Active Int Ext>
     Local AS:    69 Peer AS:    69
     Age: 1:25:49    Metric2: 1
     AIGP 210
     Task: BGP_69.10.255.70.103+179
     Announcement bits (1): 0-green-l2vpn
     AS path: I
     Communities: target:11111:1 Layer2-info: encaps:VPLS,
                   control flags:, mtu: 0
     Label-base: 800008, range: 8
     Localpref: 100
     Router ID: 10.255.70.103
     Primary Routing Table bgp.l2vpn.0

10.255.71.52:1:1:1/96 (1 entry, 1 announced)
   *L2VPN  Preference: 170/-1
     Next-hop reference count: 5
     Protocol next hop: 10.255.71.52
     Indirect next hop: 0 -
     State: <Active Int Ext>
     Age: 1:31:40    Metric2: 1
     Task: green-l2vpn
     Announcement bits (1): 1-BGP.0.0.0.0+179
     AS path: I
     Communities: Layer2-info: encaps:VPLS, control flags:Site-Down,
                   mtu: 0
     Label-base: 800016, range: 8, status-vector: 0x9F

10.255.71.52:1:5:1/96 (1 entry, 1 announced)
   *L2VPN  Preference: 170/-101
     Next-hop reference count: 5
     Protocol next hop: 10.255.71.52
     Indirect next hop: 0 -
     State: <Active Int Ext>
     Age: 1:31:40    Metric2: 1
     Task: green-l2vpn
     Announcement bits (1): 1-BGP.0.0.0.0+179
     AS path: I
     Communities: Layer2-info: encaps:VPLS, control flags:, mtu: 0
     Label-base: 800008, range: 8, status-vector: 0x9F

...
Protocol next hop: 10.245.255.63  Indirect next hop: 86af000 296
State: <Active Int>
Local AS: 99
Age: 10:21
Task: l2 circuit
Announcement bits (1): 0-LDP
AS path: I
VC Label 100000, MTU 1500, VLAN ID 512

show route detail (with BGP Multipath)

user@host> show route detail

10.1.1.8/30 (2 entries, 1 announced)
  *BGP  Preference: 170/-101
  Next hop type: Router, Next hop index: 262142
  Address: 0x901a010
  Next-hop reference count: 2
  Source: 10.1.1.2
  Next hop: 10.1.1.2 via ge-0/3/0.1, selected
  Next hop: 10.1.1.6 via ge-0/3/0.5
  State: <Active Ext>
  Local AS: 1 Peer AS: 2
  Age: 5:04:43
  Task: BGP_2.10.1.1.2+59955
  Announcement bits (1): 0-KRT
  AS path: 2 I
  Accepted Multipath
  Localpref: 100
  Router ID: 1.1.1.2
  BGP  Preference: 170/-101
  Next hop type: Router, Next hop index: 678
  Address: 0x8f97520
  Next-hop reference count: 9
  Source: 10.1.1.6
  Next hop: 10.1.1.6 via ge-0/3/0.5, selected
  State: <NotBest Ext>
  Inactive reason: Not Best in its group - Active preferred
  Local AS: 1 Peer AS: 2
  Age: 5:04:43
  Task: BGP_2.10.1.1.6+58198
  AS path: 2 I
  Accepted MultipathContrib
  Localpref: 100
  Router ID: 1.1.1.3

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show route label 299872 detail
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
  *LDP  Preference: 9
  Next hop type: Flood
  Next-hop reference count: 3
  Address: 0x9097d90
  Next hop: via vt-0/1/0.1
  Next-hop index: 261
  Label operation: Pop
  Address: 0x9172130
  Next hop: via so-0/0/3.0
  Next-hop index: 654
Label operation: Swap 299872
State: **Active Int**
Local AS:  1001
Age: 8:20       Metric: 1
Task: LDP
Announcement bits (1): 0-KRT
AS path: I
FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1,
src 192.168.142.2
**show route exact**

**Syntax**

```
show route exact destination-prefix
<brief | detail | extensive | terse>
logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**

```
show route exact destination-prefix
<brief | detail | extensive | terse>
```

**Release Information**

Command introduced before Junos OS Release 7.4.<br>Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display only the routes that exactly match the specified address or range of addresses.

**Options**

- **brief | detail | extensive | terse**—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**.

  - **destination-prefix**—Address or range of addresses.

  - **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

- **view**

**List of Sample Output**

- show route exact on page 3191
- show route exact detail on page 3191
- show route exact extensive on page 3192
- show route exact terse on page 3192

**Output Fields**

For information about output fields, see the output field tables for the **show route** command, the **show route detail** command, the **show route extensive** command, or the **show route terse** command.

**Sample Output**

**show route exact**

```
user@host> show route exact 207.17.136.0/24

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
207.17.136.0/24 *[Static/5] 2d 03:30:22
    > to 192.168.71.254 via fxp0.0
```

**show route exact detail**

```
user@host> show route exact 207.17.136.0/24 detail

inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
Restart Complete
207.17.136.0/24 (1 entry, 1 announced)
    *Static Preference: 5
```
Next-hop reference count: 29
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Local AS: 69
Age: 2d 3:30:26
Task: RT
Announcement bits (2): 0-KRT 3-Resolve tree 2
AS path: I

show route exact extensive

user@host> show route exact 207.17.136.0/24 extensive
inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
207.17.136.0/24 (1 entry, 1 announced)
TSI:
KRT in-kernel 207.17.136.0/24 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 29
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 1:25:18
  Task: RT
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

show route exact terse

user@host> show route exact 207.17.136.0/24 terse
inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
A Destination  P Prf Metric 1 Metric 2  Next hop        AS path
* 207.17.136.0/24  S 5    >192.168.71.254
show route export

**Syntax**
show route export
<brief | detail>
<instance <instance-name> | routing-table-name>
<logical-system (all | logical-system-name)>

**Syntax (EX Series Switches)**
show route export
<brief | detail>
<instance <instance-name> | routing-table-name>

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display policy-based route export information. Policy-based export simplifies the process of exchanging route information between routing instances.

**Options**
- none—(Same as brief.) Display standard information about policy-based export for all instances and routing tables on all systems.
- brief | detail—(Optional) Display the specified level of output.
- instance <instance-name>—(Optional) Display a particular routing instance for which policy-based export is currently enabled.
- logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
- routing-table-name—(Optional) Display information about policy-based export for all routing tables whose name begins with this string (for example, inet.0 and inet6.0 are both displayed when you run the show route export inet command).

**Required Privilege**
view

**List of Sample Output**
- show route export on page 3194
- show route export detail on page 3194
- show route export instance detail on page 3194

**Output Fields**
Table 391 on page 3193 lists the output fields for the show route export command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table or table-name</td>
<td>Name of the routing tables that either import or export routes.</td>
<td>All levels</td>
</tr>
<tr>
<td>Routes</td>
<td>Number of routes exported from this table into other tables. If a particular route is exported to different tables, the counter will only increment by one.</td>
<td>brief none</td>
</tr>
<tr>
<td>Export</td>
<td>Whether the table is currently exporting routes to other tables: Y or N (Yes or No).</td>
<td>brief none</td>
</tr>
</tbody>
</table>
Table 391: show route export Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Tables currently importing routes from the originator table. (Not displayed for tables that are not exporting any routes.)</td>
<td>detail</td>
</tr>
<tr>
<td>Flags</td>
<td>(instance keyword only) Flags for this feature on this instance:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• config auto-policy—The policy was deduced from the configured IGP export policies.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• cleanup—Configuration information for this instance is no longer valid.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• config—The instance was explicitly configured.</td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>(instance keyword only) Configured option displays the type of routing tables the feature handles:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• unicast—Indicates instance.inet.0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• multicast—Indicates instance.inet.2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unicast multicast—Indicates instance.inet.0 and instance.inet.2.</td>
<td></td>
</tr>
<tr>
<td>Import policy</td>
<td>(instance keyword only) Policy that route export uses to construct the import-export matrix. Not displayed if the instance type is vrf.</td>
<td>detail</td>
</tr>
<tr>
<td>Instance</td>
<td>(instance keyword only) Name of the routing instance.</td>
<td>detail</td>
</tr>
<tr>
<td>Type</td>
<td>(instance keyword only) Type of routing instance: forwarding, non-forwarding, or vrf.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show route export

```
user@host> show route export
Table                  Export Routes
inet.0                 N 0
black.inet.0           Y 3
red.inet.0             Y 4
```

show route export detail

```
user@host> show route export detail
inet.0 Routes: 0
black.inet.0 Routes: 3
  Import: [ inet.0 ]
red.inet.0 Routes: 4
  Import: [ inet.0 ]
```

show route export instance detail

```
user@host> show route export instance detail
Instance: master Type: forwarding
  Flags: <config auto-policy> Options: <unicast multicast>
  Import policy: [ (ospf-master-from-red || isis-master-from-black) ]
```
Instance: black
Type: non-forwarding

Instance: red
Type: non-forwarding
**show route extensive**

**Syntax**
```
show route extensive
<destination-prefix>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route extensive
<destination-prefix>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display extensive information about the active entries in the routing tables.

**Options**
- **none**—Display all active entries in the routing table.
- **destination-prefix**—(Optional) Display active entries for the specified address or range of addresses.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view

**List of Sample Output**
- show route extensive on page 3202
- show route extensive (Access Route) on page 3208
- show route extensive (BGP PIC Edge) on page 3209
- show route extensive (FRR and LFA) on page 3209
- show route extensive (Route Reflector) on page 3210
- show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 3210

**Output Fields**
Table 190 on page 1594 describes the output fields for the `show route extensive` command. Output fields are listed in the approximate order in which they appear.

**Table 392: show route extensive Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
</tbody>
</table>
| number routes     | Number of routes in the routing table and total number of routes in the following states:  
  - active (routes that are active).  
  - holdown (routes that are in the pending state before being declared inactive).  
  - hidden (routes that are not used because of a routing policy). |
Table 392: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-destination (entry, announced)</td>
<td>Route destination (for example: 10.0.0.1/24). The entry value is the number of route for this destination, and the announced value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>• <strong>MPLS-label</strong> (for example, 80001).</td>
</tr>
<tr>
<td></td>
<td>• <strong>interface-name</strong> (for example, ge-1/0/2).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address</strong>:control-word-status:encapsulation type:vc-id:source** (Layer 2 circuit only; for example, 10.1.1.195:NoCtrlWord:1:1:Local:/96).</td>
</tr>
<tr>
<td></td>
<td>• <strong>neighbor-address</strong>—Address of the neighbor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>control-word-status</strong>—Whether the use of the control word has been negotiated for this virtual circuit: <strong>NoCtrlWord</strong> or <strong>CtrlWord</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>encapsulation type</strong>—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport.</td>
</tr>
<tr>
<td></td>
<td>• <strong>vc-id</strong>—Virtual circuit identifier.</td>
</tr>
<tr>
<td></td>
<td>• <strong>source</strong>—Source of the advertisement: <strong>Local</strong> or <strong>Remote</strong>.</td>
</tr>
<tr>
<td>TSI</td>
<td>Protocol header information.</td>
</tr>
<tr>
<td>label stacking</td>
<td>(Next-to-the-last-hop routing device for MPLS only) Depth of the MPLS label stack, where the label-popping operation is needed to remove one or more labels from the top of the stack. A pair of routes is displayed, because the pop operation is performed only when the stack depth is two or more labels.</td>
</tr>
<tr>
<td></td>
<td>• <strong>S=0 route</strong> indicates that a packet with an incoming label stack depth of two or more exits this router with one fewer label (the label-popping operation is performed).</td>
</tr>
<tr>
<td></td>
<td>• If there is no <strong>S=</strong> information, the route is a normal MPLS route, which has a stack depth of 1 (the label-popping operation is not performed).</td>
</tr>
<tr>
<td>[protocol, preference]</td>
<td>Protocol from which the route was learned and the preference value for the route.</td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>• - —A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>• *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route.</td>
</tr>
<tr>
<td></td>
<td>In every routing metric except for the BGP <strong>LocalPref</strong> attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the <strong>LocalPref</strong> value in the <strong>Preference2</strong> field. For example, if the <strong>LocalPref</strong> value for Route 1 is 100, the <strong>Preference2</strong> value is -101. If the <strong>LocalPref</strong> value for Route 2 is 155, the <strong>Preference2</strong> value is -156. Route 2 is preferred because it has a higher <strong>LocalPref</strong> value and a lower <strong>Preference2</strong> value.</td>
</tr>
<tr>
<td>Level</td>
<td>(IS-IS only). In IS-IS, a single autonomous system (AS) can be divided into smaller groups called areas. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area. When the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs.</td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>IP subnet augmented with a 64-bit prefix.</td>
</tr>
</tbody>
</table>
### Table 392: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next-hop type</strong></td>
<td>Type of next hop. For a description of possible values for this field, see the Output Field table in the <code>show route detail</code> command.</td>
</tr>
<tr>
<td><strong>Next-hop reference count</strong></td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td><strong>Flood next-hop branches exceed maximum message</strong></td>
<td>Indicates that the number of flood next-hop branches exceeded the system limit of 32 branches, and only a subset of the flood next-hop branches were installed in the kernel.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>IP address of the route source.</td>
</tr>
<tr>
<td><strong>Next hop</strong></td>
<td>Network layer address of the directly reachable neighboring system.</td>
</tr>
<tr>
<td><strong>via</strong></td>
<td>Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word <em>Selected</em>. This field can also contain the following information:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Weight</strong>—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Balance</strong>—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.</td>
</tr>
<tr>
<td><strong>Label-switched-path</strong></td>
<td>Name of the LSP used to reach the next hop.</td>
</tr>
<tr>
<td><strong>lsp-path-name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Label operation</strong></td>
<td>MPLS label and operation occurring at this routing device. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label).</td>
</tr>
<tr>
<td><strong>Offset</strong></td>
<td>Whether the metric has been increased or decreased by an offset value.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>(Local only) Local interface name.</td>
</tr>
<tr>
<td><strong>Protocol next hop</strong></td>
<td>Network layer address of the remote routing device that advertised the prefix. This address is used to recursively derive a forwarding next hop.</td>
</tr>
<tr>
<td><strong>label-operation</strong></td>
<td>MPLS label and operation occurring at this routing device. The operation can be <strong>pop</strong> (where a label is removed from the top of the stack), <strong>push</strong> (where another label is added to the label stack), or <strong>swap</strong> (where a label is replaced by another label).</td>
</tr>
</tbody>
</table>
### Table 392: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| **Indirect next hops**| When present, a list of nodes that are used to resolve the path to the next-hop destination, in the order that they are resolved. When BGP PIC Edge is enabled, the output lines that contain *Indirect next hop: weight* follow next hops that the software can use to repair paths where a link failure occurs. The next-hop weight has one of the following values:  
  - 0x1 indicates active next hops.  
  - 0x4000 indicates passive next hops. |
| **State**             | State of the route (a route can be in more than one state). See the Output Field table in the `show routetable detail` command. |
| **Session ID**        | The BFD session ID number that represents the protection using MPLS fast route (FRR) and loop-free alternate (LFA). |
| **Weight**            | Weight for the backup path. If the weight of an indirect next hop is larger than zero, the weight value is shown. For sample output, see `show routetable`. |
Table 392: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inactive reason</strong></td>
<td>If the route is inactive, the reason for its current state is indicated. Typical reasons include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active preferred</strong>—Currently active route was selected over this route.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Always compare MED</strong>—Path with a lower multiple exit discriminator (MED) is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AS path</strong>—Shorter AS path is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco Non-deterministic MED selection</strong>—Cisco nondeterministic MED is enabled and a path with a lower MED is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cluster list length</strong>—Path with a shorter cluster list length is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Forwarding use only</strong>—Path is only available for forwarding purposes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IGP metric</strong>—Path through the next hop with a lower IGP metric is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IGP metric type</strong>—Path with a lower OSPF link-state advertisement type is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Interior &gt; Exterior &gt; Exterior via Interior</strong>—Direct, static, IGP, or EBGP path is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Local preference</strong>—Path with a higher local preference value is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Next hop address</strong>—Path with a lower metric next hop is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>No difference</strong>—Path from a neighbor with a lower IP address is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Best in its group</strong>—Occurs when multiple peers of the same external AS advertise the same prefix and are grouped together in the selection process. When this reason is displayed, an additional reason is provided (typically one of the other reasons listed).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Number of gateways</strong>—Path with a higher number of next hops is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Origin</strong>—Path with a lower origin code is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OSPF version</strong>—Path does not support the indicated OSPF version.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RIB preference</strong>—Route from a higher-numbered routing table is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route destinguisher</strong>—64-bit prefix added to IP subnets to make them unique.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route metric or MED comparison</strong>—Route with a lower metric or MED is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Route preference</strong>—Route with a lower preference value is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Router ID</strong>—Path through a neighbor with a lower ID is available.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unusable path</strong>—Path is not usable because of one of the following conditions: the route is damped, the route is rejected by an import policy, or the route is unresolved.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Update source</strong>—Last tiebreaker is the lowest IP address value.</td>
</tr>
<tr>
<td><strong>Local AS</strong></td>
<td>Autonomous system (AS) number of the local routing device.</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>How long the route has been known.</td>
</tr>
<tr>
<td><strong>AIGP</strong></td>
<td>Accumulated interior gateway protocol (AIGP) BGP attribute.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>Cost value of the indicated route. For routes within an AS, the cost is determined by IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.</td>
</tr>
<tr>
<td><strong>MED-plus-IGP</strong></td>
<td>Metric value for BGP path selection to which the IGP cost to the next-hop destination has been added.</td>
</tr>
<tr>
<td><strong>TTL-Action</strong></td>
<td>For MPLS LSPs, state of the TTL propagation attribute. Can be enabled or disabled for all RSVP-signaled and LDP-signaled LSPs or for specific VRF routing instances.</td>
</tr>
</tbody>
</table>

For sample output, see [show route table](#).
Table 392: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Name of the protocol that has added the route.</td>
</tr>
<tr>
<td>Announcement bits</td>
<td>List of protocols that announce this route. \textit{n-Resolve inet} indicates that the route is used for route resolution for next hops found in the routing table. \textit{n} is an index used by Juniper Networks customer support only.</td>
</tr>
<tr>
<td>AS path</td>
<td>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
</tr>
<tr>
<td></td>
<td>• \textit{Recorded}—The AS path is recorded by the sample process (sampled).</td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete; typically, the AS path was aggregated.</td>
</tr>
<tr>
<td></td>
<td>When AS path numbers are included in the route, the format is as follows:</td>
</tr>
<tr>
<td></td>
<td>• [ ]—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured.</td>
</tr>
<tr>
<td></td>
<td>• { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.</td>
</tr>
<tr>
<td></td>
<td>• ()—Parentheses enclose a confederation.</td>
</tr>
<tr>
<td></td>
<td>• ( [ ] )—Parentheses and brackets enclose a confederation set.</td>
</tr>
<tr>
<td></td>
<td>\textbf{NOTE:} In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.</td>
</tr>
<tr>
<td>FECs bound to route</td>
<td>Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.</td>
</tr>
<tr>
<td>AS path: I &lt;Originator&gt;</td>
<td>(For route reflected output only) Originator ID attribute set by the route reflector.</td>
</tr>
<tr>
<td>VC Label</td>
<td>MPLS label assigned to the Layer 2 circuit virtual connection.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) of the Layer 2 circuit.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN identifier of the Layer 2 circuit.</td>
</tr>
<tr>
<td>Cluster list</td>
<td>(For route reflected output only) Cluster ID sent by the route reflector.</td>
</tr>
<tr>
<td>Originator ID</td>
<td>(For route reflected output only) Address of router that originally sent the route to the route reflector.</td>
</tr>
<tr>
<td>Prefixes bound to route</td>
<td>Forwarding equivalent class (FEC) bound to this route. Applicable only to routes installed by LDP.</td>
</tr>
<tr>
<td>Communities</td>
<td>Community path attribute for the route. See the Output Field table in the \texttt{show route detail} command for all possible values for this field.</td>
</tr>
<tr>
<td>Layer2-info: encaps</td>
<td>Layer 2 encapsulation (for example, VPLS).</td>
</tr>
</tbody>
</table>
Table 392: show route extensive Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>control flags</td>
<td>Control flags: none or Site Down.</td>
</tr>
<tr>
<td>mtu</td>
<td>Maximum transmission unit (MTU) information.</td>
</tr>
<tr>
<td>Label-Base, range</td>
<td>First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.</td>
</tr>
<tr>
<td>status vector</td>
<td>Layer 2 VPN and VPLS network layer reachability information (NLRI).</td>
</tr>
<tr>
<td>Localpref</td>
<td>Local preference value included in the route.</td>
</tr>
<tr>
<td>Router ID</td>
<td>BGP router ID as advertised by the neighbor in the open message.</td>
</tr>
<tr>
<td>Primary Routing Table</td>
<td>In a routing table group, the name of the primary routing table in which the route resides.</td>
</tr>
<tr>
<td>Secondary Tables</td>
<td>In a routing table group, the name of one or more secondary tables in which the route resides.</td>
</tr>
<tr>
<td>Originating RIB</td>
<td>Name of the routing table whose active route was used to determine the forwarding next-hop entry in the resolution database. For example, in the case of inet.0 resolving through inet.0 and inet.3, this field indicates which routing table, inet.0 or inet.3, provided the best path for a particular prefix.</td>
</tr>
<tr>
<td>Node path count</td>
<td>Number of nodes in the path.</td>
</tr>
<tr>
<td>Forwarding nexthops</td>
<td>Number of forwarding next hops. The forwarding next hop is the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.</td>
</tr>
</tbody>
</table>

Sample Output

```
user@host> show route extensive
inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI: KRT in-kernel 10.10.0.0/16 -> (192.168.71.254)
   *Static Preference: 5
   Next-hop reference count: 29
   Next hop: 192.168.71.254 via fxp0.0, selected
   State: <Active NoReadvrt Int Ext>
   Local AS:    69
   Age: 1:34:06
   Task: RT
   Announcement bits (2): 0-KRT 3-Resolve tree 2
   AS path: I

10.31.1.0/30 (2 entries, 1 announced)
   *Direct Preference: 0
   Next hop type: Interface
   Next-hop reference count: 2
   Next hop: via so-0/3/0.0, selected
   State: <Active Int>
```
Local AS: 69
Age: 1:32:40
Task: IF
Announcement bits (1): 3-Resolve tree 2
AS path: I

OSPF
Preference: 10
Next-hop reference count: 1
Next hop: via so-0/3/0.0, selected
State: <Int>
Inactive reason: Route Preference
Local AS: 69
Age: 1:32:40
Metric: 1
Area: 0.0.0.0
Task: OSPF
AS path: I

10.31.1.1/32 (1 entry, 1 announced)
*Local
Preference: 0
Next hop type: Local
Next-hop reference count: 7
Interface: so-0/3/0.0
State: <Active NoReadvrt Int>
Local AS: 69
Age: 1:32:43
Task: IF
Announcement bits (1): 3-Resolve tree 2
AS path: I

...
224.0.0.22/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 224.0.0.22/32 -> {}
  *IGMP  Preference: 0
  Next-hop reference count: 18
  State: <Active NoReadvrt Int>
  Local AS:    69
  Age: 1:34:06
  Task: IGMP
  Announcement bits (2): 0-KRT 3-Resolve tree 2
  AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.255.70.103/32 (1 entry, 1 announced)
  State: <FlashAll>
  *RSVP   Preference: 7
  Next-hop reference count: 6
  Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
  Label-switched-path green-r1-r3
  Label operation: Push 100096
  State: <Active Int>
  Local AS:    69
  Age: 1:28:12 Metric: 2
  Task: RSVP
  Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
  AS path: I

10.255.71.238/32 (1 entry, 1 announced)
  State: <FlashAll>
  *RSVP   Preference: 7
  Next-hop reference count: 6
  Next hop: via so-0/3/0.0 weight 0x1, selected
  Label-switched-path green-r1-r2
  State: <Active Int>
  Local AS:    69
  Age: 1:28:12 Metric: 1
  Task: RSVP
  Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
  AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

... iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

47.0005.80ff.f800.0000.0108.0001.0102.5507.1052/152 (1 entry, 0 announced)
  *Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
  State: <Active Int>
  Local AS:    69
  Age: 1:34:07
  Task: IF
  AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

0 (1 entry, 1 announced)
TSI:
KRT in-kernel 0      /36 -> {}
  *MPLS Preference: 0
  Next hop type: Receive
  Next-hop reference count: 6
  State: <Active Int>
  Local AS: 69
  Age: 1:34:08 Metric: 1
  Task: MPLS
  Announcement bits (1): 0-KRT
  AS path: I

... mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
299776 (1 entry, 1 announced)
TSI:
KRT in-kernel 299776 /52 -> {Flood}
  *RSVP Preference: 7
  Next hop type: Flood
  Next-hop reference count: 130
  Flood nexthop branches exceed maximum
  Address: 0x8ea65d0

800010 (1 entry, 1 announced)
TSI:
KRT in-kernel 800010 /36 -> {vt-3/2/0.32769}
  *VPLS Preference: 7
  Next-hop reference count: 2
  Next hop: via vt-3/2/0.32769, selected
  Label operation: Pop
  State: <Active Int>
  Age: 1:31:53
  Task: Common L2 VC
  Announcement bits (1): 0-KRT
  AS path: I

vt-3/2/0.32769 (1 entry, 1 announced)
TSI:
KRT in-kernel vt-3/2/0.32769.0      /16 -> {indirect(1048574)}
  *VPLS Preference: 7
  Next-hop reference count: 2
  Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
  Label-switched-path green-r1-r3
  Label operation: Push 800012, Push 100096(top)
  Protocol next hop: 10.255.70.103
  Push 800012
  Indirect next hop: 87272e4 1048574
  State: <Active Int>
  Age: 1:31:53 Metric2: 2
  Task: Common L2 VC
  Announcement bits (2): 0-KRT 1-Common L2 VC
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS,
  control flags:, mtu: 0
  Indirect next hops: 1
    Protocol next hop: 10.255.70.103 Metric: 2
      Push 800012
      Indirect next hop: 87272e4 1048574
Indirect path forwarding next hops: 1
Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1
10.255.70.103/32 Originating RIB: inet.3
Metric: 2 Node path count: 1
Forwarding nexthops: 1
Next hop: 10.31.1.6 via ge-3/1/0.0

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

abcd::10:255:71:52/128 (1 entry, 0 announced)
  Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: lo0.0, selected
  State: <Active Int>
  Local AS: 69
  Age: 1:34:07
  Task: IF
  AS path: I

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
  Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: lo0.0, selected
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:34:07
  Task: IF
  AS path: I

ff02::2/128 (1 entry, 1 announced)
  TSI:
  KRT in-kernel ff02::2/128 -> {}
  PIM
    Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:08
    Task: PIM Recv6
    Announcement bits (1): 0-KRT
    AS path: I

ff02::d/128 (1 entry, 1 announced)
  TSI:
  KRT in-kernel ff02::d/128 -> {}
  PIM
    Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:08
    Task: PIM Recv6
    Announcement bits (1): 0-KRT
    AS path: I

ff02::16/128 (1 entry, 1 announced)
  TSI:
  KRT in-kernel ff02::16/128 -> {}
  MLD
    Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
Local AS: 69
Age: 1:34:06
Task: MLD
Announcement bits (1): 0-KRT
AS path: I

private.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
*Direct Preference: 0
Next hop type: Interface
Next-hop reference count: 1
Next hop: via lo0.16385, selected
State: <Active NoReadvrt Int>
Age: 1:34:07
Task: IF
AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
*BGP Preference: 170/-101
Route Distinguisher: 10.255.70.103:1
Next-hop reference count: 7
Source: 10.255.70.103
Protocol next hop: 10.255.70.103
Indirect next hop: 2 no-forward
State: <Secondary Active Int Ext>
Local AS: 69 Peer AS: 69
Age: 1:28:12 Metric2: 1
Task: BGP_69.10.255.70.103+179
Announcement bits (1): 0-green-l2vpn
AS path: I
Communities: target:11111:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0
Label-base: 800008, range: 8
Localpref: 100
Router ID: 10.255.70.103
Primary Routing Table bgp.l2vpn.0

10.255.71.52:1:1:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699540
*B2VPN Preference: 170/-1
Next-hop reference count: 5
Protocol next hop: 10.255.71.52
Indirect next hop: 0 -
State: <Active Int Ext>
Age: 1:34:03 Metric2: 1
Task: green-l2vpn
Announcement bits (1): 1-BGP.0.0.0.0+179
AS path: I
Communities: Layer2-info: encaps:VPLS, control flags:Site-Down, mtu: 0
Label-base: 800016, range: 8, status-vector: 0x9F

10.255.71.52:1:5:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699528
*B2VPN Preference: 170/-101
Next-hop reference count: 5
Protocol next hop: 10.255.71.52
Indirect next hop: 0 -
State: <Active Int Ext>
Age: 1:34:03   Metric2: 1
Task: green-l2vpn
Announcement bits (1): 1-BGP.0.0.0.0+179
AS path: I
Communities: Layer2-info: encaps:VPLS, control flags:, mtu: 0
Label-base: 800008, range: 8, status-vector: 0x9F

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

TSI:

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  *L2CKT Preference: 7
  Next hop: via so-1/1/2.0 weight 1, selected
  Label-switched-path my-lsp
  Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
  State: <Active Int>
  Local AS: 99
  Age: 10:21
  Task: l2 circuit
  Announcement bits (1): 0-LDP
  AS path: I
  VC Label 100000, MTU 1500, VLAN ID 512

55.0.0.0/24 (1 entry, 1 announced)
TSI:

KRT queued (pending) add
55.0.0.0/24 -> {Push 300112}
  *BGP Preference: 170/-101
  Next hop type: Router
  Address: 0x925c208
  Next-hop reference count: 2
  Source: 10.0.0.9
  Next hop: 10.0.0.9 via ge-1/2/0.15, selected
  Label operation: Push 300112
  Label TTL action: prop-ttl
  State: <Active Ext>
  Local AS: 7019 Peer AS: 13979
  Age: lw0d 23:06:56
  AIGP: 25
  Task: BGP_13979.10.0.0.9+56732
  Announcement bits (1): 0-KRT
  AS path: 13979 7018 I
  Accepted
  Route Label: 300112
  Localpref: 100
  Router ID: 10.9.9.1

show route extensive (Access Route)

user@host> show route 13.160.0.102 extensive
inet.0: 39256 destinations, 39258 routes (39255 active, 0 holddown, 1 hidden)
13.160.0.102/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.102/32 -> {13.160.0.2}
OSPF area : 0.0.0.0, LSA ID : 13.160.0.102, LSA type : Extern
  Access Preference: 13
  Next-hop reference count: 78472
  Next hop: 13.160.0.2 via fe-0/0/0.0, selected
  State: <Active Int>
  Age: 12
  Task: RPD Unix Domain Server./var/run/rpd_serv.local
  Announcement bits (2): 0-KRT 1-OSPFv2
AS path: I

show route extensive (BGP PIC Edge)

user@host> show route 1.1.1.6 extensive
ed.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
  1.1.1.6/32 (3 entries, 2 announced)
    State: <CalcForwarding>
    TSI:
    KRT in-kernel 1.1.1.6/32 -> {indirect(1048574), indirect(1048577)}
      Page 0 idx 0 Type 1 val 9219e30
      Nexthop: Self
      AS path: [2] 3 I
      Communities: target:2:1
    Path 1.1.1.6 from 1.1.1.4 Vector len 4. Val: 0
      #Multipath Preference: 255
      Next hop type: Indirect
      Address: 0x93f4010
      Next-hop reference count: 2
    Protocol next hop: 1.1.1.4
    Push 299824
    Indirect next hop: 944c000 1048574 INH Session ID: 0x3
    Indirect next hop: weight 0x1
    Protocol next hop: 1.1.1.5
    Push 299824
    Indirect next hop: 944c1d8 1048577 INH Session ID: 0x4
    Indirect next hop: weight 0x4000
    State: <ForwardingOnly Int Ext>
    Inactive reason: Forwarding use only
    Age: 25  Metric2: 15
    Validation State: unverified
    Task: RT
    Announcement bits (1): 0-KRT
    AS path: 3 I
    Communities: target:2:1

show route extensive (FRR and LFA)

user@host> show route 20.31.2.0 extensive
inet.0: 46 destinations, 49 routes (45 active, 0 holddown, 1 hidden)
  20.31.2.0/24 (2 entries, 1 announced)
    State: FlashAll
    TSI:
    KRT in-kernel 20.31.2.0/24 -> {Push 299776, Push 299792}
      *RSVP
      Preference: 7/1
      Next hop type: Router, Next hop index: 1048574
      Address: 0xbbbc010
      Next-hop reference count: 5
      Next hop: 10.31.1.2 via ge-2/1/8.0 weight 0x1, selected
      Label-switched-path europa-d-to-europa-e
show route extensive (Route Reflector)

user@host> show route extensive
1.0.0.0/8 (1 entry, 1 announced)

TSI:
KRT in-kernel 1.0.0.0/8 -> {indirect(40)}
  *BGP Preference: 170/-101
  Source: 192.168.4.214
  Protocol next hop: 207.17.136.192 Indirect next hop: 84ac908 40
  State: <Active Int Ext>
  Local AS: 10458 Peer AS: 10458
  Age: 3:09 Metric: 0 Metric2: 0
  Task: BGP_10458.192.168.4.214+1033
  Announcement bits (2): 0-KRT 4-Resolve inet.0
  AS path: 3944 7777 I <Originator>
  Cluster list: 1.1.1.1
  Originator ID: 10.255.245.88
  Communities: 7777:7777
  Localpref: 100
  Router ID: 4.4.4.4
  Indirect next hops: 1
    Protocol next hop: 207.17.136.192 Metric: 0
    Indirect next hop: 84ac908 40
    Indirect path forwarding next hops: 0
    Next hop type: Discard

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show route label 299872 detail
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
  *LDP Preference: 9
Next hop type: Flood
Next-hop reference count: 3
Address: 0x9097d90
Next hop: via vt-0/1/0.1
Next-hop index: 661
Label operation: Pop
Address: 0x9172130
Next hop: via so-0/0/3.0
Next-hop index: 654
Label operation: Swap 299872
State: **Active Int>
Local AS:  1001
Age: 8:20       Metric: 1
Task: LDP
Announcement bits (1): 0-KRT
AS path: I
FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1,
src 192.168.142.2
**show route flow validation**

**Syntax**

```
show route flow validation
<brief | detail>
<ip-prefix>
<table table-name>
logical-system (all | logical-system-name)
```

**Syntax (EX Series Switches)**

```
show route flow validation
<brief | detail>
<ip-prefix>
<table table-name>
```

**Release Information**


**Description**

Display flow route information.

**Options**

none—Display flow route information.

brief | detail—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.

ip-prefix—(Optional) IP address for the flow route.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

table table-name—(Optional) Display flow route information for all routing tables whose name begins with this string (for example, inet.0 and inet6.0 are both displayed when you run the **show route flow validation inet** command).

**Required Privilege**

Level view

**List of Sample Output**

`show route flow validation on page 3213`

**Output Fields**

Table 393 on page 3212 lists the output fields for the **show route flow validation** command. Output fields are listed in the approximate order in which they appear.

**Table 393: show route flow validation Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>routing-table-name</code></td>
<td>Name of the routing table (for example, inet.0).</td>
<td>All levels</td>
</tr>
<tr>
<td><code>prefix</code></td>
<td>Route address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Active unicast route</td>
<td>Active route in the routing table.</td>
<td>All levels</td>
</tr>
<tr>
<td>Dependent flow</td>
<td>Number of flows for which there are</td>
<td>All levels</td>
</tr>
<tr>
<td>destinations</td>
<td>routes in the routing table.</td>
<td></td>
</tr>
</tbody>
</table>
Table 393: show route flow validation Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin</td>
<td>Source of the route flow.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbor AS</td>
<td>Autonomous system identifier of the neighbor.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flow destination</td>
<td>Number of entries and number of destinations that match the route flow.</td>
<td>All levels</td>
</tr>
<tr>
<td>Unicast best match</td>
<td>Destination that is the best match for the route flow.</td>
<td>All levels</td>
</tr>
<tr>
<td>Flags</td>
<td>Information about the route flow.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show route flow validation

```
user@host> show route flow validation
inet.0:
10.0.5.0/24 Active unicast route
Dependent flow destinations: 1
Origin: 192.168.224.218, Neighbor AS: 65001
Flow destination (3 entries, 1 match origin)
Unicast best match: 10.0.5.0/24
Flags: SubtreeApex Consistent
```
**show route inactive-path**

**Syntax**
```
show route inactive-path
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route inactive-path
  <brief | detail | extensive | terse>
```

**Release Information**

**Description**
Display routes for destinations that have no active route. An inactive route is a route that was not selected as the best path.

**Options**
- **none**—Display all inactive routes.
- **brief | detail | extensive | terse**—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**
view

**List of Sample Output**
- show route inactive-path on page 3214
- show route inactive-path detail on page 3215
- show route inactive-path extensive on page 3216
- show route inactive-path terse on page 3216

**Output Fields**
For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

**Sample Output**
```
show route inactive-path

user@host> show route inactive-path

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
10.12.100.12/30     [OSPF/10] 03:57:28, metric 1
  > via so-0/3/0.0
private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.0.0.0/8          [Direct/0] 04:39:56
  > via fxp1.0
```
show route inactive-path detail

user@host> show route inactive-path detail

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Restart Complete

10.12.100.12/30 (2 entries, 1 announced)
   OSPF  Preference: 10
   Next-hop reference count: 1
   Next hop: via so-0/3/0.0, selected
   State: <Int>
   Inactive reason: Route Preference
   Local AS:     1
   Age: 3:58:24    Metric: 1
   Area: 0.0.0.0
   Task: OSPF
   AS path: I

private1__.inet6.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

10.0.0.0/8 (2 entries, 0 announced)
   Direct Preference: 0
   Next hop type: Interface
   Next-hop reference count: 1
   Next hop: via fxp1.0, selected
   State: <NotBest Int>
   Inactive reason: No difference
   Age: 4:40:52
   Task: IF
   AS path: I

red.inet.0: 6 destinations, 8 routes (4 active, 0 holddown, 3 hidden)
Restart Complete

10.12.80.0/30 (2 entries, 1 announced)
   BGP    Preference: 170/-101
   Next-hop reference count: 6
   Source: 10.12.80.1
show route inactive-path extensive

The output for the show route inactive-path extensive command is identical to that of the show route inactive-path detail command. For sample output, see show route inactive-path detail on page 3215.

show route inactive-path terse

user@host> show route inactive-path terse

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Reset Complete
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf  Metric 1  Metric 2  Next hop        AS path
10.12.100.12/30     O  10          1            >so-0/3/0.0

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf  Metric 1  Metric 2  Next hop        AS path
10.0.0.0/8            D   0                       >fxp1.0

red.inet.0: 6 destinations, 8 routes (4 active, 0 holddown, 3 hidden)
Reset Complete
+ = Active Route, - = Last Active, * = Both

A Destination        P Prf  Metric 1  Metric 2  Next hop        AS path
10.12.80.0/30       B 170        100            >10.12.80.1      100 I

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Reset Complete

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Reset Complete

bgp.l3vpn.0: 3 destinations, 3 routes (0 active, 0 holddown, 3 hidden)
Reset Complete

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Reset Complete

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
**show route inactive-prefix**

**Syntax**
```
show route inactive-prefix
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route inactive-prefix
<brief | detail | extensive | terse>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display inactive route destinations in each routing table.

**Options**
- `none`—Display all inactive route destination.
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**
- `view`

**List of Sample Output**
- `show route inactive-prefix on page 3217`
- `show route inactive-prefix detail on page 3217`
- `show route inactive-prefix extensive on page 3218`
- `show route inactive-prefix terse on page 3218`

**Output Fields**
For information about output fields, see the output field tables for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

**Sample Output**

**show route inactive-prefix**
```
user@host> show route inactive-prefix
inet.0: 14 destinations, 14 routes (13 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
127.0.0.1/32 [Direct/0] 00:04:54
  > via lo0.0
```

**show route inactive-prefix detail**
```
user@host> show route inactive-prefix detail
inet.0: 14 destinations, 14 routes (13 active, 0 holddown, 1 hidden)
127.0.0.1/32 (1 entry, 0 announced)
  Direct Preference: 0
  Next hop type: Interface
```
show route inactive-prefix extensive

The output for the `show route inactive-prefix extensive` command is identical to that of the `show route inactive-path detail` command. For sample output, see `show route inactive-prefix detail` on page 3217.

show route inactive-prefix terse

```
user@host> show route inactive-prefix terse

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination P Prf Metric 1 Metric 2 Next hop AS path
127.0.0.1/32 D 0 0  >via lo0.0
```
show route instance

Syntax

`show route instance <brief | detail | summary> <instance-name> <logical-system (all | logical-system-name)> <operational>`

Syntax (EX Series Switches and QFX Series)

`show route instance <brief | detail | summary> <instance-name> <operational>`

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display routing instance information.

Options

`none`—(Same as `brief`) Display standard information about all routing instances.

`brief | detail | summary`—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to `brief`. (These options are not available with the `operational` keyword.)

`instance-name`—(Optional) Display information for all routing instances whose name begins with this string (for example, `cust1`, `cust11`, and `cust111` are all displayed when you run the `show route instance cust1` command).

`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

`operational`—(Optional) Display operational routing instances.

Required Privilege Level

`view`

List of Sample Output

`show route instance on page 3220`
`show route instance detail (Graceful Restart Complete) on page 3221`
`show route instance detail (Graceful Restart Incomplete) on page 3222`
`show route instance detail (VPLS Routing Instance) on page 3224`
`show route instance operational on page 3225`
`show route instance summary on page 3225`

Output Fields

Table 394 on page 3219 lists the output fields for the `show route instance` command. Output fields are listed in the approximate order in which they appear.

Table 394: show route instance Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance or <code>instance-name</code></td>
<td>Name of the routing instance.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 394: show route instance Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Routing Instances</td>
<td>(operational keyword only) Names of all operational routing instances.</td>
<td>—</td>
</tr>
<tr>
<td>Type</td>
<td>Type of routing instance: forwarding, l2vpn, no-forwarding, vpls, virtual-router, or vrf.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the routing instance: active or inactive.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Name of interfaces belonging to this routing instance.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Restart State</td>
<td>Status of graceful restart for this instance: Pending or Complete.</td>
<td>detail</td>
</tr>
<tr>
<td>Path selection timeout</td>
<td>Maximum amount of time, in seconds, remaining until graceful restart is declared complete. The default is 300.</td>
<td>detail</td>
</tr>
<tr>
<td>Tables</td>
<td>Tables (and number of routes) associated with this routing instance.</td>
<td>brief detail none</td>
</tr>
<tr>
<td>Route-distinguisher</td>
<td>Unique route distinguisher associated with this routing instance.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-import</td>
<td>VPN routing and forwarding instance import policy name.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-export</td>
<td>VPN routing and forwarding instance export policy name.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-import-target</td>
<td>VPN routing and forwarding instance import target community name.</td>
<td>detail</td>
</tr>
<tr>
<td>Vrf-export-target</td>
<td>VPN routing and forwarding instance export target community name.</td>
<td>detail</td>
</tr>
<tr>
<td>Fast-reroute-priority</td>
<td>Fast reroute priority setting for a VPLS routing instance: high, medium, or low. The default is low.</td>
<td>detail</td>
</tr>
<tr>
<td>Restart State</td>
<td>Restart state:</td>
<td>detail</td>
</tr>
<tr>
<td>Primary rib</td>
<td>Primary table for this routing instance.</td>
<td>brief none summary</td>
</tr>
<tr>
<td>Active/holddown/hidden</td>
<td>Number of active, hold-down, and hidden routes.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

### Sample Output

**show route instance**

```
user@host> show route instance
Instance   Type       Active/holddown/hidden
master     forwarding  16/0/1
inet.0
```
show route instance detail (Graceful Restart Complete)

user@host> show route instance detail
master:
  Router ID: 10.255.14.176
  Type: forwarding        State: Active
  Restart State: Complete Path selection timeout: 300
  Tables:
    inet.0        : 17 routes (15 active, 0 holddown, 1 hidden)
      Restart Complete
    inet.3        : 2 routes (2 active, 0 holddown, 0 hidden)
      Restart Complete
    iso.0         : 1 routes (1 active, 0 holddown, 0 hidden)
      Restart Complete
    mpls.0        : 19 routes (19 active, 0 holddown, 0 hidden)
      Restart Complete
    bgp.l3vpn.0   : 10 routes (10 active, 0 holddown, 0 hidden)
      Restart Complete
    inet6.0       : 2 routes (2 active, 0 holddown, 0 hidden)
      Restart Complete
    bgp.l2vpn.0   : 1 routes (1 active, 0 holddown, 0 hidden)
      Restart Complete

BGP-INET:
  Router ID: 10.69.103.1
  Type: vrf               State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.103
  Route-distinguisher: 10.255.14.176:103
  Vrf-import: [ BGP-INET-import ]
  Vrf-export: [ BGP-INET-export ]
  Tables:
    BGP-INET.inet.0        : 4 routes (4 active, 0 holddown, 0 hidden)
      Restart Complete

BGP-L:
  Router ID: 10.69.104.1
  Type: vrf               State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
    t3-0/0/0.104
  Route-distinguisher: 10.255.14.176:104
  Vrf-import: [ BGP-L-import ]
  Vrf-export: [ BGP-L-export ]
  Tables:
    BGP-L.inet.0           : 4 routes (4 active, 0 holddown, 0 hidden)
      Restart Complete
    BGP-L.mpls.0           : 3 routes (3 active, 0 holddown, 0 hidden)
      Restart Complete

L2VPN:
  Router ID: 0.0.0.0
  Type: l2vpn               State: Active
  Restart State: Complete Path selection timeout: 300
  Interfaces:
show route instance detail (Graceful Restart Incomplete)

user@host> show route instance detail
master:
  Router ID: 10.255.14.176
  Type: forwarding  State: Active
  Restart State: Pending  Path selection timeout: 300
  Tables:
  inet.0  : 17 routes (15 active, 1 holddown, 1 hidden)
    Restart Pending: OSPF LDP
  inet.3  : 2 routes (2 active, 0 holddown, 0 hidden)
    Restart Pending: OSPF LDP
  iso.0   : 1 routes (1 active, 0 holddown, 0 hidden)
    Restart Complete
  mpls.0  : 23 routes (23 active, 0 holddown, 0 hidden)
    Restart Pending: LDP VPN
  bgp.13vpn.0  : 10 routes (10 active, 0 holddown, 0 hidden)
    Restart Pending: BGP VPN
  inet6.0 : 2 routes (2 active, 0 holddown, 0 hidden)
  bgp.12vpn.0 : 1 routes (1 active, 0 holddown, 0 hidden)
  Restart Pending: BGP VPN
BGP-INET:
  Router ID: 10.69.103.1
  Type: vrf  State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.103
  Route-distinguisher: 10.255.14.176:103
  Vrf-import: [ BGP-INET-import ]
  Vrf-export: [ BGP-INET-export ]
  Tables:
    BGP-INET.inet.0 : 6 routes (5 active, 0 holddown, 0 hidden)
      Restart Pending: VPN
BGP-L:
  Router ID: 10.69.104.1
  Type: vrf  State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.104
  Route-distinguisher: 10.255.14.176:104
  Vrf-import: [ BGP-L-import ]
  Vrf-export: [ BGP-L-export ]
  Tables:
    BGP-L.inet.0 : 6 routes (5 active, 0 holddown, 0 hidden)
      Restart Pending: VPN
    BGP-L.mpls.0 : 2 routes (2 active, 0 holddown, 0 hidden)
      Restart Pending: VPN
L2VPN:
  Router ID: 0.0.0.0
  Type: l2vpn  State: Active
  Restart State: Pending  Path selection timeout: 300
  Interfaces:
    t3-0/0/0.512
  Route-distinguisher: 10.255.14.176:512
  Vrf-import: [ L2VPN-import ]
  Vrf-export: [ L2VPN-export ]
  Tables:
    L2VPN.l2vpn.0 : 2 routes (2 active, 0 holddown, 0 hidden)
      Restart Pending: VPN L2VPN
LDP:
  Router ID: 10.69.105.1
  Type: vrf  State: Active
  Restart State: Pending  Path selection timeout: 300
Interfaces:
  t3-0/0/0.105
  Route-distinguisher: 10.255.14.176:105
  Vrf-import: [ LDP-import ]
  Vrf-export: [ LDP-export ]
Tables:
  LDP.inet.0 : 5 routes (4 active, 1 holddown, 0 hidden)
  Restart Pending: OSPF LDP VPN

OSPF:
  Router ID: 10.69.101.1
  Type: vrf    State: Active
  Restart State: Pending  Path selection timeout: 300
Interfaces:
  t3-0/0/0.101
  Vrf-import: [ OSPF-import ]
  Vrf-export: [ OSPF-export ]
Tables:
  OSPF.inet.0 : 8 routes (7 active, 1 holddown, 0 hidden)
  Restart Pending: OSPF VPN

RIP:
  Router ID: 10.69.102.1
  Type: vrf    State: Active
  Restart State: Pending  Path selection timeout: 300
Interfaces:
  t3-0/0/0.102
  Vrf-import: [ RIP-import ]
  Vrf-export: [ RIP-export ]
Tables:
  RIP.inet.0 : 8 routes (6 active, 2 holddown, 0 hidden)
  Restart Pending: RIP VPN

STATIC:
  Router ID: 10.69.100.1
  Type: vrf    State: Active
  Restart State: Pending  Path selection timeout: 300
Interfaces:
  t3-0/0/0.100
  Route-distinguisher: 10.255.14.176:100
  Vrf-import: [ STATIC-import ]
  Vrf-export: [ STATIC-export ]
Tables:
  STATIC.inet.0 : 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Pending: VPN

show route instance detail (VPLS Routing Instance)
show route instance operational

user@host> show route instance operational
Operational Routing Instances:

master
default

show route instance summary

user@host> show route instance summary

<table>
<thead>
<tr>
<th>Instance</th>
<th>Type</th>
<th>Primary rib</th>
<th>Active/holddown/hidden</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>forwarding</td>
<td>inet.0</td>
<td>15/0/1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iso.0</td>
<td>1/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mpls.0</td>
<td>35/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>l3vpn.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>inet6.0</td>
<td>2/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>l2vpn.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>l2circuit.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>BGP-INET</td>
<td>vrf</td>
<td>BGP-INET.inet.0</td>
<td>5/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-INET.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-INET.inet6.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>BGP-L</td>
<td>vrf</td>
<td>BGP-L.inet.0</td>
<td>5/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-L.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-L.mpls.0</td>
<td>4/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BGP-L.inet6.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>L2VPN</td>
<td>l2vpn</td>
<td>L2VPN.inet.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2VPN.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2VPN.inet6.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2VPN.l2vpn.0</td>
<td>2/0/0</td>
</tr>
<tr>
<td>LDP</td>
<td>vrf</td>
<td>LDP.inet.0</td>
<td>4/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.mpls.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.inet6.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LDP.l2circuit.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>OSPF</td>
<td>vrf</td>
<td>OSPF.inet.0</td>
<td>7/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSPF.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSPF.inet6.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>RIP</td>
<td>vrf</td>
<td>RIP.inet.0</td>
<td>6/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RIP.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RIP.inet6.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td>STATIC</td>
<td>vrf</td>
<td>STATIC.inet.0</td>
<td>4/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>STATIC.iso.0</td>
<td>0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>STATIC.inet6.0</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>
**show route label**

**Syntax**

```
show route label
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**

```
show route label label
<brief | detail | extensive | terse>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.5 for EX Series switches.

**Description**

Display the routes based on a specified Multiprotocol Label Switching (MPLS) label value.

**Options**

- **label**—Value of the MPLS label.
- **brief | detail | extensive | terse**—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

- Level: view

**List of Sample Output**

- show route label on page 3226
- show route label detail on page 3226
- show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 3227
- show route label extensive on page 3227
- show route label terse on page 3227

**Output Fields**

For information about output fields, see the output field table for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

**Sample Output**

**show route label**

```
user@host> show route label 100016

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both
100016  *[VPN/170] 03:25:41
     > to 10.12.80.1 via ge-6/3/2.0, Pop
```

**show route label detail**

```
user@host> show route label 100016 detail

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
```
Restart Complete
100016 (1 entry, 1 announced)
  *VPN
    Preference: 170
    Next-hop reference count: 2
    Source: 10.12.80.1
    Next hop: 10.12.80.1 via ge-6/3/2.0, selected
    Label operation: Pop
    State: <Active Int Ext>
    Local AS: 1
    Age: 3:23:31
    Task: BGP.0.0.0.0+179
    Announcement bits (1): 0-KRT
    AS path: 100 I
    Ref Cnt: 2

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show route label 299872 detail
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
  *LDP
    Preference: 9
    Next hop type: Flood
    Next-hop reference count: 3
    Address: 0x9097d90
    Next hop: via vt-0/1/0.1
    Next-hop index: 661
    Label operation: Pop
    Address: 0x9172130
    Next hop: via so-0/0/3.0
    Next-hop index: 654
    Label operation: Swap 299872
    State: **Active Int>
    Local AS: 1001
    Age: 8:20       Metric: 1
    Task: LDP
    Announcement bits (1): 0-KRT
    AS path: I
    FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1, src 192.168.142.2

show route label extensive

The output for the show route label extensive command is identical to that of the show route label detail command. For sample output, see show route label detail on page 3226.

show route label terse

user@host> show route label 100016 terse
mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 100016</td>
<td>V 170</td>
<td></td>
<td></td>
<td>&gt;10.12.80.1</td>
<td></td>
</tr>
</tbody>
</table>
show route label-switched-path

Syntax

show route label-switched-path path-name
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show route label-switched-path path-name
  <brief | detail | extensive | terse>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.5 for EX Series switches.

Description

Display the routes used in an MPLS label-switched path (LSP).

Options

brief | detail | extensive | terse—(Optional) Display the specified level of output.

path-name—LSP tunnel name.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

Level

view

List of Sample Output

show route label-switched-path on page 3228

Output Fields

For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output

show route label-switched-path

user@host> show route label-switched-path sf-to-ny
inet.0: 29 destinations, 29 routes (29 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

1.1.1.1/32          [MPLS/7] 00:00:06, metric 0
  > to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

3.3.3.3/32         *[MPLS/7] 00:00:06, metric 0
  > to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

2.2.2.2/32         *[MPLS/7] 00:00:06, metric 0
  > to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

4.4.4.4/32         *[MPLS/7] 00:00:06, metric 0
  > to 111.222.1.9 via s0-0/0/0, label-switched-path abc
  > to 111.222.1.9 via s0-0/0/0, label-switched-path xyz
  > to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny

111.222.1.9/32      [MPLS/7] 00:00:06, metric 0
  > to 111.222.1.9 via s0-0/0/0, label-switched-path sf-to-ny
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

mpls.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
show route martians

**Syntax**

```
show route martians
<logical-system (all | logical-system-name)>
<table routing-table-name>
```

**Syntax (EX Series Switches)**

```
show route martians
<table routing-table-name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display the martian (invalid and ignored) entries associated with each routing table.

**Options**

- `none`—Display standard information about route martians for all routing tables.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `table routing-table-name`—(Optional) Display information about route martians for all routing tables whose name begins with this string (for example, `inet.0` and `inet6.0` are both displayed when you run the `show route martians table inet` command).

**Required Privilege Level**

view

**Related Documentation**

- Example: Configuring Martian Addresses

**List of Sample Output**

show route martians on page 3230

**Output Fields**

Table 395 on page 3230 lists the output fields for the `show route martians` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>table-name</code></td>
<td>Name of the route table in which the route martians reside.</td>
</tr>
<tr>
<td><code>destination-prefix</code></td>
<td>Route destination.</td>
</tr>
<tr>
<td><code>match-value</code></td>
<td>Route match parameter.</td>
</tr>
<tr>
<td><code>status</code></td>
<td>Status of the route: <code>allowed</code> or <code>disallowed</code>.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show route martians
```

```
user@host> show route martians
```
inet.0:
  0.0.0.0/0 exact -- allowed
  0.0.0.0/8 orlonger -- disallowed
  127.0.0.0/8 orlonger -- disallowed
  192.0.0.0/24 orlonger -- disallowed
  240.0.0.0/4 orlonger -- disallowed
  224.0.0.0/4 exact -- disallowed
  224.0.0.0/24 exact -- disallowed

inet.1:
  0.0.0.0/0 exact -- allowed
  0.0.0.0/8 orlonger -- disallowed
  127.0.0.0/8 orlonger -- disallowed
  192.0.0.0/24 orlonger -- disallowed
  240.0.0.0/4 orlonger -- disallowed

inet.2:
  0.0.0.0/0 exact -- allowed
  0.0.0.0/8 orlonger -- disallowed
  127.0.0.0/8 orlonger -- disallowed
  192.0.0.0/24 orlonger -- disallowed
  240.0.0.0/4 orlonger -- disallowed
  224.0.0.0/4 exact -- disallowed
  224.0.0.0/24 exact -- disallowed

inet.3:
  0.0.0.0/0 exact -- allowed
  0.0.0.0/8 orlonger -- disallowed
  127.0.0.0/8 orlonger -- disallowed
  192.0.0.0/24 orlonger -- disallowed
  240.0.0.0/4 orlonger -- disallowed
  224.0.0.0/4 exact -- disallowed
  224.0.0.0/24 exact -- disallowed

inet6.0:
  ::1/128 exact -- disallowed
  ff00::/8 exact -- disallowed
  ff02::/16 exact -- disallowed

inet6.1:
  ::1/128 exact -- disallowed

inet6.2:
  ::1/128 exact -- disallowed
  ff00::/8 exact -- disallowed
  ff02::/16 exact -- disallowed

inet6.3:
  ::1/128 exact -- disallowed
  ff00::/8 exact -- disallowed
  ff02::/16 exact -- disallowed

...
show route next-hop

**Syntax**
```
show route next-hop next-hop
   <brief | detail | extensive | terse>
   <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route next-hop next-hop
   <brief | detail | extensive | terse>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display the entries in the routing table that are being sent to the specified next-hop address.

**Options**
- `brief` | `detail` | `extensive` | `terse`—(Optional) Display the specified level of output.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**next-hop**—Next-hop address.

**Required Privilege Level**
```
view
```

**List of Sample Output**
- show route next-hop on page 3232
- show route next-hop detail on page 3233
- show route next-hop extensive on page 3235
- show route next-hop terse on page 3236

**Output Fields**
For information about output fields, see the output field tables for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

**Sample Output**
show route next-hop

```
user@host> show route next-hop 192.168.71.254

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

10.10.0.0/16   *[Static/5] 06:26:25
   > to 192.168.71.254 via fxp0.0
10.209.0.0/16  *[Static/5] 06:26:25
   > to 192.168.71.254 via fxp0.0
172.16.0.0/12  *[Static/5] 06:26:25
   > to 192.168.71.254 via fxp0.0
192.168.0.0/16 *[Static/5] 06:26:25
   > to 192.168.71.254 via fxp0.0
192.168.102.0/23 *[Static/5] 06:26:25
   > to 192.168.71.254 via fxp0.0
```

3232 Copyright © 2013, Juniper Networks, Inc.
show route next-hop detail

user@host> show route next-hop 192.168.71.254 detail

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
Restart Complete
10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

172.16.0.0/12 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 36
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 1
  Age: 6:27:41
  Task: RT
  Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2
  AS path: I

192.168.0.0/16 (1 entry, 1 announced)
*Static Preference: 5  
Next-hop reference count: 36  
Next hop: 192.168.71.254 via fxp0.0, selected  
State: <Active NoReadvrt Int Ext>  
Local AS:     1  
Age: 6:27:41  
Task: RT  
Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2  
AS path: I  

192.168.102.0/23 (1 entry, 1 announced)  
*Static Preference: 5  
Next-hop reference count: 36  
Next hop: 192.168.71.254 via fxp0.0, selected  
State: <Active NoReadvrt Int Ext>  
Local AS:     1  
Age: 6:27:41  
Task: RT  
Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2  
AS path: I  

207.17.136.0/24 (1 entry, 1 announced)  
*Static Preference: 5  
Next-hop reference count: 36  
Next hop: 192.168.71.254 via fxp0.0, selected  
State: <Active NoReadvrt Int Ext>  
Local AS:     1  
Age: 6:27:41  
Task: RT  
Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2  
AS path: I  

207.17.136.192/32 (1 entry, 1 announced)  
*Static Preference: 5  
Next-hop reference count: 36  
Next hop: 192.168.71.254 via fxp0.0, selected  
State: <Active NoReadvrt Int Ext>  
Local AS:     1  
Age: 6:27:41  
Task: RT  
Announcement bits (3): 0-KRT 3-Resolve tree 1 5-Resolve tree 2  
AS path: I  

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)  
red.inet.0: 4 destinations, 5 routes (4 active, 0 holddown, 0 hidden)  
Restart Complete  

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)  
Restart Complete  

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)  
Restart Complete  

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)  
Restart Complete  

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
show route next-hop extensive

user@host> show route next-hop 192.168.71.254 extensive

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.10.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.209.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

172.16.0.0/12 (1 entry, 1 announced)
TSI:
KRT in-kernel 172.16.0.0/12 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

192.168.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 192.168.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

192.168.102.0/23 (1 entry, 1 announced)
TSI:
KRT in-kernel 192.168.102.0/23 -> {192.168.71.254}
  *Static Preference: 5
Next-hop reference count: 22
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Local AS:    69
Age: 2:02:28
Task: RT
Announcement bits (1): 0-KRT
AS path: I

207.17.136.0/24 (1 entry, 1 announced)

TSI:
KRT in-kernel 207.17.136.0/24 --> {192.168.71.254}
  #Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS:    69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

207.17.136.192/32 (1 entry, 1 announced)

TSI:
KRT in-kernel 207.17.136.192/32 --> {192.168.71.254}
  #Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS:    69
  Age: 2:02:28
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
green.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
red.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

show route next-hop terse

user@host> show route next-hop 192.168.71.254 terse

inet.0: 25 destinations, 26 routes (24 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 10.10.0.16</td>
<td>S S</td>
<td></td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 10.209.0.16</td>
<td>S S</td>
<td></td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>* 172.16.0.12</td>
<td>S S</td>
<td></td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
</tbody>
</table>
* 192.168.0.0/16  S  S  >192.168.71.254
* 192.168.102.0/23  S  S  >192.168.71.254
* 207.17.136.0/24  S  S  >192.168.71.254
* 207.17.136.192/32  S  S  >192.168.71.254

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
red.inet.0: 4 destinations, 5 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete

mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Restart Complete

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
show route no-community

Syntax

show route no-community

Syntax (EX Series Switches)

show route no-community

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the route entries in each routing table that are not associated with any community.

Options

none—(Same as brief) Display the route entries in each routing table that are not associated with any community.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

Level

view

List of Sample Output

show route no-community on page 3238
show route no-community detail on page 3239
show route no-community extensive on page 3239
show route no-community terse on page 3240

Output Fields

For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output

show route no-community

user@host> show route no-community
inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.10.0.0/16  *[Static/5] 00:36:27
> to 192.168.71.254 via fxp0.0

10.209.0.0/16  *[Static/5] 00:36:27
> to 192.168.71.254 via fxp0.0

10.255.71.52/32  *[Direct/0] 00:36:27
> via lo0.0

10.255.71.63/32  *[OSPF/10] 00:04:39, metric 1
> to 35.1.1.2 via ge-3/1/0.0

10.255.71.64/32  *[OSPF/10] 00:00:08, metric 2
> to 35.1.1.2 via ge-3/1/0.0

10.255.71.240/32  *[OSPF/10] 00:05:04, metric 2
> via so-0/1/2.0
show route no-community detail

user@host> show route no-community detail

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Age: 38:08
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Age: 38:08
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

show route no-community extensive

user@host> show route no-community extensive

inet.0: 18 destinations, 18 routes (17 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.10.0.0/16 -> {192.168.71.254}
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Local AS: 69
  Age: 2:03:33
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.209.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.209.0.0/16 -> {192.168.71.254}
*Static Preference: 5
Next-hop reference count: 22
Next hop: 192.168.71.254 via fxp0.0, selected
State: <Active NoReadvrt Int Ext>
Local AS:    69
Age: 2:03:33
Task: RT
Announcement bits (1): 0-KRT
AS path: 1

show route no-community terse

user@host> show route no-community terse

inet.0: 28 destinations, 30 routes (27 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.0/16</td>
<td>S 5</td>
<td></td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>10.209.0.0/16</td>
<td>S 5</td>
<td></td>
<td></td>
<td>&gt;192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>10.255.71.32/32</td>
<td>D 0</td>
<td></td>
<td></td>
<td>&gt;lo0.0</td>
<td></td>
</tr>
<tr>
<td>10.255.71.63/32</td>
<td>0 10</td>
<td>1</td>
<td></td>
<td>&gt;35.1.1.2</td>
<td></td>
</tr>
<tr>
<td>10.255.71.64/32</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>&gt;35.1.1.2</td>
<td></td>
</tr>
<tr>
<td>10.255.71.240/32</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>so-0/1/2.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&gt;so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>10.255.71.241/32</td>
<td>0 10</td>
<td>1</td>
<td></td>
<td>&gt;so-0/1/2.0</td>
<td></td>
</tr>
<tr>
<td>10.255.71.242/32</td>
<td>0 10</td>
<td>1</td>
<td></td>
<td>&gt;so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>12.1.1.0/24</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>&gt;so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>14.1.1.0/24</td>
<td>0 10</td>
<td>3</td>
<td></td>
<td>&gt;35.1.1.2</td>
<td>so-0/1/2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>so-0/3/2.0</td>
<td></td>
</tr>
<tr>
<td>16.1.1.0/24</td>
<td>0 10</td>
<td>2</td>
<td></td>
<td>&gt;so-0/1/2.0</td>
<td></td>
</tr>
</tbody>
</table>
...
show route protocol

Syntax

show route protocol protocol
   <brief | detail | extensive | terse>
   <logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show route protocol protocol
   <brief | detail | extensive | terse>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
opsf2 and ospf3 options introduced in Junos OS Release 9.2.
opsf2 and ospf3 options introduced in Junos OS Release 9.2 for EX Series switches.
flow option introduced in Junos OS Release 10.0.
flow option introduced in Junos OS Release 10.0 for EX Series switches.

Description

Display the route entries in the routing table that were learned from a particular protocol.

Options

brief | detail | extensive | terse—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

protocol—Protocol from which the route was learned:

- access—Access route for use by DHCP application
- access-internal—Access-internal route for use by DHCP application
- aggregate—Locally generated aggregate route
- arp—Route learned through the Address Resolution Protocol
- atmvpn—Asynchronous Transfer Mode virtual private network
- bgp—Border Gateway Protocol
- ccc—Circuit cross-connect
- direct—Directly connected route
- dvmrp—Distance Vector Multicast Routing Protocol
- eisis—End System-to-Intermediate System
- flow—Locally defined flow-specification route
- frf—Precomputed protection route or backup route used when a link goes down
- isis—Intermediate System-to-Intermediate System
- ldp—Label Distribution Protocol
- l2circuit—Layer 2 circuit
- l2vpn—Layer 2 virtual private network
- **local**—Local address
- **mpls**—Multiprotocol Label Switching
- **msdp**—Multicast Source Discovery Protocol
- **ospf**—Open Shortest Path First versions 2 and 3
- **ospf2**—Open Shortest Path First versions 2 only
- **ospf3**—Open Shortest Path First version 3 only
- **pim**—Protocol Independent Multicast
- **rip**—Routing Information Protocol
- **ripng**—Routing Information Protocol next generation
- **rsvp**—Resource Reservation Protocol
- **rtarget**—Local route target virtual private network
- **static**—Statically defined route
- **tunnel**—Dynamic tunnel
- **vpn**—Virtual private network

---

**NOTE:** EX Series switches run a subset of these protocols. See the switch CLI for details.

<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>List of Sample Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>view</strong></td>
<td>show route protocol access on page 3243</td>
</tr>
<tr>
<td></td>
<td>show route protocol access-internal extensive on page 3243</td>
</tr>
<tr>
<td></td>
<td>show route protocol arp on page 3243</td>
</tr>
<tr>
<td></td>
<td>show route protocol bgp on page 3244</td>
</tr>
<tr>
<td></td>
<td>show route protocol bgp detail on page 3244</td>
</tr>
<tr>
<td></td>
<td>show route protocol bgp extensive on page 3244</td>
</tr>
<tr>
<td></td>
<td>show route protocol bgp terse on page 3245</td>
</tr>
<tr>
<td></td>
<td>show route protocol direct on page 3245</td>
</tr>
<tr>
<td></td>
<td>show route protocol frr on page 3246</td>
</tr>
<tr>
<td></td>
<td>show route protocol l2circuits detail on page 3246</td>
</tr>
<tr>
<td></td>
<td>show route protocol l2vpn on page 3247</td>
</tr>
<tr>
<td></td>
<td>show route protocol ldp on page 3248</td>
</tr>
<tr>
<td></td>
<td>show route protocol ldp extensive on page 3248</td>
</tr>
<tr>
<td></td>
<td>show route protocol ospf (Layer 3 VPN) on page 3249</td>
</tr>
<tr>
<td></td>
<td>show route protocol ospf detail on page 3250</td>
</tr>
<tr>
<td></td>
<td>show route protocol rip on page 3250</td>
</tr>
<tr>
<td></td>
<td>show route protocol rip detail on page 3250</td>
</tr>
<tr>
<td></td>
<td>show route protocol ripng table inet6 on page 3251</td>
</tr>
<tr>
<td></td>
<td>show route protocol static detail on page 3251</td>
</tr>
</tbody>
</table>
Output Fields  For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output

show route protocol access

user@host> show route protocol access
inet.0: 30380 destinations, 30382 routes (30379 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

13.160.0.3/32 *[Access/13] 00:00:09
  > to 13.160.0.2 via fe-0/0/0.0
13.160.0.4/32 *[Access/13] 00:00:09
  > to 13.160.0.2 via fe-0/0/0.0
13.160.0.5/32 *[Access/13] 00:00:09
  > to 13.160.0.2 via fe-0/0/0.0

show route protocol access-internal extensive

user@host> show route protocol access-internal 13.160.0.19 extensive
inet.0: 100020 destinations, 100022 routes (100019 active, 0 holddown, 1 hidden)
13.160.0.19/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.19/32 -> {13.160.0.2}
  *Access-internal Preference: 12
  Next-hop reference count: 200000
  Next hop: 13.160.0.2 via fe-0/0/0.0, selected
  State: <Active Int>
  Age: 36
  Task: RPD Unix Domain Server./var/run/rpd_serv.local
  Announcement bits (1): 0-KRT
  AS path: I

show route protocol arp

user@host> show route protocol arp
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)
inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.4/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.5/32 [ARP/4294967293] 00:04:32, from 20.20.1.1
  Unusable
20.20.1.6/32 [ARP/4294967293] 00:04:34, from 20.20.1.1
  Unusable
20.20.1.7/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.8/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.9/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
20.20.1.10/32 [ARP/4294967293] 00:04:35, from 20.20.1.1
  Unusable
show route protocol bgp

user@host> show route protocol bgp 192.168.64.0/21
inet.0: 335832 destinations, 335833 routes (335383 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.64.0/21 *[BGP/170] 6d 10:41:16, localpref 100, from 192.168.69.71
AS path: 10458 14203 2914 4788 4788 I
> to 192.168.167.254 via fxp0.0

show route protocol bgp detail

user@host> show route protocol bgp 66.117.63.0/24 detail
inet.0: 335805 destinations, 335806 routes (335356 active, 0 holddown, 450 hidden)
66.117.63.0/24 (1 entry, 1 announced)
*BGP Preference: 170/-101
Next hop type: Indirect
Next-hop reference count: 1006436
Source: 192.168.69.71
Next hop type: Router, Next hop index: 324
Next hop: 192.168.167.254 via fxp0.0, selected
Protocol next hop: 192.168.69.71
Indirect next hop: 8e166c0 342
State: <Active Ext>
Local AS: 69 Peer AS: 10458
Age: 6d 10:42:42 Metric2: 0
Task: BGP_10458.192.168.69.71+179
Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree
1
AS path: 10458 14203 2914 4788 4788 I
Communities: 2914:410 2914:2403 2914:3400
Accepted
Localpref: 100
Router ID: 207.17.136.192

show route protocol bgp extensive

user@host> show route protocol bgp 192.168.64.0/21 extensive
inet.0: 335827 destinations, 335828 routes (335378 active, 0 holddown, 450 hidden)
192.168.64.0/21 (1 entry, 1 announced)
TSI:
KRT in-kernel 1.9.0.0/16 -> {indirect(342)}
Page 0 idx 1 Type 1 val db31a80
Nexthop: Self
AS path: [69] 10458 14203 2914 4788 4788 I
Communities: 2914:410 2914:2403 2914:3400
Path 1.9.0.0 from 192.168.69.71 Vector len 4. Val: 1
*BGP Preference: 170/-101
Next hop type: Indirect
Next-hop reference count: 1000502
Source: 192.168.69.71
Next hop type: Router, Next hop index: 324
Next hop: 192.168.167.254 via fxp0.0, selected
Protocol next hop: 192.168.69.71
Indirect next hop: 8e166c0 342
State: <Active Ext>
Local AS: 69 Peer AS: 10458
Age: 6d 10:44:45 Metric2: 0
Task: BGP_10458.192.168.69.71+179
Announcement bits (3): 0-krt 2-bgp rt Background 3-resolve tree
1
AS path: 10458 14203 2914 4788 4788 I
Communities: 2914:410 2914:2403 2914:3400
Accepted
Localpref: 100
Router ID: 207.17.136.192
Indirect next hops: 1
Protocol next hop: 192.168.69.71
Indirect next hop: 8e166c0 342
Indirect path forwarding next hops: 1
Next hop type: Router
Next hop: 192.168.167.254 via fxp0.0
192.168.0.0/16 Originating RIB: inet.0
Node path count: 1
Forwarding nexthops: 1
Nexthop: 192.168.167.254 via fxp0.0

show route protocol bgp terse

user@host> show route protocol bgp 192.168.64.0/21 terse

inet.0: 24 destinations, 32 routes (23 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
A Destination P Prf Metric1 Metric2 Next hop AS path
192.168.64.0/21 B 170 100 >100.1.3.2 10023 21 I

show route protocol direct

user@host> show route protocol direct

inet.0: 335843 destinations, 335844 routes (335394 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both
8.8.8.0/24 *[Direct/0] 17w0d 10:31:49
> via fe-1/3/1.0
10.255.165.1/32 *[Direct/0] 25w4d 04:13:18
> via lo0.0
30.30.30.0/24 *[Direct/0] 17w0d 23:06:26
> via fe-1/3/2.0
192.168.164.0/22 *[Direct/0] 25w4d 04:13:20
> via fxp0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
47.0005.80ff.800.0000.0108.0001.0102.5516.5001/152
*[Direct/0] 25w4d 04:13:21
> via lo0.0

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
abcd::10:255:165:1/128
  *[Direct/0] 25w4d 04:13:21
    > via lo0.0

fe80::2a0:a5ff:fe12:ad7/128
  *[Direct/0] 25w4d 04:13:21
    > via lo0.0

show route protocol frr

user@host> show route protocol frr
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)
inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
  + = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>20.20.1.3/32</th>
<th>*[FRR/200] 00:05:38, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; to 20.20.1.3 via ge-4/1/0.0</td>
</tr>
<tr>
<td></td>
<td>&gt; to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.20.1.4/32</th>
<th>*[FRR/200] 00:05:38, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; to 20.20.1.4 via ge-4/1/0.0</td>
</tr>
<tr>
<td></td>
<td>&gt; to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.20.1.5/32</th>
<th>*[FRR/200] 00:05:35, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; to 20.20.1.5 via ge-4/1/0.0</td>
</tr>
<tr>
<td></td>
<td>&gt; to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.20.1.6/32</th>
<th>*[FRR/200] 00:05:37, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; to 20.20.1.6 via ge-4/1/0.0</td>
</tr>
<tr>
<td></td>
<td>&gt; to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.20.1.7/32</th>
<th>*[FRR/200] 00:05:38, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; to 20.20.1.7 via ge-4/1/0.0</td>
</tr>
<tr>
<td></td>
<td>&gt; to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.20.1.8/32</th>
<th>*[FRR/200] 00:05:38, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; to 20.20.1.8 via ge-4/1/0.0</td>
</tr>
<tr>
<td></td>
<td>&gt; to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.20.1.9/32</th>
<th>*[FRR/200] 00:05:38, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>&gt; to 20.20.1.9 via ge-4/1/0.0</td>
</tr>
<tr>
<td></td>
<td>&gt; to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>20.20.1.10/32</th>
<th>*[FRR/200] 00:05:38, from 20.20.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>

show route protocol l2circuit detail

user@host> show route protocol l2circuit detail
mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
1000000 (1 entry, 1 announced)
  *L2Ckt Preference: 7
    Next hop: via ge-2/0/0.0, selected
    Label operation: Pop Offset: 4
    State: <Active Int>
    Local AS: 99
    Age: 9:52
    Task: Common L2 VC
    Announcement bits (1): 0-KRT
    AS path: I

ge-2/0/0.0 (1 entry, 1 announced)
  *L2Ckt Preference: 7
    Next hop: via so-1/1/2.0 weight 1, selected
    Label-switched-path my-lsp
Label operation: Push 100000, Push 100000(top)[0] Offset: -4
Protocol next hop: 10.245.255.63
Push 100000 Offset: -4
Indirect next hop: 86af0c0 298
State: <Active Int>
Local AS: 99
Age: 9:52
Task: Common L2 VC
Announcement bits (2): 0-KRT 1-Common L2 VC
AS path: I

12circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  *L2CKT Preference: 7
  Next hop: via so-1/1/2.0 weight 1, selected
  Label-switched-path my-lsp
  Label operation: Push 100000[0]
  Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
  State: <Active Int>
  Local AS: 99
  Age: 10:21
  Task: l2 circuit
  Announcement bits (1): 0-LDP
  AS path: I
  VC Label 100000, MTU 1500, VLAN ID 512

show route protocol l2vpn extensive

user@host> show route protocol l2vpn extensive

inet.0: 14 destinations, 15 routes (13 active, 0 holddown, 1 hidden)
inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)

800001 (1 entry, 1 announced)
  TSI:
  KRT in-kernel 800001 /36 -> {so-0/0/0.0}
    *L2VPN Preference: 7
    Next hop: via so-0/0/0.0 weight 49087 balance 97%, selected
    Label operation: Pop Offset: 4
    State: <Active Int>
    Local AS: 69
    Age: 7:48
    Task: Common L2 VC
    Announcement bits (1): 0-KRT
    AS path: I

so-0/0/0.0 (1 entry, 1 announced)
  TSI:
  KRT in-kernel so-0/0/0.0 /16 -> {indirect(288)}
    *L2VPN Preference: 7
    Next hop: via so-0/0/1.0, selected
    Label operation: Push 800000 Offset: -4
    Push 800000 Offset: -4
    Indirect next hop: 85142a0 288
    State: <Active Int>
Local AS: 69
Age: 7:48
Task: Common L2 VC
Announcement bits (2): 0-KRT 1-Common L2 VC
AS path: I
Communities: target:69:1 Layer2-info: encaps:PPP,
control flags:2, mtu: 0

show route protocol ldp

user@host> show route protocol ldp
inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.16.1/32 *[LDP/9] 1d 23:03:35, metric 1
  > via t1-4/0/0.0, Push 100000
192.168.17.1/32 *[LDP/9] 1d 23:03:35, metric 1
  > via t1-4/0/0.0

private1__.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
100064 *[LDP/9] 1d 23:03:35, metric 1
  > via t1-4/0/0.0, Pop
100064(S=0) *[LDP/9] 1d 23:03:35, metric 1
  > via t1-4/0/0.0, Pop
100080 *[LDP/9] 1d 23:03:35, metric 1
  > via t1-4/0/0.0, Swap 100000

show route protocol ldp extensive

user@host> show route protocol ldp extensive
192.168.16.1/32 (1 entry, 1 announced)
  State: <FlashAll>
    *LDP  Preference: 9
    Next-hop reference count: 3
    Next hop: via t1-4/0/0.0, selected
    Label operation: Push 100000
    State: <Active Int>
    Local AS: 65500
    Age: 1d 23:03:58  Metric: 1
    Task: LDP
    Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
    AS path: I

192.168.17.1/32 (1 entry, 1 announced)
  State: <FlashAll>
    *LDP  Preference: 9
    Next-hop reference count: 3
    Next hop: via t1-4/0/0.0, selected
    State: <Active Int>
    Local AS: 65500
    Age: 1d 23:03:58  Metric: 1
    Task: LDP
    Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
    AS path: I
show route protocol ospf (Layer 3 VPN)

user@host> show route protocol ospf
inet.0: 40 destinations, 40 routes (39 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.4/30    *[OSPF/10] 00:05:18, metric 4
    > via t3-3/2/0.0
10.39.1.8/30    *[OSPF/10] 00:05:18, metric 2
    > via t3-3/2/0.0
10.255.14.171/32 *[OSPF/10] 00:05:18, metric 4
    > via t3-3/2/0.0
10.255.14.179/32 *[OSPF/10] 00:05:18, metric 2
    > via t3-3/2/0.0

Copyright © 2013, Juniper Networks, Inc.
show route protocol ospf detail

user@host> show route protocol ospf detail
VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30 (2 entries, 0 announced)
OSPF Preference: 10
Nexthop: via so-0/2/2.0, selected
State: <Int>
Inactive reason: Route Preference
Age: 6:25 Metric: 1
Area: 0.0.0.0
Task: VPN-AB-OSPF
AS path: I
Communities: Route-Type:0.0.0.0:1:0

show route protocol rip

user@host> show route protocol rip
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32 *RIP Preference: 100
Nexthop: 10.39.1.22 via t3-0/2/2.0, selected
State: <Active Int>
Age: 20:25:02 Metric: 2
Task: VPN-AB-RIPv2
Announcement bits (2): 0-KRT 2-BGP.0.0.0.0+179
AS path: I
Route learned from 10.39.1.22 expires in 96 seconds

show route protocol rip detail

user@host> show route protocol rip detail
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32 *RIP Preference: 100
Nexthop: 10.39.1.22 via t3-0/2/2.0, selected
State: <Active Int>
Age: 20:25:02 Metric: 2
Task: VPN-AB-RIPv2
Announcement bits (2): 0-KRT 2-BGP.0.0.0.0+179
AS path: I
Route learned from 10.39.1.22 expires in 96 seconds
show route protocol ripng table inet6

user@host> show route protocol ripng table inet6
inet6.0: 4215 destinations, 4215 routes (4214 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

1111::1/128        *[RIPng/100] 02:13:33, metric 2
> to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::2/128        *[RIPng/100] 02:13:33, metric 2
> to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::3/128        *[RIPng/100] 02:13:33, metric 2
> to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::4/128        *[RIPng/100] 02:13:33, metric 2
> to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::5/128        *[RIPng/100] 02:13:33, metric 2
> to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::6/128        *[RIPng/100] 02:13:33, metric 2
> to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0

show route protocol static detail

user@host> show route protocol static detail
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

10.5.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.10.0.0/16 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

10.13.10.0/23 (1 entry, 1 announced)
  *Static Preference: 5
  Next hop type: Router, Next hop index: 324
  Address: 0x9274010
  Next-hop reference count: 27
  Next hop: 192.168.187.126 via fxp0.0, selected
  Session Id: 0x0
  State: <Active NoReadvrt Int Ext>
  Age: 7w3d 21:24:25
  Validation State: unverified
Task: RT
Announcement bits (1): 0-KRT
AS path: I
**show route range**

**Syntax**

```
show route range
  <brief | detail | extensive | terse>
  <destination-prefix>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**

```
show route range
  <brief | detail | extensive | terse>
  <destination-prefix>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display routing table entries using a prefix range.

**Options**

- **none**—Display standard information about all routing table entries using a prefix range.
- **brief | detail | extensive | terse**—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to **brief**.
- **destination-prefix**—(Optional) Destination and prefix mask for the range.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

- view

**List of Sample Output**

- `show route range on page 3253`
- `show route range destination-prefix on page 3254`
- `show route range detail on page 3254`
- `show route range extensive on page 3255`
- `show route range terse on page 3256`

**Output Fields**

For information about output fields, see the output field tables for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

**Sample Output**

```
show route range

user@host> show route range

inet.0: 11 destinations, 11 routes (10 active, 0 holddown, 1 hidden)
  + = Active Route, - = Last Active, * = Both

10.10.0.0/16  *[Static/5]  00:30:01
  > to 192.168.71.254 via fxp0.0
10.209.0.0/16  *[Static/5]  00:30:01
  > to 192.168.71.254 via fxp0.0
10.255.71.14/32  *[Direct/0]  00:30:01
  > via lo0.0
```
172.16.0.0/12  *[Static/5] 00:30:01
    > to 192.168.71.254 via fxp0.0
192.168.0.0/16  *[Static/5] 00:30:01
    > to 192.168.71.254 via fxp0.0
192.168.64.0/21  *[Direct/0] 00:30:01
    > via fxp0.0
192.168.71.14/32  *[Local/0] 00:30:01
    Local via fxp0.0
192.168.102.0/23  *[Static/5] 00:30:01
    > to 192.168.71.254 via fxp0.0
...
AS path: I

172.16.0.0/12 (1 entry, 1 announced)
  *Static Preference: 5
  Next-hop reference count: 22
  Next hop: 192.168.71.254 via fxp0.0, selected
  State: <Active NoReadvrt Int Ext>
  Age: 30:05
  Task: RT
  Announcement bits (1): 0-KRT
  AS path: I

...
show route range terse

user@host> show route range terse

inet.0: 11 destinations, 11 routes (10 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.0/16</td>
<td>S</td>
<td>5</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>10.209.0.0/16</td>
<td>S</td>
<td>5</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>10.255.71.14/32</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>172.16.0.0/12</td>
<td>S</td>
<td>5</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>192.168.0.0/16</td>
<td>S</td>
<td>5</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>192.168.64.0/21</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>192.168.71.14/32</td>
<td>L</td>
<td>0</td>
<td></td>
<td></td>
<td>Local</td>
<td></td>
</tr>
<tr>
<td>192.168.102.0/23</td>
<td>S</td>
<td>5</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>207.17.136.0/24</td>
<td>S</td>
<td>5</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
<tr>
<td>207.17.136.192/32</td>
<td>S</td>
<td>5</td>
<td></td>
<td></td>
<td>192.168.71.254</td>
<td></td>
</tr>
</tbody>
</table>

juniper_private1_.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>fxp2.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>fxp1.0</td>
<td></td>
</tr>
<tr>
<td>10.0.0.4/32</td>
<td>L</td>
<td>0</td>
<td></td>
<td></td>
<td>Local</td>
<td></td>
</tr>
</tbody>
</table>

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>47.0005.80ff.f800.0000.0108.0001.0102.5507.1014/152</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>lo0.0</td>
<td></td>
</tr>
</tbody>
</table>

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>abcd:10:255:71:14/128</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>lo0.0</td>
<td></td>
</tr>
<tr>
<td>fe80:280:42ff:fell:226f/128</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>lo0.0</td>
<td></td>
</tr>
</tbody>
</table>

juniper_private1_.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

<table>
<thead>
<tr>
<th>A Destination</th>
<th>P</th>
<th>Prf</th>
<th>Metric 1</th>
<th>Metric 2</th>
<th>Next hop</th>
<th>AS path</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80:280:42ff:fell:226f/128</td>
<td>D</td>
<td>0</td>
<td></td>
<td></td>
<td>lo0.16385</td>
<td></td>
</tr>
</tbody>
</table>
**show route receive-protocol**

**Syntax**

```
show route receive-protocol protocol neighbor-address

<b brief | detail | extensive | terse>

<logical-system (all | logical-system-name)
```

**Syntax (EX Series Switches)**

```
show route receive-protocol protocol neighbor-address

<b brief | detail | extensive | terse>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display the routing information as it was received through a particular neighbor using a particular dynamic routing protocol.

**Options**

`brief | detail | extensive | terse`—(Optional) Display the specified level of output.

`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

`protocol neighbor-address`—Protocol transmitting the route (`bgp`, `dvmrp`, `msdp`, `pim`, `rip`, or `ripng`) and address of the neighboring router from which the route entry was received.

**Additional Information**

The output displays the selected routes and the attributes with which they were received, but does not show the effects of import policy on the routing attributes.

**Required Privilege**

`view`

**List of Sample Output**

- show route receive-protocol bgp on page 3260
- show route receive-protocol bgp extensive on page 3260
- show route receive-protocol bgp table extensive on page 3260
- show route receive-protocol bgp logical-system extensive on page 3261
- show route receive-protocol bgp detail (Layer 2 VPN) on page 3262
- show route receive-protocol bgp extensive (Layer 2 VPN) on page 3262
- show route receive-protocol bgp (Layer 3 VPN) on page 3263
- show route receive-protocol bgp detail (Layer 3 VPN) on page 3263
- show route receive-protocol bgp extensive (Layer 3 VPN) on page 3264

**Output Fields**

Table 396 on page 3257 describes the output fields for the `show route receive-protocol` command. Output fields are listed in the approximate order in which they appear.

**Table 396: show route receive-protocol Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table—for example, inet.0.</td>
<td>All levels</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 396: show route receive-protocol Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• holddown (routes that are in pending state before being declared inactive)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy)</td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>Destination prefix.</td>
<td>none brief</td>
</tr>
<tr>
<td>MED</td>
<td>Multiple exit discriminator value included in the route.</td>
<td>none brief</td>
</tr>
<tr>
<td>destination-prefix (entry, announced)</td>
<td>Destination prefix. The <em>entry</em> value is the number of routes for this destination, and the <em>announced</em> value is the number of routes being announced for this destination.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Route Distinguisher</td>
<td>64-bit prefix added to IP subnets to make them unique.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Label-Base, range</td>
<td>First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>VPN Label</td>
<td>Virtual private network (VPN) label. Packets are sent between CE and PE routing devices by advertising VPN labels. VPN labels transit over either an RSVP or an LDP label-switched path (LSP) tunnel.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Next hop</td>
<td>Next hop to the destination. An angle bracket (&gt;) indicates that the route is the selected route.</td>
<td>All levels</td>
</tr>
<tr>
<td>Localpref or Lclpref</td>
<td>Local preference value included in the route.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 396: show route receive-protocol Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
</table>
| AS path    | Autonomous system (AS) path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:  
  • I—IGP.  
  • E—EGP.  
  • ?—Incomplete; typically, the AS path was aggregated.  
  When AS path numbers are included in the route, the format is as follows:  
  • [ ]—Brackets enclose the number that precedes the AS path. This number represents the number of ASs present in the AS path, when calculated as defined in RFC 4271. This value is used the AS-path merge process, as defined in RFC 4893.  
  • [ ]—If more than one AS number is configured on the router, or if AS path prepending is configured, brackets enclose the local AS number associated with the AS path.  
  • { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order.  
  • ( )—Parentheses enclose a confederation.  
  • ( [ ] )—Parentheses and brackets enclose a confederation set.  
  NOTE: In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance. | All levels |
| Cluster list | (For route reflected output only) Cluster ID sent by the route reflector. | detail extensive |
| Originator ID | (For route reflected output only) Address of routing device that originally sent the route to the route reflector. | detail extensive |
| Communities | Community path attribute for the route. See the Output Field table in the show route detail command for all possible values for this field. | detail extensive |
| AIGP | Accumulated interior gateway protocol (AIGP) BGP attribute. | detail extensive |
| Attrset AS | Number, local preference, and path of the AS that originated the route. These values are stored in the Attrset attribute at the originating routing device. | detail extensive |
| Layer2-info: encaps | Layer 2 encapsulation (for example, VPLS). | detail extensive |
| control flags | Control flags: none or Site Down. | detail extensive |
| mtu | Maximum transmission unit (MTU) of the Layer 2 circuit. | detail extensive |
Sample Output

show route receive-protocol bgp

user@host> show route receive-protocol bgp 10.255.245.215

inet.0: 28 destinations, 33 routes (27 active, 0 holddown, 1 hidden)

Prefix              Next hop                MED    Lclpref AS path
10.22.1.0/24        10.255.245.215       0       100        I
10.22.2.0/24        10.255.245.215       0       100        I

show route receive-protocol bgp extensive

user@host> show route receive-protocol bgp 10.255.245.63 extensive

inet.0: 244 destinations, 244 routes (243 active, 0 holddown, 1 hidden)

Prefix              Next hop                MED    Lclpref AS path
1.1.1.0/24 (1 entry, 1 announced)
   Next hop: 10.0.50.3
   Localpref: 100
   AS path: I <Originator>
   Cluster list:  10.2.3.1
   Originator ID: 10.255.245.45
165.3.0.0/16 (1 entry, 1 announced)
   Next hop: 111.222.5.254
   Localpref: 100
   AS path: I <Originator>
   Cluster list:  10.2.3.1
   Originator ID: 10.255.245.68
165.4.0.0/16 (1 entry, 1 announced)
   Next hop: 111.222.5.254
   Localpref: 100
   AS path: I <Originator>
   Cluster list:  10.2.3.1
   Originator ID: 10.255.245.45
195.1.2.0/24 (1 entry, 1 announced)
   Next hop: 111.222.5.254
   Localpref: 100
   AS path: I <Originator>
   Cluster list:  10.2.3.1
   Originator ID: 10.255.245.68

inet.2: 63 destinations, 63 routes (63 active, 0 holddown, 0 hidden)

show route receive-protocol bgp table extensive

user@host> show route receive-protocol bgp 207.17.136.192 table

inet.0: 227315 destinations, 227316 routes (227302 active, 0 holddown, 13 hidden)
* 66.117.63.0/24 (1 entry, 1 announced)
   Next hop: 207.17.136.29
   Localpref: 100
   AS path: AS2 PA[6]: 14203 2914 3356 29748 33437 AS_TRANS
   AS path: AS4 PA[2]: 33437 393219
   AS path: Merged[6]: 14203 2914 3356 29748 33437 393219 I
   Communities: 2914:420
show route receive-protocol bgp logical-system extensive

user@host> show route receive-protocol bgp 10.0.0.9 logical-system PE4 extensive
inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)
  * 10.0.0.0/30 (1 entry, 1 announced)
    Accepted
    Route Label: 3
    Nexthop: 10.0.0.9
    AS path: 13979 I

  * 10.0.0.4/30 (1 entry, 1 announced)
    Accepted
    Route Label: 3
    Nexthop: 10.0.0.9
    AS path: 13979 I

  10.0.0.8/30 (2 entries, 1 announced)
    Accepted
    Route Label: 3
    Nexthop: 10.0.0.9
    AS path: 13979 I

  * 10.9.9.1/32 (1 entry, 1 announced)
    Accepted
    Route Label: 3
    Nexthop: 10.0.0.9
    AS path: 13979 I

  * 10.100.1.1/32 (1 entry, 1 announced)
    Accepted
    Route Label: 3
    Nexthop: 10.0.0.9
    AS path: 13979 I

  * 44.0.0.0/24 (1 entry, 1 announced)
    Accepted
    Route Label: 300096
    Nexthop: 10.0.0.9
    AS path: 13979 I
    AIGP: 203

  * 55.0.0.0/24 (1 entry, 1 announced)
    Accepted
    Route Label: 300112
    Nexthop: 10.0.0.9
    AS path: 13979 7018 I
    AIGP: 25

  * 66.0.0.0/24 (1 entry, 1 announced)
    Accepted
    Route Label: 300144
    Nexthop: 10.0.0.9
    AS path: 13979 7018 I

  * 99.0.0.0/24 (1 entry, 1 announced)
    Accepted
    Route Label: 300160
    Nexthop: 10.0.0.9
    AS path: 13979 7018 I
show route receive-protocol bgp detail (Layer 2 VPN)

user@host> show route receive-protocol bgp 10.255.14.171 detail
inet.0: 68 destinations, 68 routes (67 active, 0 holddown, 1 hidden)
Prefix Nexthop MED Lclpref AS path
inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
mpls.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
frame-vpn.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
10.255.245.35:1:5:1/96 (1 entry, 1 announced)
  Route Distinguisher: 10.255.245.35:1
  Label-base : 800000, range : 4, status-vector : 0x0
  Nexthop: 10.255.245.35
  Localpref: 100
  AS path: I
  Communities: target:65299:100 Layer2-info: encaps:FRAME RELAY, control flags: 0, mtu: 0
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
10.255.245.35:1:5:1/96 (1 entry, 0 announced)
  Route Distinguisher: 10.255.245.35:1
  Label-base : 800000, range : 4, status-vector : 0x0
  Nexthop: 10.255.245.35
  Localpref: 100
  AS path: I
  Communities: target:65299:100 Layer2-info: encaps:FRAME RELAY, control flags: 0, mtu: 0

show route receive-protocol bgp extensive (Layer 2 VPN)

user@host> show route receive-protocol bgp 10.255.14.171 extensive
inet.0: 68 destinations, 68 routes (67 active, 0 holddown, 1 hidden)
Prefix Nexthop MED Lclpref AS path
inet.3: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
mpls.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
frame-vpn.l2vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
10.255.245.35:1:5:1/96 (1 entry, 1 announced)
  Route Distinguisher: 10.255.245.35:1
  Label-base : 800000, range : 4, status-vector : 0x0
  Nexthop: 10.255.245.35
  Localpref: 100
  AS path: I
  Communities: target:65299:100 Layer2-info: encaps:FRAME RELAY, control flags: 0, mtu: 0
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix Nexthop MED Lclpref AS path
10.255.245.35:1:5:1/96 (1 entry, 0 announced)
  Route Distinguisher: 10.255.245.35:1
  Label-base : 800000, range : 4, status-vector : 0x0
  Nexthop: 10.255.245.35
  Localpref: 100
show route receive-protocol bgp (Layer 3 VPN)

user@host> show route receive-protocol bgp 10.255.14.171
inget.0: 33 destinations, 33 routes (32 active, 0 holddown, 1 hidden)
Prefix      Nexthop        MED    Lclpref AS path
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
Prefix      Nexthop        MED    Lclpref AS path
VPN-A.inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
Prefix      Nexthop        MED    Lclpref AS path
VPN-B.inet.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
Prefix      Nexthop        MED    Lclpref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix      Nexthop        MED    Lclpref AS path
mpls.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
Prefix      Nexthop        MED    Lclpref AS path
bgp.l3vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Prefix      Nexthop        MED    Lclpref AS path
  10.255.14.171  100 I
  10.255.14.171  2    100 I
  10.255.14.171  100 2 I

show route receive-protocol bgp detail (Layer 3 VPN)

user@host> show route receive-protocol bgp 10.255.14.174 detail
inet.0: 16 destinations, 17 routes (15 active, 0 holddown, 1 hidden)
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
vpna.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
  * 10.49.0.0/30 (1 entry, 1 announced)
    Route Distinguisher: 10.255.14.176:2
    VPN Label: 101264
    Nexthop: 10.255.14.174
    Localpref: 100
    AS path: I
    Communities: target:200:100
    AttrSet AS: 100
    Localpref: 100
    AS path: I
  * 10.255.14.172/32 (1 entry, 1 announced)
    Route Distinguisher: 10.255.14.176:2
    VPN Label: 101280
    Nexthop: 10.255.14.174
    Localpref: 100
    AS path: I
    Communities: target:200:100
    AttrSet AS: 100
    Localpref: 100
    AS path: I
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
bgp.l3vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
show route receive-protocol bgp extensive (Layer 3 VPN)

inet.0: 244 destinations, 244 routes (243 active, 0 holddown, 1 hidden)
Prefix            Nexthop                MED    Lclpref AS path
1.1.1.0/24 (1 entry, 1 announced)
  Nexthop: 10.0.50.3
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.45
165.3.0.0/16 (1 entry, 1 announced)
  Nexthop: 111.222.5.254
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.68
165.4.0.0/16 (1 entry, 1 announced)
  Nexthop: 111.222.5.254
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.45
195.1.2.0/24 (1 entry, 1 announced)
  Nexthop: 111.222.5.254
  Localpref: 100
  AS path: I <Originator>
  Cluster list: 10.2.3.1
  Originator ID: 10.255.245.68
inet.2: 63 destinations, 63 routes (63 active, 0 holddown, 0 hidden)
Prefix            Nexthop                MED    Lclpref AS path
inet.3: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
Prefix            Nexthop                MED    Lclpref AS path
iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Prefix            Nexthop                MED    Lclpref AS path
mpls.0: 48 destinations, 48 routes (48 active, 0 holddown, 0 hidden)
**show route resolution**

**Syntax**

```
show route resolution
<brief | detail | extensive | summary>
<index index>
<logical-system (all | logical-system-name)>
<prefix>
<table routing-table-name>
<unresolved>
```

**Syntax (EX Series Switches)**

```
show route resolution
<brief | detail | extensive | summary>
<index index>
<prefix>
<table routing-table-name>
<unresolved>
```

**Release Information**


**Description**

Display the entries in the next-hop resolution database. This database provides for recursive resolution of next hops through other prefixes in the routing table.

**Options**

`none`—Display standard information about all entries in the next-hop resolution database.

`brief | detail | extensive | summary`—(Optional) Display the specified level of output.

`index index`—(Optional) Show the index of the resolution tree.

`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

`prefix network/destination-prefix`—(Optional) Display database entries for the specified address.

`table routing-table-name`—(Optional) Display information about a particular routing table (for example, `inet.0`) where policy-based export is currently enabled.

`unresolved`—(Optional) Display routes that could not be resolved.

**Required Privilege Level**

view

**Related Documentation**

- Example: Configuring Route Resolution on PE Routers

**List of Sample Output**

- show route resolution detail on page 3266
- show route resolution summary on page 3267
- show route resolution unresolved on page 3267
**Output Fields**  
Table 397 on page 3266 describes the output fields for the `show route resolution` command. Output fields are listed in the approximate order in which they appear.

### Table 397: show route resolution Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>routing-table-name</code></td>
<td>Name of the routing table whose prefixes are resolved using the entries in the route resolution database. For routing table groups, this is the name of the primary routing table whose prefixes are resolved using the entries in the route resolution database.</td>
</tr>
<tr>
<td>Tree index</td>
<td>Tree index identifier.</td>
</tr>
<tr>
<td>Nodes</td>
<td>Number of nodes in the tree.</td>
</tr>
<tr>
<td>Reference count</td>
<td>Number of references made to the next hop.</td>
</tr>
<tr>
<td>Contributing routing tables</td>
<td>Routing tables used for next-hop resolution.</td>
</tr>
<tr>
<td>Originating RIB</td>
<td>Name of the routing table whose active route was used to determine the forwarding next-hop entry in the resolution database. For example, in the case of <code>inet.0</code> resolving through <code>inet.0</code> and <code>inet.3</code>, this field indicates which routing table, <code>inet.0</code> or <code>inet.3</code>, provided the best path for a particular prefix.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric associated with the forwarding next hop.</td>
</tr>
<tr>
<td>Node path count</td>
<td>Number of nodes in the path.</td>
</tr>
<tr>
<td>Forwarding next hops</td>
<td>Number of forwarding next hops. The forwarding next hop is the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.</td>
</tr>
</tbody>
</table>

**Sample Output**

table route resolution detail

```
user@host> show route resolution detail
Tree Index: 1, Nodes 0, Reference Count 1
Contributing routing tables: inet.3
Tree Index: 2, Nodes 23, Reference Count 1
Contributing routing tables: inet.0 inet.3
10.10.0.0/16 Originating RIB: inet.0
   Node path count: 1
   Forwarding nexthops: 1
10.31.1.0/30 Originating RIB: inet.0
   Node path count: 1
   Forwarding nexthops: 1
10.31.1.1/32 Originating RIB: inet.0
   Node path count: 1
   Forwarding nexthops: 0
10.31.1.4/30 Originating RIB: inet.0
   Node path count: 1
   Forwarding nexthops: 1
10.31.1.5/32 Originating RIB: inet.0
```
show route resolution summary

user@host> show route resolution summary
Tree Index: 1, Nodes 24, Reference Count 1
Contributing routing tables: :voice.inet.0 :voice.inet.3
Tree Index: 2, Nodes 2, Reference Count 1
Contributing routing tables: inet.3
Tree Index: 3, Nodes 43, Reference Count 1
Contributing routing tables: inet.0 inet.3

show route resolution unresolved

user@host> show route resolution unresolved
Tree Index 1
vt-3/2/0.32769.0 /16
    Protocol Nexthop: 10.255.71.238 Push 800000
    Indirect nexthop: 0 -
vt-3/2/0.32772.0 /16
    Protocol Nexthop: 10.255.70.103 Push 800008
    Indirect nexthop: 0 -
Tree Index 2
show route snooping

Syntax
 show route snooping
  <brief | detail | extensive | terse>
  <all>
  <best address/prefix>
  <exact address>
  <range prefix-range>
  <summary>
  <table table-name>

Release Information
 Command introduced in Junos OS Release 8.5.
 Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
 Display the entries in the routing table that were learned from snooping.

Options
 none—Display the entries in the routing table that were learned from snooping.

brief | detail | extensive | terse—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief.

all—(Optional) Display all entries, including hidden entries.

best address/prefix—(Optional) Display the longest match for the provided address and optional prefix.

exact address/prefix—(Optional) Display exact matches for the provided address and optional prefix.

range prefix-range—(Optional) Display information for the provided address range.

summary—(Optional) Display route snooping summary statistics.

table table-name—(Optional) Display information for the named table.

Required Privilege
 view

List of Sample Output
 show route snooping detail on page 3268

Output Fields
 For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output
 show route snooping detail

user@host> show route snooping detail
---domainAll---inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
  224.0.0.2/32 (1 entry, 1 announced)
     *IGMP Preference: 0
     Next hop type: MultiRecv
     Next-hop reference count: 4
     State: <Active NoReadvrt Int>
Age: 2:24
Task: IGMP
Announcement bits (1): 0-KRT
AS path: I

224.0.0.22/32 (1 entry, 1 announced)
*IGMP  Preference: 0
Next hop type: MultiRecv
Next-hop reference count: 4
State: <Active NoReadvrt Int>
Age: 2:24
Task: IGMP
Announcement bits (1): 0-KRT
AS path: I

__+domainAll__.inet.1: 36 destinations, 36 routes (36 active, 0 holddown, 0 hidden)

224.0.0.0.0.0.0.0/24 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4), Next hop index: 1048584
Next-hop reference count: 4
State: <Active Int>
Age: 2:24
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.2.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:13
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.3.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:15
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.4.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:17
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.5.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 1:58
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.6.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:14
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.7.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:12
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.9.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:13
Task: MC
Announcement bits (1): 0-KRT
AS path: I

225.0.0.10.11.11.11.100.3.9.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:15
Task: MC
Announcement bits (1): 0-KRT
AS path: I

226.0.0.1.11.11.11.100.3.10.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 2:09
Task: MC
Announcement bits (1): 0-KRT
AS path: I

226.0.0.2.11.11.11.100.3.10.0.0/80 (1 entry, 1 announced)
*Multicast Preference: 180
Next hop type: Multicast (IPv4)
Next-hop reference count: 113
State: <Active Int>
Age: 8
Task: MC
Announcement bits (1): 0-KRT
AS path: I

226.0.0.4.11.11.11.100.3.10.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:10
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

226.0.0.8.11.11.11.100.3.10.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:12
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

226.0.0.12.11.11.11.100.3.10.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 1:56
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

227.0.0.1.11.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:10
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

227.0.0.2.11.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:13
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

227.0.0.3.11.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:16
Task: MC
Announcement bits (1): 0-KRT
AS path: I

227.0.0.4.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:15
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

227.0.0.5.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 1:57
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

227.0.0.7.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 1:57
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

227.0.0.8.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:10
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

227.0.0.10.11.11.100.3.11.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:15
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

228.0.0.1.11.11.100.3.12.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:09
  Task: MC
Announcement bits (1): 0-KRT
AS path: I

228.0.0.2.11.11.11.100.3.12.0.0/80 (1 entry, 1 announced)
* Multicast Preference: 180
   Next hop type: Multicast (IPv4)
   Next-hop reference count: 113
   State: <Active Int>
   Age: 2:18
   Task: MC
   Announcement bits (1): 0-KRT
   AS path: I

228.0.0.7.11.11.11.100.3.12.0.0/80 (1 entry, 1 announced)
* Multicast Preference: 180
   Next hop type: Multicast (IPv4)
   Next-hop reference count: 113
   State: <Active Int>
   Age: 2:11
   Task: MC
   Announcement bits (1): 0-KRT
   AS path: I

228.0.0.8.11.11.11.100.3.12.0.0/80 (1 entry, 1 announced)
* Multicast Preference: 180
   Next hop type: Multicast (IPv4)
   Next-hop reference count: 113
   State: <Active Int>
   Age: 2:17
   Task: MC
   Announcement bits (1): 0-KRT
   AS path: I

228.0.0.9.11.11.11.100.3.12.0.0/80 (1 entry, 1 announced)
* Multicast Preference: 180
   Next hop type: Multicast (IPv4)
   Next-hop reference count: 113
   State: <Active Int>
   Age: 8
   Task: MC
   Announcement bits (1): 0-KRT
   AS path: I

228.0.0.10.11.11.11.100.3.12.0.0/80 (1 entry, 1 announced)
* Multicast Preference: 180
   Next hop type: Multicast (IPv4)
   Next-hop reference count: 113
   State: <Active Int>
   Age: 2:12
   Task: MC
   Announcement bits (1): 0-KRT
   AS path: I

229.0.0.3.11.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
* Multicast Preference: 180
   Next hop type: Multicast (IPv4)
   Next-hop reference count: 113
   State: <Active Int>
   Age: 2:09
   Task: MC
   Announcement bits (1): 0-KRT
AS path: I

229.0.0.4.11.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:12
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

229.0.0.5.11.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 9
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

229.0.0.6.11.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:15
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

229.0.0.7.11.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:15
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

229.0.0.8.11.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:15
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I

229.0.0.9.11.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:14
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I
229.0.0.10.11.11.100.3.13.0.0/80 (1 entry, 1 announced)
  *Multicast Preference: 180
  Next hop type: Multicast (IPv4)
  Next-hop reference count: 113
  State: <Active Int>
  Age: 2:13
  Task: MC
  Announcement bits (1): 0-KRT
  AS path: I
**show route source-gateway**

**Syntax**

```plaintext
show route source-gateway address
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**

```plaintext
show route source-gateway address
  <brief | detail | extensive | terse>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display the entries in the routing table that were learned from a particular address. The `Source` field in the `show route detail` command output lists the source for each route, if known.

**Options**

`brief | detail | extensive | terse`—(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to `brief`.

`address`—IP address of the system.

`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

`view`

**List of Sample Output**

- show route source-gateway on page 3276
- show route source-gateway detail on page 3277
- show route source-gateway extensive on page 3279

**Output Fields**

For information about output fields, see the output field tables for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

**Sample Output**

```
show route source-gateway

user@host> show route source-gateway 10.255.70.103
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
  Restart Complete

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
  Restart Complete

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Restart Complete

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
  Restart Complete
```
inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)  
Restart Complete

private1__.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)  
Restart Complete

+ = Active Route, - = Last Active, * = Both

10.255.70.103:1:3:1/96
  *[BGP/170] 12:12:24, localpref 100, from 10.255.70.103
  AS path: I
  > via so-0/3/0.0, label-switched-path green-r1-r3

red.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)  
Restart Complete

+ = Active Route, - = Last Active, * = Both

10.255.70.103:2:3:1/96
  *[BGP/170] 12:12:24, localpref 0, from 10.255.70.103
  AS path: I
  > via so-0/3/0.0, label-switched-path green-r1-r3

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)  
Restart Complete

+ = Active Route, - = Last Active, * = Both

10.255.70.103:1:3:1/96
  *[BGP/170] 12:12:24, localpref 100, from 10.255.70.103
  AS path: I
  > via so-0/3/0.0, label-switched-path green-r1-r3

10.255.70.103:2:3:1/96
  *[BGP/170] 12:12:24, localpref 0, from 10.255.70.103
  AS path: I
  > via so-0/3/0.0, label-switched-path green-r1-r3

show route source-gateway detail

user@host> show route source-gateway 10.255.70.103 detail
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)  
Restart Complete

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)  
Restart Complete

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)  
Restart Complete

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)  
Restart Complete

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)  
Restart Complete

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)  
Restart Complete

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
  *BGP    Preference: 170/-101
Route Distinguisher: 10.255.70.103:1
Next-hop reference count: 7
Source: 10.255.70.103
Protocol next hop: 10.255.70.103
Indirect next hop: 2 no-forward
State: <Secondary Active Int Ext>
Local AS: 69 Peer AS: 69
Age: 12:14:00 Metric2: 1
Task: BGP_69.10.255.70.103+179
Announcement bits (1): 0-green-l2vpn
AS path: I
Communities: target:11111:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0
Label-base: 800008, range: 8
Localpref: 100
Router ID: 10.255.70.103
Primary Routing Table bgp.l2vpn.0

red.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:2:3:1/96 (1 entry, 1 announced)
  ^BGP  Preference: 170/-1
  Route Distinguisher: 10.255.70.103:2
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Secondary Active Int Ext>
  Local AS: 69 Peer AS: 69
  Age: 12:14:00 Metric2: 1
  Task: BGP_69.10.255.70.103+179
  Announcement bits (1): 0-red-l2vpn
  AS path: I
  Communities: target:11111:2 Layer2-info: encaps:VPLS, control flags:Site-Down, mtu: 0
  Label-base: 800008, range: 8
  Localpref: 0
  Router ID: 10.255.70.103
  Primary Routing Table bgp.l2vpn.0

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:1:3:1/96 (1 entry, 0 announced)
  ^BGP  Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Active Int Ext>
  Local AS: 69 Peer AS: 69
  Age: 12:14:00 Metric2: 1
  Task: BGP_69.10.255.70.103+179
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS, control flags:, mtu: 0
  Label-base: 800008, range: 8
  Localpref: 100
  Router ID: 10.255.70.103
show route source-gateway extensive

user@host> show route source-gateway 10.255.70.103 extensive
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
  Restart Complete

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
  Restart Complete

private1__.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)
  Restart Complete

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Restart Complete

mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
  Restart Complete

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
  Restart Complete

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
  Restart Complete
10.255.70.103:113:1/96 (1 entry, 1 announced)
  *BGP  Preference: 170/-101
      Route Distinguisher: 10.255.70.103:1
      Next-hop reference count: 7
      Source: 10.255.70.103
      Protocol next hop: 10.255.70.103
      Indirect next hop: 2 no-forward
      State: <Secondary Active Int Ext>
      Local AS:  69 Peer AS:  69
      Age: 12:15:24  Metric2: 1
      Task: BGP_69.10.255.70.103+179
      Announcement bits (1): 0-green-l2vpn
      AS path: I
      Communities: target:11111:1 Layer2-info: encaps:VPLS,
                    control flags:, mtu: 0
      Label-base: 800008, range: 8
      Localpref: 100
      Router ID: 10.255.70.103
Primary Routing Table bgp.l2vpn.0

bgp.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:2:3:1/96 (1 entry, 1 announced)
  *BGP   Preference: 170/-1
  Route Distinguisher: 10.255.70.103:2
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Secondary Active Int Ext>
  Local AS:    69 Peer AS:    69
  Age: 12:15:24   Metric2: 1
  Task: BGP_69.10.255.70.103+179
  Announcement bits (1): 0-red-l2vpn
  AS path: I
  Communities: target:11111:2 Layer2-info: encaps:VPLS,
  control flags:Site-Down, mtu: 0
  Label-base: 800016, range: 8
  Localpref: 0
  Router ID: 10.255.70.103
  Primary Routing Table bgp.l2vpn.0

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete

10.255.70.103:1:3:1/96 (1 entry, 0 announced)
  *BGP   Preference: 170/-101
  Route Distinguisher: 10.255.70.103:1
  Next-hop reference count: 7
  Source: 10.255.70.103
  Protocol next hop: 10.255.70.103
  Indirect next hop: 2 no-forward
  State: <Active Int Ext>
  Local AS:    69 Peer AS:    69
  Age: 12:15:24   Metric2: 1
  Task: BGP_69.10.255.70.103+179
  AS path: I
  Communities: target:11111:1 Layer2-info: encaps:VPLS,
  control flags:, mtu: 0
  Label-base: 800008, range: 8
  Localpref: 100
  Router ID: 10.255.70.103
  Secondary Tables: green.l2vpn.0
  Indirect next hops: 1
  Protocol next hop: 10.255.70.103 Metric: 2
  Indirect next hop: 2 no-forward
  Indirect path forwarding next hops: 1
  Next hop: via so-0/3/0.0 weight 0x1
  10.255.70.103/32 Originating RIB: inet.3
  Metric: 2                       Node path count: 1
  Forwarding nexthops: 1
  Nexthop: via so-0/3/0.0

10.255.70.103:2:3:1/96 (1 entry, 0 announced)
  *BGP   Preference: 170/-1
  Route Distinguisher: 10.255.70.103:2
  Next-hop reference count: 7
  Source: 10.255.70.103
Protocol next hop: 10.255.70.103
Indirect next hop: 2 no-forward
State: <Active Int Ext>
Local AS: 69 Peer AS: 69
Age: 12:15:24 Metric2: 1
Task: BGP_69.10.255.70.103+179
AS path: I
Communities: target:11111:2 Layer2-info: encaps:VPLS,
control flags:Site-Down,
mtu: 0
Label-base: 800016, range: 8
Localpref: 0
Router ID: 10.255.70.103
Secondary Tables: red.l2vpn.0
Indirect next hops: 1
  Protocol next hop: 10.255.70.103 Metric: 2
  Indirect next hop: 2 no-forward
  Indirect path forwarding next hops: 1
Next hop: via so-0/3/0.0 weight 0x1
  10.255.70.103/32 Originating RIB: inet.3
  Metric: 2
  Node path count: 1
  Forwarding nexthops: 1
  Nexthop: via so-0/3/0.0
show route summary

**Syntax**
```
show route summary
<logical-system (all | logical-system-name)>
<table routing-table-name>
```

**Syntax (EX Series Switches)**
```
show route summary
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display summary statistics about the entries in the routing table.

CPU utilization might increase while the device learns routes. We recommend that you use the `show route summary` command after the device learns and enters the routes into the routing table. Depending on the size of your network, this might take several minutes. If you receive a “timeout communicating with routing daemon” error when using the `show route summary` command, wait several minutes before attempting to use the command again. This is not a critical system error, but you might experience a delay in using the command-line interface (CLI).

**Options**

- **none**—Display summary statistics about the entries in the routing table.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **table routing-table-name**—(Optional) Display summary statistics for all routing tables whose name begins with this string (for example, `inet.0` and `inet6.0` are both displayed when you run the `show route summary table inet` command). If you only want to display statistics for a specific routing table, make sure to enter the exact name of that routing table.

**Required Privilege Level**
`view`

**List of Sample Output**
- `show route summary on page 3283`
- `show route summary table on page 3284`
- `show route summary table (with Route Limits Configured for the Routing Table) on page 3284`

**Output Fields**
Table 398 on page 3282 lists the output fields for the `show route summary` command. Output fields are listed in the approximate order in which they appear.

**Table 398: show route summary Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router-id</code></td>
<td>Address of the local routing device.</td>
</tr>
<tr>
<td><code>routing-table-name</code></td>
<td>Name of the routing table (for example, <code>inet.0</code>).</td>
</tr>
</tbody>
</table>
### Table 398: show route summary Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
</tbody>
</table>
| routes | Number of routes in the routing table:  
- **active**—Number of routes that are active.  
- **holddown**—Number of routes that are in the hold-down state before being declared inactive.  
- **hidden**—Number of routes that are not used because of routing policy. |
| Limit/Threshold | Displays the configured route limits for the routing table set with the `maximum-prefixes` and the `maximum-paths` statements. If you do not configure route limits for the routing table, the show output does not display this information.  
- **destinations**—The first number represents the maximum number of route prefixes installed in the routing table. The second number represents the number of route prefixes that trigger a warning message.  
- **routes**—The first number represents the maximum number of routes. The second number represents the number of routes that trigger a warning message. |

### Direct
- Routes on the directly connected network.

### Local
- Local routes.

### protocol-name
- Name of the protocol from which the route was learned. For example, **OSPF**, **RSVP**, and **Static**.

---

**Sample Output**

```
show route summary
Autonomous system number: 69
Router ID: 10.255.71.52
Maximum-ECMP: 32
inet.0: 24 destinations, 25 routes (23 active, 0 holddown, 1 hidden)
  Restart Complete
  Direct: 6 routes, 5 active
  Local: 4 routes, 4 active
  OSPF: 5 routes, 4 active
  Static: 7 routes, 7 active
  IGMP: 1 routes, 1 active
  PIM: 2 routes, 2 active

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
  Restart Complete
  RSVP: 2 routes, 2 active

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Restart Complete
  Direct: 1 routes, 1 active
```

---

Copyright © 2013, Juniper Networks, Inc.
mpls.0: 7 destinations, 7 routes (5 active, 0 holddown, 2 hidden)
Restart Complete
  MPLS: 3 routes, 3 active
  VPLS: 4 routes, 2 active

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
Restart Complete
  Direct: 2 routes, 2 active
  PIM: 2 routes, 2 active
  MLD: 1 routes, 1 active

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
  BGP: 2 routes, 2 active
  L2VPN: 2 routes, 2 active

red.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
Restart Complete
  BGP: 2 routes, 2 active
  L2VPN: 1 routes, 1 active

bgp.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
Restart Complete
  BGP: 4 routes, 4 active

show route summary table

user@host> show route summary table inet
Router ID: 192.168.0.1

inet.0: 32 destinations, 34 routes (31 active, 0 holddown, 1 hidden)
  Direct: 6 routes, 5 active
  Local: 9 routes, 9 active
  OSPF: 3 routes, 1 active
  Static: 13 routes, 13 active
  IGMP: 1 routes, 1 active
  PIM: 2 routes, 2 active

inet.1: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Multicast: 1 routes, 1 active

inet6.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
  Local: 1 routes, 1 active
  PIM: 2 routes, 2 active

inet6.1: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
  Multicast: 1 routes, 1 active

show route summary table (with Route Limits Configured for the Routing Table)

user@host> show route summary table VPN-A.inet.0
Autonomous system number: 100
Router ID: 10.255.182.142

VPN-A.inet.0: 13 destinations, 14 routes (13 active, 0 holddown, 0 hidden)
Limit/Threshold: 2000/200 destinations 20/12 routes
  Direct: 2 routes, 2 active
  Local: 1 routes, 1 active
  OSPF: 4 routes, 3 active
  BGP: 4 routes, 4 active
IGMP: 1 routes, 1 active
PIM: 2 routes, 2 active
**show route table**

**Syntax**
```
show route table routing-table-name
  <brief | detail | extensive | terse>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switches)**
```
show route table routing-table-name
  <brief | detail | extensive | terse>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display the route entries in a particular routing table.

**Options**
- `brief | detail | extensive | terse`—(Optional) Display the specified level of output.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `routing-table-name`—Display route entries for all routing tables whose name begins with this string (for example, inet.0 and inet6.0 are both displayed when you run the `show route table inet` command).

**Required Privilege Level**
view

**Related Documentation**
- show route summary on page 3282
  - show route table bgp.l2.vpn on page 3287
  - show route table bgp.l3vpn.0 on page 3287
  - show route table bgp.l3vpn.0 detail on page 3287
  - show route table bgp.rtargen.0 (When Proxy BGP Route Target Filtering Is Configured) on page 3289
  - show route table inet.0 on page 3289
  - show route table inet6.0 on page 3289
  - show route table inet6.3 on page 3290
  - show route table inetflow detail on page 3290
  - show route table l2circuit.0 on page 3290
  - show route table mpls on page 3291
  - show route table mpls extensive on page 3291
  - show route table mpls.0 on page 3291
  - show route table mpls.0 (RSVP Route—Transit LSP) on page 3292
  - show route table vpls_1 detail on page 3292
  - show route table vpn-a on page 3292
  - show route table vpn-a.mdt.0 on page 3293
  - show route table VPN-A detail on page 3293
  - show route table VPN-AB.inet.0 on page 3293
  - show route table VPN_blue.mvpn-inet6.0 on page 3294
  - show route table VPN-A detail on page 3294
Output Fields  For information about output fields, see the output field tables for the show route command, the show route detail command, the show route extensive command, or the show route terse command.

Sample Output

show route table bgp.l2.vpn

user@host>  show route table bgp.l2.vpn
bgp.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

  *[BGP/170] 01:08:58, localpref 100, from 192.168.24.1
  AS path: I
  > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am

show route table bgp.l3vpn.0

user@host>  show route table bgp.l3vpn.0
bgp.l3vpn.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.255.71.15:100:10.255.71.17/32
  *[BGP/170] 00:03:59, MED 1, localpref 100, from 10.255.71.15
  AS path: I
  > via so-2/1/0.0, Push 100020, Push 100011(top)

10.255.71.15:200:10.255.71.18/32
  *[BGP/170] 00:03:59, MED 1, localpref 100, from 10.255.71.15
  AS path: I
  > via so-2/1/0.0, Push 100021, Push 100011(top)

show route table bgp.l3vpn.0 detail

user@host>  show route table bgp.l3vpn.0 detail
bgp.l3vpn.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)

10.255.245.12:1:4.0.0.0/8 (1 entry, 1 announced)
  *BGP   Preference: 170/-101
  Route Distinguisher: 10.255.245.12:1
  Source: 10.255.245.12
  Next hop: 192.168.208.66 via fe-0/0/0.0, selected
  Label operation: Push 182449
  Protocol next hop: 10.255.245.12
  Push 182449
  Indirect next hop: 863a630 297
  State: <Active Int Ext>
  Local AS: 35 Peer AS: 35
  Age: 12:19   Metric2: 1
  Task: BGP_35.10.255.245.12+179
  Announcement bits (1): 0-BGP.0.0.0.0+179
  AS path: 30 10458 14203 2914 3356 I (Atomic) Aggregator: 3356 4.68.0.11
  Communities: 2914:420 target:11111:1 origin:56:78
  VPN Label: 182449
  Localpref: 100
Router ID: 10.255.245.12

10.255.245.12:1:4.17.225.0/24 (1 entry, 1 announced)
*BGP Preference: 170/-101
Route Distinguisher: 10.255.245.12:1
Source: 10.255.245.12
Next hop: 192.168.208.66 via fe-0/0/0.0, selected
Label operation: Push 182465
Protocol next hop: 10.255.245.12
Push 182465
Indirect next hop: 863a8f0 305
State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP_35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 11853 11853 11853 6496 6496 6496 6496 6496 6496 6496 I
Communities: 2914:410 target:12:34 target:11111:1 origin:12:34
VPN Label: 182465
Localpref: 100
Router ID: 10.255.245.12

10.255.245.12:1:4.17.226.0/23 (1 entry, 1 announced)
*BGP Preference: 170/-101
Route Distinguisher: 10.255.245.12:1
Source: 10.255.245.12
Next hop: 192.168.208.66 via fe-0/0/0.0, selected
Label operation: Push 182465
Protocol next hop: 10.255.245.12
Push 182465
Indirect next hop: 86bd210 330
State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP_35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 11853 11853 11853 6496 6496 6496 6496 6496 6496 6496 I
Communities: 2914:410 target:12:34 target:11111:1 origin:12:34
VPN Label: 182465
Localpref: 100
Router ID: 10.255.245.12

10.255.245.12:1:4.17.251.0/24 (1 entry, 1 announced)
*BGP Preference: 170/-101
Route Distinguisher: 10.255.245.12:1
Source: 10.255.245.12
Next hop: 192.168.208.66 via fe-0/0/0.0, selected
Label operation: Push 182465
Protocol next hop: 10.255.245.12
Push 182465
Indirect next hop: 86bd210 330
State: <Active Int Ext>
Local AS: 35 Peer AS: 35
Age: 12:19 Metric2: 1
Task: BGP_35.10.255.245.12+179
Announcement bits (1): 0-BGP.0.0.0.0+179
AS path: 30 10458 14203 2914 11853 11853 11853 6496 6496 6496 6496 6496 6496 6496 I
Communities: 2914:410 target:12:34 target:11111:1 origin:12:34
VPN Label: 182465
Localpref: 100
Router ID: 10.255.245.12
show route table bgp.rtarget.0 (When Proxy BGP Route Target Filtering Is Configured)

```
user@host> show route table bgp.rtarget.0
bgp.rtarget.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
100:100:100/96
  *[RTarget/5] 00:03:14
  for 10.255.165.103
  for 10.255.166.124
  Local
```

show route table inet.0

```
user@host> show route table inet.0
inet.0: 12 destinations, 12 routes (11 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0     *[Static/5] 00:51:57
  > to 111.222.5.254 via fxp0.0
1.0.0.1/32    *[Direct/0] 00:51:58
  > via at-5/3/0.0
1.0.0.2/32    *[Local/0] 00:51:58
  Local
12.12.12.21/32*[Local/0] 00:51:57
  Reject
13.13.13.32/32*[Direct/0] 00:51:58
  > via t3-5/2/1.0
13.13.13.34/32*[Local/0] 00:51:58
  Local
13.13.13.35/32*[Local/0] 00:51:58
  Local
13.13.13.36/32*[Direct/0] 00:33:59
  > via t3-5/2/0.0
127.0.0.1/32  *[Direct/0] 00:51:58
  > via lo0.0
111.222.5.0/24*[Direct/0] 00:51:58
  > via fxp0.0
111.222.5.81/32*[Local/0] 00:51:58
  Local
```

show route table inet6.0

```
user@host> show route table inet6.0
inet6.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Route, * = Both
fec0:0:0:3::/64 *[Direct/0] 00:01:34
  >via fe-0/1/0.0
fec0:0:0:3::128 *[Local/0] 00:01:34
  >Local
fec0:0:0:4::/64 *[Static/5] 00:01:34
  >to fec0:0:0:3::fff via fe-0/1/0.0
```
show route table inet6.3

user@router> show route table inet6.3
inet6.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::10.255.245.195/128
*[LDP/9] 00:00:22, metric 1
> via so-1/0/0.0

::10.255.245.196/128
*[LDP/9] 00:00:08, metric 1
> via so-1/0/0.0, Push 100008

show route table inetflow detail

user@host> show route table inetflow detail
inetflow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
10.12.44.1,*/48 (1 entry, 1 announced)
*BGP Preference: 170/-101
Next-hop reference count: 2
State: <Active Ext>
Local AS: 65002 Peer AS: 65000
Age: 4
Task: BGP_65000.10.12.99.5+3792
Announcement bits (1): 0-Flow
AS path: 65000 I
Communities: traffic-rate:0:0
Validation state: Accept, Originator: 10.12.99.5
Via: 10.12.44.0/24, Active
Localpref: 100
Router ID: 10.255.71.161

10.12.56.1,*/48 (1 entry, 1 announced)
*Flow Preference: 5
Next-hop reference count: 2
State: <Active>
Local AS: 65002
Age: 6:30
Task: RT Flow
Announcement bits (2): 0-Flow 1-BGP.0.0.0.0+179
AS path: I
Communities: 1:1

show route table l2circuit.0

user@host> show route table l2circuit.0
l2circuit.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.1.1.195:NoCtrlWord:1:1:Local/96
*[L2CKT/7] 00:50:47
> via so-0/1/2.0, Push 100049
via so-0/1/3.0, Push 100049

*[LDP/9] 00:50:14
Discard

10.1.1.195:CtrlWord:1:2:Local/96
*[L2CKT/7] 00:50:47
> via so-0/1/2.0, Push 100049
via so-0/1/3.0, Push 100049

show route table mpls

```
user@host> show route table mpls
mpls.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 00:13:55, metric 1
Receive
1                  *[MPLS/0] 00:13:55, metric 1
Receive
2                  *[MPLS/0] 00:13:55, metric 1
Receive
1024               *[VPN/0] 00:04:18
Receive

show route table mpls extensive

```

```
user@host> show route table mpls extensive
100000 (1 entry, 1 announced)
TSI:
KRT in-kernel 100000 /36 -> {so-1/0/0.0}
  *LDP Preference:  9
  Next hop:  via so-1/0/0.0, selected
  Pop
  State: <Active Int>
  Age: 29:50      Metric: 1
  Task: LDP
  Announcement bits (1): 0-KRT
  AS path: I
  Prefixes bound to route: 10.0.0.194/32

show route table mpls.0

```

```
user@host> show route table mpls.0
mpls.0: 11 destinations, 11 routes (11 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 00:45:09, metric 1
Receive
1                  *[MPLS/0] 00:45:09, metric 1
Receive
2                  *[MPLS/0] 00:45:09, metric 1
Receive
100000             *[L2VPN/7] 00:43:04
Receive
> via so-0/1/0.1, Pop
100001             *[L2VPN/7] 00:43:03
Receive
> via so-0/1/0.2, Pop       Offset: 4
100002             *[LDP/9] 00:43:22, metric 1
Receive
via so-0/1/2.0, Pop
> via so-0/1/3.0, Pop
100002(S=0)        *[LDP/9] 00:43:22, metric 1
Receive
via so-0/1/2.0, Pop
> via so-0/1/3.0, Pop
100003             *[LDP/9] 00:43:22, metric 1
Receive
via so-0/1/2.0, Swap 100002
via so-0/1/3.0, Swap 100002
100004             *[LDP/9] 00:43:16, metric 1
Receive
via so-0/1/2.0, Swap 100049
> via so-0/1/3.0, Swap 100049
```
show route table mpls.0 (RSVP Route—Transit LSP)

```
user@host> show route table mpls.0

mpls.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

0                  *[MPLS/0] 00:37:31, metric 1
           Receive
1                  *[MPLS/0] 00:37:31, metric 1
           Receive
2                  *[MPLS/0] 00:37:31, metric 1
           Receive
13                 *[MPLS/0] 00:37:31, metric 1
           Receive
300352             *[RSVP/7/1] 00:08:00, metric 1
           > to 8.64.0.106 via ge-1/0/1.0, label-switched-path lsp1_p2p
300352(S=0)        *[RSVP/7/1] 00:08:00, metric 1
           > to 8.64.0.106 via ge-1/0/1.0, label-switched-path lsp1_p2p
300384             *[RSVP/7/2] 00:05:20, metric 1
           > to 8.64.1.106 via ge-1/0/0.0, Pop
300384(S=0)        *[RSVP/7/2] 00:05:20, metric 1
           > to 8.64.1.106 via ge-1/0/0.0, Pop
```

show route table vpls_1 detail

```
user@host> show route table vpls_1 detail

vpls_1.l2vpn.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
Restart Complete

1.1.1.11:1000:1:1/96 (1 entry, 1 announced)
*L2VPN Preference: 170/-1
Receive table: vpls_1.12vpn.0
Next-hop reference count: 2
State: <Active Int Ext>
Age: 4:29:47 Metric2: 1
Task: vpls_1-l2vpn
Announcement bits (1): 1-BGP.0.0.0.0+179
AS path: I
Communities: Layer2-info: encaps:VPLS, control flags:Site-Down
Label-base: 800000, range: 8, status-vector: 0xFF
```

show route table vpn-a

```
user@host> show route table vpn-a

vpn-a.l2vpn.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.16.1:1:1/1:1/96
*[VPN/7] 05:48:27
          Discard
192.168.24.1:1:2/1/96
*[VPN/7] 00:02:53, localpref 100, from 192.168.24.1
           AS path: I
           > to 10.0.16.2 via fe-0/0/1.0, label-switched-path am
show route table vpn-a.mdt.0

user@host> show route table vpn-a.mdt.0

vpn-a.mdt.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

  *[MVPN/70] 01:23:05, metric 2 1
  Indirect

  *[BGP/170] 00:57:49, localpref 100, from 10.255.14.218
  AS path: 1
  > via so-0/0/0.0, label-switched-path r0-e-to-r1

  *[BGP/170] 00:57:49, localpref 100, from 10.255.14.217
  AS path: 1
  > via so-0/0/1.0, label-switched-path r0-e-to-r2

show route table VPN-A detail

user@host> show route table VPN-A detail

VPN-AB.inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
10.255.179.9/32 (1 entry, 1 announced)
  *BGP
  Preference: 170/-101
  Route Distinguisher: 10.255.179.13:200
  Next hop type: Indirect
  Next-hop reference count: 5
  Source: 10.255.179.13
  Next hop type: Router, Next hop index: 732
  Next hop: 10.39.1.14 via fe-0/3/0.0, selected
  Label operation: Push 299824, Push 299824(top)
  Protocol next hop: 10.255.179.13
  Push 299824
  Indirect next hop: 8f275a0 1048574
  State: (Secondary Active Int Ext)
  Local AS: 1 Peer AS: 1
  Age: 3:41:06 Metric: 1 Metric2: 1
  Task: BGP.1.10.255.179.13+64309
  Announcement bits (2): 0-KRT 1-BGP RT Background
  AS path: 1
  Communities: target:1:200 rte-type:0.0.0.0:1:0
  Import Accepted
  VPN Label: 299824 TTL Action: vrf-ttl-propagate
  Localpref: 100
  Router ID: 10.255.179.13
  Primary Routing Table bgp.l3vpn.0

show route table VPN-AB.inet.0

user@host> show route table VPN-AB.inet.0

VPN-AB.inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.0/30  *[OSPF/10] 00:07:24, metric 1
  > via so-7/3/1.0

10.39.1.4/30  *[Direct/0] 00:08:42
  > via so-5/1/0.0
show route table VPN_blue.mvpn-inet6.0

show route table VPN-Adetail
show route table inetflow detail

inetflow.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
10.12.44.1,*/48 (1 entry, 1 announced)
  *BGP  Preference: 170/-101
  Next-hop reference count: 2
  State: <Active Ext>
  Local AS: 65002 Peer AS: 65000
  Age: 4
  Task: BGP_65000.10.12.99.5+3792
  Announcement bits (1): 0-Flow
  AS path: 65000 I
  Communities: traffic-rate:0:0
  Validation state: Accept, Originator: 10.12.99.5
  Via: 10.12.44.0/24, Active
  Localpref: 100
  Router ID: 10.255.71.161

10.12.56.1,*/48 (1 entry, 1 announced)
  *Flow  Preference: 5
  Next-hop reference count: 2
  State: <Active>
  Local AS: 65002
  Age: 6:30
  Task: RT Flow
  Announcement bits (2): 0-Flow 1-BGP.0.0.0.0+179
  AS path: I
  Communities: 1:1

show route table green.l2vpn.0 (VPLS Multihoming with FEC 129)
green.l2vpn.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1.1.1.2:100:1.1.1.2/96 AD
  *[VPLS/170] 1d 03:11:03, metric2 1
  Indirect

1.1.1.4:100:1.1.1.4/96 AD
  *[BGP/170] 1d 03:11:02, localpref 100, from 1.1.1.4
  AS path: I, validation-state: unverified
  >    via ge-1/2/1.5

1.1.1.2:100:1.0/96 MH
  *[VPLS/170] 1d 03:11:03, metric2 1
  Indirect

1.1.1.4:100:1.0/96 MH
  *[BGP/170] 1d 03:11:02, localpref 100, from 1.1.1.4
  AS path: I, validation-state: unverified
user@host> show route table red extensive
red.inet.0: 364481 destinations, 714087 routes (364480 active, 48448 holddown, 1 hidden)
22.0.0.0/32 (3 entries, 1 announced)
  State: <OnList CalcForwarding>
  TSI:
   KRT in-kernel 22.0.0.0/32 -> {composite(1048575)} Page 0 idx 1 Type 1 val 0x934342c
  Nexthop: Self
  AS path: [2] I
  Communities: target:2:1
Path 22.0.0.0 from 2.3.0.0 Vector len 4. Val: 1
  @BGP
      Preference: 170/-1
      Next hop type: Indirect
      Address: 0x258059e4
      Next-hop reference count: 2
      Source: 2.2.0.0
      Next hop type: Router
      Next hop: 10.1.1.1 via ge-1/1/9.0, selected
      Label operation: Push 707633
      Label TTL action: prop-ttl
      Session Id: 0x17d8
      Protocol next hop: 2.2.0.0
      Push 16
      Composite next hop: 0x25805988 - INH Session ID: 0x193c
      Indirect next hop: 0x23eea900 - INH Session ID: 0x193c
      State: <Secondary Active Int Ext ProtectionPath ProtectionCand>
      Local AS: 2 Peer AS: 2
      Age: 23 Metric2: 35
      Validation State: unverified
      Task: BGP_2.2.2.0.0+34549
      AS path: I
      Communities: target:2:1
      Import Accepted
      VPN Label: 16
      Localpref: 0
      Router ID: 2.2.0.0
      Primary Routing Table bgp.l3vpn.0
      Composite next hops: 1
        Protocol next hop: 2.2.0.0 Metric: 35
        Push 16
        Composite next hop: 0x25805988 - INH Session ID: 0x193c
        Indirect next hop: 0x23eea900 - INH Session ID: 0x193c
        Indirect path forwarding next hops: 1
        Next hop type: Router
        Next hop: 10.1.1.1 via ge-1/1/9.0
        Session Id: 0x17d8
        2.2.0.0/32 Originating RIB: inet.3
        Metric: 35 Node path count: 1
        Forwarding nexthops: 1
        Nexthop: 10.1.1.1 via ge-1/1/9.0
  BGP Preference: 170/-1
Route Distinguisher: 2:1
Next hop type: Indirect
Address: 0x9347028
Next-hop reference count: 3
Source: 2.3.0.0
Next hop type: Router, Next hop index: 702
Next hop: 10.1.4.2 via ge-1/0/0.0, selected
Label operation: Push 634278
Label TTL action: prop-ttl
Session Id: 0x17d9
Protocol next hop: 2.3.0.0
Push 16
Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da
Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da
State: <Secondary NotBest Int Ext ProtectionPath ProtectionCand>

Inactive reason: Not Best in its group - IGP metric
Local AS: 2 Peer AS: 2
Age: 3:34 Metric2: 70
Validation State: unverified
Task: BGP_2.2.3.0.0+32805
Announcement bits (2): 0-KRT 1-BGP_RT_Background
AS path: I
Communities: target:2:1
Import Accepted
VPN Label: 16
Localpref: 0
Router ID: 2.3.0.0
Primary Routing Table bgp.l3vpn.0
Composite next hops: 1
  Protocol next hop: 2.3.0.0 Metric: 70
  Push 16
  Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da

Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da

Indirect path forwarding next hops: 1
  Next hop type: Router
  Next hop: 10.1.4.2 via ge-1/0/0.0
  Session Id: 0x17d9
  2.3.0.0/32 Originating RIB: inet.3
  Metric: 70 Node path count: 1
  Forwarding nexthops: 1
    Nexthop: 10.1.4.2 via ge-1/0/0.0

#Multipath Preference: 255
Next hop type: Indirect
Address: 0x24afca30
Next-hop reference count: 1
Next hop type: Router
Next hop: 10.1.1.1 via ge-1/1/9.0, selected
Label operation: Push 707633
Label TTL action: prop-ttl
Session Id: 0x17d8
Next hop type: Router, Next hop index: 702
Next hop: 10.1.4.2 via ge-1/0/0.0
Label operation: Push 634278
Label TTL action: prop-ttl
Session Id: 0x17d9
Protocol next hop: 2.2.0.0
Push 16
Composite next hop: 0x25805988 - INH Session ID: 0x193c
Indirect next hop: 0x23eea900 - INH Session ID: 0x193c Weight 0x1

Protocol next hop: 2.3.0.0
Push 16
Composite next hop: 0x93463a0 1048575 INH Session ID: 0x17da
Indirect next hop: 0x91e8800 1048574 INH Session ID: 0x17da Weight 0x4000

State: <ForwardingOnly Int Ext>
Inactive reason: Forwarding use only
Age: 23 Metric2: 35
Validation State: unverified
Task: RT
AS path: I
Communities: target:2:1
show route terse

Syntax

show route terse
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show route terse

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display a high-level summary of the routes in the routing table.

NOTE: For BGP routes, the show route terse command displays the local preference attribute and MED instead of the metric1 and metric2 values. This is mostly due to historical reasons.

To display the metric1 and metric2 value of a BGP route, use the show route extensive command.

Options

none—Display a high-level summary of the routes in the routing table.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

List of Sample Output

show route terse on page 3301

Output Fields

Table 399 on page 3299 describes the output fields for the show route terse command. Output fields are listed in the approximate order in which they appear.

Table 399: show route terse Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routing-table-name</td>
<td>Name of the routing table (for example, inet.0).</td>
</tr>
<tr>
<td>number destinations</td>
<td>Number of destinations for which there are routes in the routing table.</td>
</tr>
<tr>
<td>number routes</td>
<td>Number of routes in the routing table and total number of routes in the following states:</td>
</tr>
<tr>
<td></td>
<td>• active (routes that are active)</td>
</tr>
<tr>
<td></td>
<td>• holddown (routes that are in the pending state before being declared inactive)</td>
</tr>
<tr>
<td></td>
<td>• hidden (routes that are not used because of a routing policy)</td>
</tr>
</tbody>
</table>
### Table 399: show route terse Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>route key</strong></td>
<td>Key for the state of the route:</td>
</tr>
<tr>
<td></td>
<td>• +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table.</td>
</tr>
<tr>
<td></td>
<td>• -—A hyphen indicates the last active route.</td>
</tr>
<tr>
<td></td>
<td>• *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route.</td>
</tr>
<tr>
<td><strong>A</strong></td>
<td>Active route. An asterisk (*) indicates this is the active route.</td>
</tr>
<tr>
<td><strong>V</strong></td>
<td>Validation status of the route:</td>
</tr>
<tr>
<td></td>
<td>• ?—Not evaluated. Indicates that the route was not learned through BGP.</td>
</tr>
<tr>
<td></td>
<td>• I—Invalid. Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database.</td>
</tr>
<tr>
<td></td>
<td>• N—Unknown. Indicates that the prefix is not among the prefixes or prefix ranges in the database.</td>
</tr>
<tr>
<td></td>
<td>• V—Valid. Indicates that the prefix and autonomous system pair are found in the database.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td>Destination of the route.</td>
</tr>
<tr>
<td><strong>P</strong></td>
<td>Protocol through which the route was learned:</td>
</tr>
<tr>
<td></td>
<td>• A—Aggregate</td>
</tr>
<tr>
<td></td>
<td>• B—BGP</td>
</tr>
<tr>
<td></td>
<td>• C—CCC</td>
</tr>
<tr>
<td></td>
<td>• D—Direct</td>
</tr>
<tr>
<td></td>
<td>• G—GMPLS</td>
</tr>
<tr>
<td></td>
<td>• I—IS-IS</td>
</tr>
<tr>
<td></td>
<td>• L—L2CKT, L2VPN, LDP, Local</td>
</tr>
<tr>
<td></td>
<td>• K—Kernel</td>
</tr>
<tr>
<td></td>
<td>• M—MPLS, MSDP</td>
</tr>
<tr>
<td></td>
<td>• O—OSPF</td>
</tr>
<tr>
<td></td>
<td>• P—PIM</td>
</tr>
<tr>
<td></td>
<td>• R—RIP, RIPng</td>
</tr>
<tr>
<td></td>
<td>• S—Static</td>
</tr>
<tr>
<td></td>
<td>• T—Tunnel</td>
</tr>
<tr>
<td><strong>Prf</strong></td>
<td>Preference value of the route. In every routing metric except for the BGP LocalPref attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the LocalPref value in the Preference2 field. For example, if the LocalPref value for Route 1 is 100, the Preference2 value is -101. If the LocalPref value for Route 2 is 155, the Preference2 value is -156. Route 2 is preferred because it has a higher LocalPref value and a lower Preference2 value.</td>
</tr>
<tr>
<td><strong>Metric 1</strong></td>
<td>First metric value in the route. For routes learned from BGP, this is the MED metric.</td>
</tr>
<tr>
<td><strong>Metric 2</strong></td>
<td>Second metric value in the route. For routes learned from BGP, this is the IGP metric.</td>
</tr>
</tbody>
</table>
Table 399: show route terse Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next hop</td>
<td>Next hop to the destination. An angle bracket (&gt;) indicates that the route is the selected route.</td>
</tr>
<tr>
<td>AS path</td>
<td>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</td>
</tr>
<tr>
<td></td>
<td>• I—IGP.</td>
</tr>
<tr>
<td></td>
<td>• E—EGP.</td>
</tr>
<tr>
<td></td>
<td>• ?—Incomplete; typically, the AS path was aggregated.</td>
</tr>
</tbody>
</table>

Sample Output

```
user@host> show route terse
inet.0: 10 destinations, 12 routes (10 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

A V Destination        P Prf   Metric 1   Metric 2  Next hop        AS path
* ? 1.0.1.1/32         O  10          1            >10.0.0.2
      unverified
?                          
? 1.1.1.1/32              D  0            100       >10.0.0.2
      unverified
* V 2.2.0.2/32            B 170         110       >10.0.0.2
      valid
* ? 10.0.0.0/30           D  0            100       >10.0.0.2
      unverified
?                          
? 10.0.0.1/32             L  0            100       >10.0.0.2
      Local
* ? 10.0.0.4/30           B 170         100       >10.0.0.2
      unverified
* ? 10.0.0.8/30           B 170         100       >10.0.0.2
      unverified
* I 172.16.1.1/32         B 170         90        >10.0.0.2
      invalid
* N 192.168.2.3/32        B 170         100       >10.0.0.2
      unknown
* ? 224.0.0.5/32          O  10          1         MultiRecv

```
PART 21

Multicast

- Overview on page 3305
- Configuration on page 3315
- Administration on page 3407
Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on VLANs on a switch. When IGMP snooping is enabled on a VLAN, a Juniper Networks EX Series Ethernet Switch examines IGMP messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

IGMP snooping on EX Series switches supports IGMP version 1 (IGMPv1), IGMPv2, and IGMPv3. For details on IGMP, see the following standards:

- IGMPv1—See RFC 1112, Host extensions for IP multicasting.

This topic covers:

- How IGMP Snooping Works on page 3306
- IGMP Message Types on page 3306
- How Hosts Join and Leave Multicast Groups on page 3307
- Support for IGMPv3 Multicast Sources on page 3307
- IGMP Snooping and Forwarding Interfaces on page 3308
- General Forwarding Rules on page 3308
- Examples of IGMP Snooping Multicast Forwarding on page 3309
How IGMP Snooping Works

A Layer 2 switch usually learns *unicast* media access control (MAC) addresses by checking the source address field of the frames it receives. However, a *multicast* MAC address can never be the source address for a packet. As a result, the switch floods multicast traffic on the VLAN, consuming significant amounts of bandwidth.

You can enable IGMP snooping on a switch to avoid this flooding. When IGMP snooping is enabled, the switch monitors IGMP messages between receivers and multicast routers and uses the content of the messages to build an IPv4 multicast forwarding table—a database of multicast groups and the interfaces that are connected to members of the groups. When the switch receives multicast traffic for a multicast group, it uses the forwarding table to forward the traffic only to interfaces that are connected to receivers that belong to the multicast group.

Figure 38 on page 3306 shows an example of multicast traffic flow with IGMP snooping enabled.

**Figure 38: Multicast Traffic Flow with IGMP Snooping Enabled**

- Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have interested listeners. In any given subnet, one multicast router acts as an IGMP querier. The IGMP querier sends out the following types of queries to hosts:
  - General query—Asks whether any host is listening to any group.
  - Group-specific query—(IGMPv2 and IGMPv3 only) Asks whether any host is listening to a specific multicast group. This query is sent in response to a host leaving the multicast group and allows the router to quickly determine if any remaining hosts are interested in the group.
• Group-and-source-specific query—(IGMPv3 only) Asks whether any host is listening to group multicast traffic from a specific multicast source. This query is sent in response to a host indicating that it is no longer interested in receiving group multicast traffic from the multicast source and allows the router to quickly determine any remaining hosts are interested in receiving group multicast traffic from that source.

Hosts that are multicast listeners send the following kinds of messages:

• Membership report—Indicates that the host wants to join a particular multicast group.
• Leave report—(IGMPv2 and IGMPv3 only) Indicates that the host wants to leave a particular multicast group.

How Hosts Join and Leave Multicast Groups

Hosts can join multicast groups in either of two ways:

• By sending an unsolicited IGMP join message to a multicast router that specifies the IP multicast group that the host is attempting to join.
• By sending an IGMP join message in response to a general query from a multicast router.

A multicast router continues to forward multicast traffic to a VLAN provided that at least one host on that VLAN responds to the periodic general IGMP queries. For a host to remain a member of a multicast group, therefore, it must continue to respond to the periodic general IGMP queries.

Hosts can leave a multicast group in either of two ways:

• By not responding to periodic queries within a set interval of time. This results in what is known as a “silent leave.” This is the only method available to IGMPv1 hosts.
• By sending a leave report. This method can be used by IGMPv2 and IGMPv3 hosts.

**NOTE:** If a host is connected to the switch through a hub, the host does not automatically leave the multicast group if it disconnects from the hub. The host remains a member of the group until group membership times out and a silent leave occurs. If another host connects to the hub port before the silent leave occurs, the new host might receive the group multicast traffic until the silent leave, even though it never sent an membership report.

Support for IGMPv3 Multicast Sources

In IGMPv3, a host can send a membership report that includes a list of source addresses. When the host sends a membership report in INCLUDE mode, the host is interested in group multicast traffic only from those sources in the source address list. If host sends a membership report in EXCLUDE mode, the host is interested in group multicast traffic from any source except the sources in the source address list. A host can also send an EXCLUDE report in which the source-list parameter is empty, which is known as an
EXCLUDE NULL report. An EXCLUDE NULL report indicates that the host wants to join the multicast group and receive packets from all sources.

EX Series switches support IGMPv3 membership reports that are in INCLUDE and EXCLUDE mode. However, EX Series switches do not support forwarding on a per-source basis. Instead, a switch consolidates all INCLUDE and EXCLUDE mode reports it receives on a VLAN for a specified group into a single route that includes all multicast sources for that group, with the next hop being all interfaces that have interested receivers for the group. As a result, interested receivers on the VLAN can receive traffic from a source that they did not include in their INCLUDE report or from a source they excluded in their EXCLUDE report. For example, if Host 1 wants traffic for G from Source A and Host 2 wants traffic for G from Source B, they both receive traffic for G regardless of whether A or B sends the traffic.

**IGMP Snooping and Forwarding Interfaces**

To determine how to forward multicast traffic, a switch with IGMP snooping enabled maintains information about the following interfaces in its multicast forwarding table:

- Multicast-router interfaces—These interfaces lead toward multicast routers or IGMP queriers.
- Group-member interfaces—These interfaces lead toward hosts that are members of multicast groups.

The switch learns about these interfaces by monitoring IGMP traffic. If an interface receives IGMP queries or Protocol Independent Multicast (PIM) updates, the switch adds the interface to its multicast forwarding table as a multicast-router interface. If an interface receives membership reports for a multicast group, the switch adds the interface to its multicast forwarding table as a group-member interface.

Table entries for interfaces that the switch learns about are subject to aging. For example, if a learned multicast-router interface does not receive IGMP queries or PIM hellos within a certain interval, the switch removes the entry for that interface from its multicast forwarding table.

**NOTE:** For a switch to learn multicast-router interfaces and group-member interfaces, an IGMP querier must exist in the network. For the switch itself to function as an IGMP querier, IGMP must be enabled on the switch.

You can statically configure an interface to be a multicast-router interface or a group-member interface. The switch adds a static interface to its multicast forwarding table without having to learn about the interface, and the entry in the table is not subject to aging. You can have a mix of statically configured and dynamically learned interfaces on a switch.

**General Forwarding Rules**

Multicast traffic received on a switch interface in a VLAN on which IGMP snooping is enabled is forwarded according to the following rules.
IGMP traffic is forwarded as follows:

- IGMP general queries received on a multicast-router interface are forwarded to all other interfaces in the VLAN.
- IGMP group-specific queries received on a multicast-router interface are forwarded to only those interfaces in the VLAN that are members of the group.
- IGMP reports received on a host interface are forwarded to multicast-router interfaces in the same VLAN, but not to the other host interfaces in the VLAN.

Multicast traffic that is not IGMP traffic is forwarded as follows:

- A multicast packet with a destination address of 224.0.0.0/24 is flooded to all other interfaces on the VLAN.
- An unregistered multicast packet—that is, a packet for a group that has no current members—is forwarded to all multicast-router interfaces in the VLAN.
- A registered multicast packet is forwarded only to those host interfaces in the VLAN that are members of the multicast group and to all multicast-router interfaces in the VLAN.

Examples of IGMP Snooping Multicast Forwarding

The following examples are provided to illustrate how IGMP snooping forwards multicast traffic in different topologies:

- Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts on page 3309
- Scenario 2: Switch Forwarding Multicast Traffic to Another Switch on page 3310
- Scenario 3: Switch Connected to Hosts Only (No IGMP Querier) on page 3311
- Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs on page 3312

**Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts**

In the topology shown in Figure 39 on page 3310, a switch acting as a Layer 2 device receives multicast traffic belonging to multicast group 239.10.1.1 from Source A, which is connected to the multicast router. It also receives multicast traffic belonging to multicast group 225.100.100.1 from Source B, which is connected directly to the switch. All interfaces on the switch belong to the same VLAN.

Because the switch receives IGMP queries from the multicast router on interface P1, IGMP snooping learns that interface P1 is a multicast-router interface and adds the interface to its multicast cache table. It forwards any IGMP general queries it receives on this interface to all host interfaces on the switch, and, in turn, forwards membership reports it receives from hosts to the multicast-router interface.

In the example, Hosts A and C have responded to the membership queries with membership reports for group 239.10.1.1. IGMP snooping adds interfaces P2 and P4 to its multicast cache table as member interfaces for group 239.10.1.1. It forwards the group multicast traffic received from Source A to Hosts A and C, but not to Hosts B and D.
Host B has responded to the membership queries with a membership report for group 225.100.100.1. The switch adds interface P3 to its multicast cache table as a member interface for group 225.100.100.1 and forwards multicast traffic it receives from Source B to Host B. The switch also forwards the multicast traffic it receives from Source B to the multicast-router interface P1.

Figure 39: Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts

Scenario 2: Switch Forwarding Multicast Traffic to Another Switch

In the topology show in Figure 40 on page 3311, a multicast source is connected to Switch A. Switch A in turn is connected to another switch, Switch B. Hosts on both Switch A and B are potential members of the multicast group. Both switches are acting as Layer 2 devices and all interfaces on the switches are members of the same VLAN.

Switch A receives IGMP queries from the multicast router on interface P1, making interface P1 a multicast-router interface for Switch A. Switch A forwards all general IGMP queries it receives on this interface to the other interfaces on the switch, including the interface connecting Switch B. Because Switch B receives the forwarded IGMP queries on interface P6, P6 is the multicast-router interface for Switch B. Switch B forwards the group membership report it receives from Host C to Switch A through its multicast-router interface. Switch A forwards the membership report to its multicast-router interface, includes interface P5 in its multicast cache table as a group-member interface, and forwards multicast traffic from the source to Switch B.
In certain implementations, you might have to configure P6 on Switch B as a static multicast-router interface to avoid a delay in a host receiving multicast traffic. For example, if Switch B receives unsolicited membership reports from its hosts before it learns which interface is its multicast-router interface, it does not forward those reports to Switch A. If Switch A then receives multicast traffic, it does not forward the traffic to Switch B, because it has not received any membership reports on interface P5. This issue will resolve when the multicast router sends out its next general query; however, it can cause a delay in the host receiving multicast traffic. You can statically configure interface P6 as a multicast-router interface to solve this issue.

**Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)**

In the topology shown in Figure 41 on page 3312, a switch is connected to a multicast source and to hosts. There is no multicast router in this topology—hence there is no IGMP querier. Without an IGMP querier to respond to, a host does not send periodic membership reports. As a result, even if the host sends an unsolicited join to join a multicast group, its membership in the multicast group times out.

For IGMP snooping to work correctly in this network so that the switch forwards multicast traffic to Hosts A and C only, you can either:

- Configure interfaces P2 and P4 as static group-member interfaces.
- Configure a routed VLAN interface (RVI) on the VLAN and enable IGMP on it. In this case, the switch itself acts as an IGMP querier, and the hosts can dynamically join the multicast group and refresh their group membership by responding to the queries.
Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

Figure 41: Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs

In the topology shown in Figure 42 on page 3313, a multicast source, Multicast Router A, and Hosts A and B are connected to the switch and are in VLAN 10. Multicast Router B and Hosts C and D are also connected to the switch and are in VLAN 20.

In a pure Layer 2 environment, traffic is not forwarded between VLANs. For Host C to receive the multicast traffic from the source on VLAN 10, RVIs must be created on VLAN 10 and VLAN 20 to permit routing of the multicast traffic between the VLANs. In addition, PIM must be enabled on the switch to perform the multicast routing.
Figure 42: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs

Related Documentation

- Understanding Multicast VLAN Registration
- Example: Configuring IGMP Snooping on EX Series Switches
- Configuring IGMP Snooping (CLI Procedure)
- Configuring Routed VLAN Interfaces (CLI Procedure)
CHAPTER 64

Configuration

- Configuration Examples on page 3315
- Configuration Tasks on page 3318
- Configuration Statements on page 3327

Configuration Examples

- Example: Configuring IGMP Snooping on page 3315

Example: Configuring IGMP Snooping

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see, Example: Configuring IGMP Snooping on EX Series Switches. For ELS details, see, “Getting Started with Enhanced Layer 2 Software” on page 3.

You can enable IGMP snooping on a VLAN to constrain the flooding of IPv4 multicast traffic on a VLAN. When IGMP snooping is enabled, a switch examines IGMP messages between hosts and multicast routers and learns which hosts are interested in receiving multicast traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces that are connected to relevant receivers instead of flooding the traffic to all interfaces.

This example describes how to configure IGMP snooping:

- Requirements on page 3315
- Overview and Topology on page 3316
- Configuration on page 3317
- Verifying IGMP Snooping Operation on page 3318

Requirements

This example uses the following hardware and software components:

- One EX4300 Series switch
Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you configure IGMP snooping, be sure you have:

- Configured a VLAN, vlan100, on the switch
- Assigned interfaces ge-0/0/0, ge-0/0/1, ge-0/0/2, and ge-0/0/12 to vlan100
- Configured ge-0/0/12 as a trunk interface

See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.

Overview and Topology

In this example, interfaces ge-0/0/0, ge-0/0/1, and ge-0/0/2 on the switch are in vlan100 and are connected to hosts that are potential multicast receivers. Interface ge-0/0/12, a trunk interface also in vlan100, is connected to a multicast router. The router acts as the IGMP querier and forwards multicast traffic for group 225.100.100.100 to the switch from a multicast source.

The sample topology is illustrated in Figure 43 on page 3316.

In this sample topology, the multicast router forwards multicast traffic to the switch from the source when it receives a membership report for group 225.100.100.100 from one of the hosts—for example, Host B. If IGMP snooping is not enabled on vlan100, the switch floods the multicast traffic on all interfaces in vlan100 (except for interface ge-0/0/12). If IGMP snooping is enabled on vlan100, the switch monitors the IGMP messages between the hosts and router, allowing it to determine that only Host B is interested in receiving the multicast traffic. The switch then forwards the multicast traffic only to interface ge-0/0/1.
This example shows how to perform the following optional configurations, which can reduce group join and leave latency:

- Configure immediate leave on the VLAN. When immediate leave is configured, the switch stops forwarding multicast traffic on an interface when it detects that the last member of the multicast group has left the group. If immediate leave is not configured, the switch waits until the group-specific queries time out before it stops forwarding traffic.

  Immediate leave is supported by IGMP version 2 (IGMPv2) and IGMPv3. With IGMPv2, we recommend that you configure immediate leave only when there is only one IGMP host on an interface. In IGMPv2, only one host on a interface sends a membership report in response to a group-specific query—any other interested hosts suppress their reports to avoid a flood of reports for the same group. This report-suppression feature implies that the switch knows about only one interested host at any given time.

- Configure ge-0/0/12 as a static multicast-router interface. In this topology, ge-0/0/12 always leads to the multicast router. By statically configuring ge-0/0/12 as a multicast-router interface, you avoid any delay imposed by the switch having to learn that ge-0/0/12 is a multicast-router interface.

### Configuration

To configure IGMP snooping on a switch:

**CLI Quick Configuration**

To quickly configure IGMP snooping, copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols igmp-snooping vlan vlan100 immediate-leave
set protocols igmp-snooping vlan vlan100 interface ge-0/0/12 multicast-router-interface
```

**Step-by-Step Procedure**

To configure IGMP snooping on vlan100:

1. Configure the switch to immediately remove a group membership from an interface when it receives a leave report from the last member of the group on the interface:

   ```
   [edit protocols]
   user@switch# set igmp-snooping vlan vlan100 immediate-leave
   ```

2. Statically configure interface ge-0/0/12 as a multicast-router interface:

   ```
   [edit protocols]
   user@switch# set igmp-snooping vlan vlan100 interface ge-0/0/12 multicast-router-interface
   ```

**Results**

Check the results of the configuration:

```
[edit protocols]
user@switch# show igmp-snooping
vlan vlan100 {
  immediate-leave;
  interface ge-0/0/12.0 {
    multicast-router-interface;
  }
}
```
Verifying IGMP Snooping Operation

To verify that IGMP snooping is operating as configured, perform the following task:

- Displaying IGMP Snooping Information for VLAN vlan100 on page 3318

Displaying IGMP Snooping Information for VLAN vlan100

Purpose

Verify that IGMP snooping is enabled on vlan100 and that ge-0/0/12 is recognized as a multicast-router interface.

Action

Enter the following command:

```
user@switch> show igmp snooping membership
VLAN: vlan100
   Interfaces: ge-0/0/12.0,
```

Meaning

By showing information for vlan100, the command output confirms that IGMP snooping is configured on the VLAN. Interface ge-0/0/12.0 is listed as a multicast-router interface, as configured. Because none of the host interfaces are listed, none of the hosts are currently receivers for the multicast group.

Related Documentation

- Configuring IGMP Snooping (CLI Procedure)
- Verifying IGMP Snooping (CLI Procedure) on page 3410
- IGMP Snooping on EX Series Switches Overview on page 3305

Configuration Tasks

- Configuring IGMP Snooping (CLI Procedure) on page 3318
- Configuring IGMP Snooping (J-Web Procedure) on page 3323
- Configuring IGMP Snooping Tracing Operations (CLI Procedure) on page 3325

Configuring IGMP Snooping (CLI Procedure)

NOTE: This topic uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see: Configuring IGMP Snooping. For ELS details see, “Getting Started with Enhanced Layer 2 Software” on page 3.

Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on a VLAN. When IGMP snooping is enabled, a switch examines IGMP messages between hosts and multicast routers and learns which hosts are interested in receiving multicast traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding the traffic to all interfaces. In IGMPv2, only one host on a interface sends a membership report in response to a group-specific query—any other interested
hosts suppress their reports to avoid a flood of reports for the same group. This
report-suppression feature means that the switch only knows about only one interested
host at any given time.

By default, IGMP snooping is enabled on the default VLAN. For many networks, IGMP
snooping requires no further configuration.

You can perform the following optional configurations for each VLAN:

- Selectively enable IGMP snooping on specific VLANs.
- Enable immediate leave on a VLAN or all VLANs. Enabling immediate leave ensures
  that the switch stops forwarding multicast traffic immediately after the last member
  host on the interface leaves the group.
- Configure an interface as a static multicast-router interface for a VLAN so that the
  switch does not need to dynamically learn that the interface is a multicast-router
  interface.
- Configure an interface as a static member of a multicast group so that the switch does
  not need to dynamically learn the interface’s membership.
- Change the value for certain timers and counters to match the values configured on
  the multicast router serving as the IGMP querier.

This topic covers:

- Enabling IGMP Snooping on VLANs on page 3319
- Enabling Immediate Leave on page 3319
- Configuring an Interface as a Multicast-Router Interface on page 3320
- Configuring Static Group Membership on an Interface on page 3321
- Changing the Timer and Counter Values on page 3322

### Enabling IGMP Snooping on VLANs

This topic describes how you can selectively enable IGMP snooping on VLANs. It assumes
that you are beginning with the factory default configuration.

To enable IGMP snooping on a VLAN:

```
[edit protocols igmp-snooping]
user@switch# set vlan vlan-name
```

You can also deactivate the IGMP snooping protocol on the switch without changing the
IGMP snooping VLAN configurations:

```
[edit]
user@switch# deactivate protocols igmp-snooping
```

### Enabling Immediate Leave

By default, when a switch with IGMP snooping enabled receives an IGMP leave report
on a member interface, it waits for hosts on the interface to respond to IGMP
group-specific queries to determine whether there still are hosts on the interface interested
in receiving the group multicast traffic. If the switch does not see any membership reports for the group within a set interval of time, it removes the interface’s group membership from the multicast forwarding table and stops forwarding multicast traffic for the group to the interface.

You can decrease the leave latency created by this default behavior by enabling immediate leave on a VLAN.

When you enable immediate leave on a VLAN, host tracking is also enabled, which allows the switch to keep track of the hosts on an interface that have joined a multicast group. When the switch receives a leave report from the last member of the group, it immediately stops forwarding traffic to the interface and does not wait for the interface group membership to time out.

Immediate leave is supported for both IGMP version 2 (IGMPv2) and IGMPv3. However, with IGMPv2, we recommend that you configure immediate leave only when there is only one IGMP host on an interface.

To enable immediate leave on a VLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan-name immediate-leave
```

### Configuring an Interface as a Multicast-Router Interface

When IGMP snooping is enabled on a switch, the switch determines which interfaces face a multicast router by monitoring interfaces for IGMP queries. If the switch receives these messages on an interface, it adds the interface to its multicast forwarding table as a multicast-router interface.

In addition to dynamically learned interfaces, the multicast forwarding table can include interfaces that you explicitly configure to be multicast-router interfaces. Unlike the table entries for dynamically learned interfaces, table entries for statically configured interfaces are not subject to aging and deletion from the forwarding table.

Examples of when you might want to configure a static multicast-router interface include:

- You have an unusual network configuration that prevents IGMP snooping from reliably learning about a multicast-router interface through monitoring IGMP queries.
- Your implementation does not require an IGMP querier.
- You have a stable topology and want to avoid the delay the dynamic learning process entails.

**NOTE:** All unregistered multicast packets, whether they are IPv4 or IPv6 packets, are forwarded only to the multicast-router interface.

To configure an interface as a static multicast-router interface:

```
[edit protocols]
```
user@switch# set igmp-snooping vlan vlan-name interface interface-name multicast-router-interface

For example, to configure ge-0/0/5.0 as a multicast-router interface on a VLAN vlan100 on the switch:

[edit protocols]
user@switch# set igmp-snooping vlan vlan100 interface ge-0/0/5.0 multicast-router-interface

Configuring Static Group Membership on an Interface

To determine how to forward multicast packets, a switch with IGMP snooping enabled maintains a multicast forwarding table containing a list of host interfaces that have interested listeners for a specific multicast group. The switch learns which host interfaces to add or delete from this table by examining IGMP membership reports as they arrive on interfaces on which IGMP snooping is enabled.

In addition to such dynamically learned interfaces, the multicast forwarding table can include interfaces that you statically configure to be members of multicast groups. When you configure a static group interface, the switch adds the interface to the forwarding table as a host interface for the group. Unlike an entry for a dynamically learned interface, a static interface entry is not subject to aging and deletion from the forwarding table.

Examples of when you might want to configure static group membership on an interface include:

- You want to simulate an attached multicast receiver for testing purposes.
- The interface has receivers that cannot send IGMP membership reports.
- You want the multicast traffic for a specific group to be immediately available to a receiver without any delay imposed by the dynamic join process.

NOTE: The switch does not simulate IGMP membership reports on behalf of a statically configured interface. Thus a multicast router might be unaware that the switch has an interface that is a member of the multicast group. You can configure a static group interface on the router to ensure that the switch receives the group multicast traffic.

To configure a host interface as a static member of a multicast group:

[edit protocols]
user@switch# set igmp-snooping vlan vlan-name interface interface-name static group ip-address

For example, to configure interface ge-0/0/11.0 in vlan100 as a static member of multicast group 225.0.0.1:

[edit protocols]
user@switch# set igmp-snooping vlan vlan100 interface ge-0/0/11.0 static group 225.0.0.1
Changing the Timer and Counter Values

IGMP uses various timers and counters to determine how often an IGMP querier sends out membership queries and when group memberships time out. On EX Series switches, the default values of the IGMP and IGMP snooping timers and counters are set to the values recommended in RFC 2236, *Internet Group Management Protocol, Version 2*. These values work well for most multicast implementations.

There might be cases, however, where you might want to modify the timer and counter values—for example, to reduce burstiness, to reduce leave latency, or to adjust for expected packet loss on a subnet. If you change a timer or counter value for the IGMP querier on a VLAN, we recommend that you change the value for all multicast routers and switches on the VLAN so that all devices time out group memberships at approximately the same time.

You can configure the following timers and counters on a switch:

- **query-interval**—The length of time the IGMP querier waits between sending general queries (the default is 125 seconds). You can change this interval to tune the number of IGMP messages on the subnet; larger values cause general queries to be sent less often.

  You cannot configure this value directly for IGMP snooping. IGMP snooping inherits the value from the IGMP value configured on the switch, which is applied to all VLANs on the switch.

  To configure the IGMP query-interval:

  ```
  [edit protocols]
  user@switch# set igmp-snooping vlan vlan-name query-interval seconds
  ```

- **query-response-interval**—The maximum length of time the host can wait until it responds (the default is 10 seconds). You can change this interval to adjust the burst peaks of IGMP messages on the subnet. Set a larger interval to make the traffic less bursty.

  You cannot configure this value directly for IGMP snooping. IGMP snooping inherits the value from the IGMP value configured on the switch, which is applied to all VLANs on the switch.

  To configure the IGMP query-response-interval:

  ```
  [edit protocols]
  user@switch# set igmp-snooping vlan vlan-name query-response-interval seconds
  ```

- **query-last-member-interval**—The length of time the IGMP querier waits between sending group-specific membership queries (the default is 1 second). The IGMP querier sends a group-specific query after receiving a leave report from a host. You can decrease this interval to reduce the amount of time it takes for multicast traffic to stop forwarding traffic after the last member leaves a group.
You cannot configure this value directly for IGMP snooping. IGMP snooping inherits the value from the IGMP value configured on the switch, which is applied to all VLANs on the switch.

To configure the IGMP query-last-member-interval:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan-name query-last-member-interval seconds
```

- **robust-count**—The number of times the querier resends a general membership query or a group-specific membership query (the default is 2 times). You can increase this count to tune for higher expected packet loss.

For IGMP snooping, you can configure `robust-count` for a specific VLAN. If a VLAN does not have `robust-count` configured, the robust-count value is the value configured for IGMP.

To configure `robust-count` for IGMP snooping on a VLAN:

```
[edit protocols]
user@switch# set igmp-snooping vlan vlan-name robust-count number
```

The values configured for `query-interval`, `query-response-interval`, and `robust-count` determine the multicast listener interval—the length of time the switch waits for a group membership report after a general query before removing a multicast group from its multicast forwarding table. The switch calculates the multicast listener interval by multiplying `query-interval` by the `robust-count` and then adding `query-response-interval` to the product:

\[(query-interval \times robust-count) + query-response-interval = multicast listener interval.\]

For example, the multicast listener interval is 260 seconds when the default settings for `query-interval`, `query-response-interval`, and `robust-count` are used:

\[(125 \times 2) + 10 = 260\]

You can display the time remaining in the multicast listener interval before a group times out by using the `show igmp-snooping membership` command.

---

### Related Documentation
- Example: Configuring IGMP Snooping on page 3315
- Verifying IGMP Snooping (CLI Procedure) on page 3410
- IGMP Snooping on EX Series Switches Overview on page 3305

### Configuring IGMP Snooping (J-Web Procedure)

IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, the EX Series switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.
You can configure IGMP snooping on one or more VLANs to allow the switch to examine IGMP packets and make forwarding decisions based on packet content. By default, IGMP snooping is enabled on EX Series switches.

To enable IGMP snooping and configure individual options by using the J-Web interface:

1. Select **Configure > Switching > IGMP Snooping**.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Creates an IGMP snooping configuration for the VLAN.
   - **Edit**—Modifies an IGMP snooping configuration for the VLAN.
   - **Delete**—Deletes a selected VLAN from the IGMP snooping configuration.

   When you are adding or editing an IGMP snooping configuration, enter information as described in Table 400 on page 3324.

3. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.

To disable IGMP snooping on a VLAN, select the VLAN from the list and click **Disable**.

**NOTE:** The Disable option is not available for EX4300 switches.

### Table 400: IGMP Snooping Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>Specifies the VLAN on which to enable IGMP snooping.</td>
<td>Select a VLAN from the list to add it to the snooping configuration.</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>Immediately removes a multicast group membership from an interface when it receives a leave message from that interface without waiting for any other IGMP messages to be exchanged (IGMP version 2 and IGMP version 3 only).</td>
<td>To enable the option, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To disable the option, clear the check box.</td>
</tr>
<tr>
<td>Robust Count</td>
<td>Specifies the number of timeout intervals the switch waits before timing out a multicast group.</td>
<td>Type a value.</td>
</tr>
</tbody>
</table>
Table 400: IGMP Snooping Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces List</td>
<td>Statically configures an interface as a switching interface toward a multicast router or as a member of a multicast group.</td>
<td>Click one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add—Adds an interface to the IGMP snooping configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select an interface from the list. For an EX8200 Virtual Chassis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration, select the member, FPC, and the interface from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select Multicast Router Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Type the maximum number of groups an interface can join.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. In Static, choose one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click Add, type a group IP address, and click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select a group and click Remove to remove the group membership.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Edit—Edits the interface settings for the IGMP snooping configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remove—Deletes an interface configured for IGMP snooping.</td>
</tr>
</tbody>
</table>

Related Documentation
- Example: Configuring IGMP Snooping on EX Series Switches
- Configuring IGMP Snooping (CLI Procedure)
- IGMP Snooping on EX Series Switches Overview on page 3305

Configuring IGMP Snooping Tracing Operations (CLI Procedure)

By enabling tracing operations for IGMP snooping, you can record detailed messages about the operation of the protocol, such as the various types of protocol packets sent and received. Table 401 on page 3325 describes the tracing operations you can enable and the flags used to specify them in the tracing configuration.

Table 401: Supported Tracing Operations for IGMP Snooping

<table>
<thead>
<tr>
<th>Tracing Operation</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace all (equivalent of including all flags).</td>
<td>all</td>
</tr>
<tr>
<td>Trace general IGMP snooping protocol events.</td>
<td>general</td>
</tr>
<tr>
<td>Trace communication over routing socket events.</td>
<td>krt</td>
</tr>
<tr>
<td>Trace leave reports (IGMPv2 and IGMPv3 only).</td>
<td>leave</td>
</tr>
</tbody>
</table>
Table 401: Supported Tracing Operations for IGMP Snooping (continued)

<table>
<thead>
<tr>
<th>Tracing Operation</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace nexthop-related events.</td>
<td>nexthop</td>
</tr>
<tr>
<td>Trace normal IGMP snooping protocol events. If you do not specify this flag, only unusual or abnormal operations are traced.</td>
<td>normal</td>
</tr>
<tr>
<td>Trace all IGMP packets.</td>
<td>packets</td>
</tr>
<tr>
<td>Trace policy processing.</td>
<td>policy</td>
</tr>
<tr>
<td>Trace IGMP membership query messages.</td>
<td>query</td>
</tr>
<tr>
<td>Trace membership reports</td>
<td>report</td>
</tr>
<tr>
<td>Trace routing information.</td>
<td>route</td>
</tr>
<tr>
<td>Trace state transitions.</td>
<td>state</td>
</tr>
<tr>
<td>Trace routing protocol task processing.</td>
<td>task</td>
</tr>
<tr>
<td>Trace timer processing.</td>
<td>timer</td>
</tr>
<tr>
<td>Trace VLAN-related events.</td>
<td>vlan</td>
</tr>
</tbody>
</table>

This topic covers:

- Configuring Tracing Operations on page 3326
- Viewing, Stopping, and Restarting Tracing Operations on page 3327

**Configuring Tracing Operations**

To configure tracing operations for IGMP snooping:

1. Configure the filename for the trace file:

   ```
   [edit protocols igmp-snooping ]
   user@switch# set traceoptions file filename
   ```

   For example:

   ```
   [edit protocols igmp-snooping ]
   user@switch# set traceoptions file mld-snoop-trace
   ```

2. (Optional) Configure the maximum number of trace files and size of the trace files:

   ```
   [edit protocols igmp-snooping ]
   user@switch# set traceoptions file files number size size
   ```

   For example:

   ```
   [edit protocols igmp-snooping ]
   user@switch# set traceoptions file files 5 size 1m
causes the contents of the trace file to be emptied and archived in a .gz file when the file reaches 1 MB. Four archive files are maintained, the contents of which are rotated whenever the current active trace file is archived.

If you omit this step, the maximum number of trace files defaults to 10, with the maximum file size defaulting to 128 K.

3. Specify one of the tracing flags shown in Table 401 on page 3325:

```
[edit protocols igmp-snooping ]
user@switch# set traceoptions flag flagname
```

For example, to perform trace operations on VLAN-related events and IGMP query messages:

```
[edit protocols igmp-snooping ]
user@switch# set traceoptions flag vlan
[edit protocols igmp-snooping ]
user@switch# set traceoptions flag query
```

**Viewing, Stopping, and Restarting Tracing Operations**

When you commit the configuration, tracing operations begin. You can view the trace file in the `/var/log` directory. For example:

```
user@switch> file show /var/log/igmp-snoop-trace
```

You can stop and restart tracing operations by deactivating and reactivating the configuration:

```
[edit]
user@switch# deactivate protocols igmp-snooping traceoptions

[edit]
user@switch# activate protocols igmp-snooping traceoptions
```

**Related Documentation**

- Configuring IGMP Snooping (CLI Procedure)
- Junos OS Tracing and Logging Operations

**Configuration Statements**

- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
- [edit protocols igmp-snooping] Configuration Statement Hierarchy on page 3329

**[edit protocols] Configuration Statement Hierarchy on EX Series Switches**

Each of the following topics lists the statements at a subhierarchy of the [edit protocols] hierarchy:

- [edit protocols bfd] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols bgp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols connections] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols dcbx] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches on page 1769
• [edit protocols igmp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols igmp-snooping] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols isis] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols lacp] Configuration Statement Hierarchy on EX Series Switches on page 2398
• [edit protocols link-management] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols lldp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols lldp-med] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols mld] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols mld-snooping] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols mpls] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols msdp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols mstp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols mvrp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols neighbor-discovery] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols oam] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols ospf] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols ospf3] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols pim] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols rip] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols ripng] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols router-advertisement] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols router-discovery] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols rstp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols rsvp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols sflow] Configuration Statement Hierarchy on EX Series Switches on page 3708
• [edit protocols stp] Configuration Statement Hierarchy on EX Series Switches
[edit protocols uplink-failure-detection] Configuration Statement Hierarchy on EX Series Switches

[edit protocols vrrp] Configuration Statement Hierarchy on EX Series Switches

[edit protocols vstp] Configuration Statement Hierarchy on EX Series Switches

Related Documentation

- EX Series Switch Software Features Overview on page 27
- EX Series Virtual Chassis Software Features Overview on page 75
- Junos® OS for EX Series Switches, Release 13.2X50

[edit protocols igmp-snooping] Configuration Statement Hierarchy

This topic lists supported and unsupported configuration statements in the [edit protocols igmp-snooping] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.

- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit protocols igmp-snooping] Hierarchy Level on page 3329
- Unsupported Statements in the [edit protocols igmp-snooping] Hierarchy Level on page 3330

**Supported Statements in the [edit protocols igmp-snooping] Hierarchy Level**

The following hierarchy shows the [edit protocols igmp-snooping] configuration statements supported on EX Series switches:

```c
protocols {
    igmp-snooping {
        vlan vlan-name {
            immediate-leave;
            interface interface-name {
                group-limit <1..65535>
                host-only-interface
                multicast-router-interface;
                immediate-leave;
                static {
                    group multicast-ip-address {
                        source <>
                    }
                }
            }
        }
    }
}
```
l2-querier {
  source-address ip-address;
}
proxy {
  source-address ip-address;
}
query-interval number;
query-last-member-interval number;
query-response-interval number;
robust-count number;
traceoptions {
  file filename <files number> <no-stamp> <replace> <size maximum-file-size> <world-readable | no-world-readable>;
  flag flag <flag-modifier>;
}
}
}

Unsupported Statements in the [edit protocols igmp-snooping] Hierarchy Level

All statements in the [edit protocols igmp-snooping] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation
- [edit protocols] Configuration Statement Hierarchy on EX Series Switches

accounting (Protocols IGMP Interface)

Syntax  (accounting | no-accounting);

Hierarchy Level  [edit logical-systems logical-system-name protocols igmp interface interface-name],
[edit protocols igmp interface interface-name]

Release Information  Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description  Enable or disable the collection of IGMP join and leave event statistics for an interface.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  • Recording IGMP Join and Leave Events
accounting (Protocols IGMP)

Syntax  accounting;

Hierarchy Level  [edit logical-systems logical-system-name protocols igmp],
[edit protocols igmp]

Release Information  Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description  Enable the collection of IGMP join and leave event statistics on the system.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  • Recording IGMP Join and Leave Events

address (Anycast RPs)

Syntax  address address <forward-msdp-sa>;

Hierarchy Level  [edit logical-systems logical-system-name protocols pim rp local (inet | inet6) anycast-pim rp-set],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp local (inet | inet6) anycast-pim rp-set],
[edit protocols pim rp local (inet | inet6) anycast-pim rp-set],
[edit routing-instances routing-instance-name protocols pim rp local (inet | inet6) anycast-pim rp-set]

Release Information  Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Configure the anycast rendezvous point (RP) addresses in the RP set. Multiple addresses can be configured in an RP set. If the RP has peer Multicast Source Discovery Protocol (MSDP) connections, then the RP must forward MSDP source active (SA) messages.

Options  address—RP address in an RP set.
forward-msdp-sa—(Optional) Forward MSDP SAs to this address.

Required Privilege Level  routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
**address (Local RPs)**

**Syntax**

```
address address;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols pim rp local family (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp local family (inet | inet6)],
[edit protocols pim rp local family (inet | inet6)],
[edit routing-instances routing-instance-name protocols pim rp local family (inet | inet6)]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure the local rendezvous point (RP) address.

**Options**

`address`—Local RP address.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring Local PIM RPs](#)

---

**anycast-pim**

**Syntax**

```
anycast-pim {
  rp-set {
    address address <forward-msdp-sa>;
  }
}
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols pim rp local family (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp local family (inet | inet6)],
[edit protocols pim rp local family (inet | inet6)],
[edit routing-instances routing-instance-name protocols pim rp local family (inet | inet6)]
```

**Release Information**

- Statement introduced in Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure properties for anycast RP using PIM.

The remaining statements are explained separately.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring PIM Anycast With or Without MSDP](#)
### assert-timeout

**Syntax**

```plaintext
assert-timeout seconds;
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name protocols pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
[edit protocols pim],
[edit routing-instances routing-instance-name protocols pim]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Multicast routing devices running PIM sparse mode often forward the same stream of multicast packets onto the same LAN through the rendezvous-point tree (RPT) and shortest-path tree (SPT). PIM assert messages help routing devices determine which routing device forwards the traffic and prunes the RPT for this group. By default, routing devices enter an assert cycle every 180 seconds. You can configure this assert timeout to be between 5 and 210 seconds.

**Options**

- `seconds`—Time for routing device to wait before another assert message cycle.
  - **Range:** 5 through 210 seconds
  - **Default:** 180 seconds

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring the PIM Assert Timeout](#)
**auto-rp**

**Syntax**
```
auto-rp {  
(announce | discovery | mapping);  
(mapping-agent-election | no-mapping-agent-election);  
}
```

**Hierarchy Level**
- `edit logical-systems logical-system-name protocols pim rp`
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp`
- `edit protocols pim rp`
- `edit routing-instances routing-instance-name protocols pim rp`

**Release Information**
Statement introduced in Junos OS Release 7.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Configure automatic RP announcement and discovery.

**Options**
- `announce`—Configure the routing device to listen only for mapping packets and also to advertise itself if it is an RP.
- `discovery`—Configure the routing device to listen only for mapping packets.
- `mapping`—Configures the routing device to announce, listen for and generate mapping packets, and announce that the routing device is eligible to be an RP.

The remaining statement is explained separately.

**Required Privilege Level**
- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring PIM Auto-RP
**bootstrap**

**Syntax**

```plaintext
bootstrap {
  family (inet | inet6) {
    export [policy-names ];
    import [policy-names ];
    priority number;
  }
}
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols pim rp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
- [edit protocols pim rp],
- [edit routing-instances routing-instance-name protocols pim rp]

**Release Information**

- Statement introduced in Junos OS Release 7.6.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure parameters to control bootstrap routers and messages.

The remaining statements are explained separately.

**Required Privilege**

- **Level**
  - routing—to view this statement in the configuration.
  - routing-control—to add this statement to the configuration.

**Related Documentation**

- Configuring PIM Bootstrap Properties for IPv4
- Configuring PIM Bootstrap Properties for IPv4 or IPv6
### bootstrap-export

**Syntax**

```plaintext
bootstrap-export [ policy-names ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols pim rp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
- [edit protocols pim rp],
- [edit routing-instances routing-instance-name protocols pim rp]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Apply one or more export policies to control outgoing PIM bootstrap messages.

**Options**

- `policy-names`—Name of one or more import policies.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring PIM Bootstrap Properties for IPv4
- Configuring PIM Bootstrap Properties for IPv4 or IPv6
- bootstrap-import on page 3337
## bootstrap-import

**Syntax**

```
bootstrap-import [ policy-names ];
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols pim rp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
- [edit protocols pim rp],
- [edit routing-instances routing-instance-name protocols pim rp]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Apply one or more import policies to control incoming PIM bootstrap messages.

**Options**

- `policy-names`—Name of one or more import policies.

**Required Privilege**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring PIM Bootstrap Properties for IPv4](#)
- [Configuring PIM Bootstrap Properties for IPv4 or IPv6](#)
- [bootstrap-export on page 3336](#)
**bootstrap-priority**

**Syntax**

```
bootstrap-priority number;
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols pim rp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
- [edit protocols pim rp],
- [edit routing-instances routing-instance-name protocols pim rp]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure whether this routing device is eligible to be a bootstrap router. In the case of a tie, the routing device with the highest IP address is elected to be the bootstrap router.

**Options**

- `number`—Priority for becoming the bootstrap router. A value of 0 means that the routing device is not eligible to be the bootstrap router.
  - **Range:** 0 through 255
  - **Default:** 0

**Required Privilege**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring PIM Bootstrap Properties for IPv4
data-forwarding

Syntax

```
data-forwarding {
    receiver {
        source-vlans vlan-list;
        install;
    }
    source {
        groups group-prefix;
    }
}
```

Hierarchy Level

[edit protocols igmp-snooping vlan (all | vlan-name )]

Release Information

Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for the QFX Series.

Description

Configure the VLAN to be a multicast source VLAN (MVLAN) or a multicast VLAN registration (MVR) receiver VLAN. Each data-forwarding VLAN, which can be a multicast source VLAN (MVLAN) or a multicast receiver VLAN, must have exactly one source statement or exactly one receiver statement. A data-forwarding VLAN can operate only in IGMP version 2 (IGMPv2) mode.

The remaining statements are explained separately.

Default

Disabled

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring Multicast VLAN Registration
- Configuring Multicast VLAN Registration (CLI Procedure)
dense-groups

Syntax

dense-groups {
  addresses;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
[edit protocols pim],
[edit routing-instances routing-instance-name protocols pim]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure which groups are operating in dense mode.

Options
addresses—Address of groups operating in dense mode.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring PIM Sparse-Dense Mode Properties

disable (IGMP Snooping)

Syntax
disable;

Hierarchy Level
[edit protocols igmp-snooping vlan (all | vlan-name)]

Release Information
Statement introduced in Junos OS Release 9.2 for EX Series switches.

Description
Disable IGMP snooping on the VLAN. Multicast traffic will be flooded to all interfaces on the VLAN except the source interface.

Default
If you do not include this statement in the configuration for a VLAN, IGMP snooping is enabled on the VLAN.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring IGMP Snooping (CLI Procedure)
• show igmp-snooping vlans
**disable (Protocols IGMP)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>disable;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hierarchy Level</strong></td>
<td>[edit logical-systems logical-system-name protocols igmp interface interface-name], [edit protocols igmp interface interface-name]</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Disable IGMP on the system.</td>
</tr>
<tr>
<td><strong>Required Privilege Level</strong></td>
<td>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td><strong>Related Documentation</strong></td>
<td>• Disabling IGMP</td>
</tr>
</tbody>
</table>
**disable (PIM)**

**Syntax**

`disable;`

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols pim],
[edit logical-systems logical-system-name protocols pim family (inet | inet6)],
[edit logical-systems logical-system-name protocols pim interface interface-name],
[edit logical-systems logical-system-name protocols pim rp local family (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp local family (inet | inet6)],
[edit protocols pim],
[edit protocols pim family (inet | inet6)],
[edit protocols pim interface interface-name],
[edit protocols pim rp local family (inet | inet6)],
[edit routing-instances routing-instance-name protocols pim],
[edit routing-instances routing-instance-name protocols pim family (inet | inet6)],
[edit routing-instances routing-instance-name protocols pim interface interface-name],
[edit routing-instances routing-instance-name protocols pim rp local family (inet | inet6)]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Explicitly disable PIM at the protocol, interface or family hierarchy levels.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- *Disabling PIM*
- `disable (PIM Graceful Restart)`
dr-election-on-p2p

Syntax  
dr-election-on-p2p;

Hierarchy Level  
[edit logical-systems logical-system-name protocols pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
[edit protocols pim],
[edit routing-instances routing-instance-name protocols pim]

Release Information  
Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Enable PIM designated router (DR) election on point-to-point (P2P) links.

Default  
No PIM DR election is performed on point-to-point links.

Required Privilege  
Level  
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation  
• Configuring PIM Designated Router Election on Point-to-Point Links

dr-register-policy

Syntax  
dr-register-policy [ policy-names ];

Hierarchy Level  
[edit logical-systems logical-system-name protocols pim rp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
[edit protocols pim rp],
[edit routing-instances routing-instance-name protocols pim rp]

Release Information  
Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  
Apply one or more policies to control outgoing PIM register messages.

Options  
policy-names—Name of one or more import policies.

Required Privilege  
Level  
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation  
• Configuring Register Message Filters on a PIM RP and DR
• rp-register-policy on page 3387
**embedded-rp**

**Syntax**
```
embedded-rp {
  group-ranges {
    destination-ip-prefix</prefix-length>;
  }
  maximum-rps limit;
}
```

**Hierarchy Level**
- [edit logical-systems logical-system-name protocols pim rp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
- [edit protocols pim rp],
- [edit routing-instances routing-instance-name protocols pim rp]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Configure properties for embedded IP version 6 (IPv6) RPs.

The remaining properties are explained separately.

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- Configuring PIM Embedded RP for IPv6
### export (Protocols PIM Bootstrap)

**Syntax**

```
export [ policy-names ];
```

**Hierarchy Level**

- `edit logical-systems logical-system-name protocols pim rp bootstrap family (inet | inet6)`
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp bootstrap family (inet | inet6)`
- `edit protocols pim rp bootstrap family (inet | inet6)`
- `edit routing-instances routing-instance-name protocols pim rp bootstrap family (inet | inet6)`

**Release Information**

- Statement introduced in Junos OS Release 7.6.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Apply one or more export policies to control outgoing PIM bootstrap messages.

**Options**

- `policy-names`—Name of one or more import policies.

**Required Privilege**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring PIM Bootstrap Properties for IPv4
- Configuring PIM Bootstrap Properties for IPv4 or IPv6
- import (Protocols PIM Bootstrap) on page 3356
family (Bootstrap)

Syntax
family (inet | inet6) {
    export [ policy-names ];
    import [ policy-names ];
    priority number;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols pim rp bootstrap],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp bootstrap],
[edit protocols pim rp bootstrap],
[edit routing-instances routing-instance-name protocols pim rp bootstrap]

Release Information
Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure which IP protocol type bootstrap properties to apply.

Options
inet—Apply IP version 4 (IPv4) local RP properties.
inet6—Apply IPv6 local RP properties.

The remaining statements are explained separately.

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Configuring PIM Bootstrap Properties for IPv4
• Configuring PIM Bootstrap Properties for IPv4 or IPv6
family (Local RP)

Syntax

```plaintext
family (inet | inet6) {
  disable;
  address address;
  anycast-pim {
    local-address address;
    rp-set {
      address address <forward-msdp-sa>;
    }
  }
  group-ranges {
    destination-ip-prefix </prefix-length>;
  }
  hold-time seconds;
  override;
  priority number;
}
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols pim rp local],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp local],
- [edit protocols pim rp local],
- [edit routing-instances routing-instance-name protocols pim rp local]

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure which IP protocol type local RP properties to apply.

Options

- `inet`—Apply IP version 4 (IPv4) local RP properties.
- `inet6`—Apply IPv6 local RP properties.

The remaining statements are explained separately.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Local PIM RPs
graceful-restart (Protocols PIM)

Syntax
```
graceful-restart {
  disable;
  no-bidirectional-mode;
  restart-duration seconds;
}
```

Hierarchy Level
- `[edit logical-systems logical-system-name protocols pim]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim]`
- `[edit protocols pim]`
- `[edit routing-instances routing-instance-name protocols pim]`

Release Information
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure PIM sparse mode graceful restart.

The remaining statements are explained separately.

Required Privilege
- Level: `routing`—To view this statement in the configuration.
- Level: `routing-control`—To add this statement to the configuration.

Related Documentation
- Configuring PIM Sparse Mode Graceful Restart

---

group (IGMP Snooping)

Syntax
```
group ip-address;
```

Hierarchy Level
- `[edit protocols igmp-snooping vlan (all | vlan-name) interface (all | interface-name) static]`

Release Information
- Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Configure a static multicast group on an interface.

Options
- `ip-address`—Valid IP multicast address for the multicast group.

Required Privilege
- Level: `routing`—To view this statement in the configuration.
- Level: `routing-control`—To add this statement to the configuration.

Related Documentation
- Configuring IGMP Snooping (CLI Procedure)
- show igmp-snooping membership on page 3453
group (Protocols IGMP)

Syntax

```plaintext
group multicast-group-address {
    exclude;
    group-count number;
    group-increment increment;
    source ip-address {
        source-count number;
        source-increment increment;
    }
}
```

Hierarchy Level

[edit logical-systems logical-system-name protocols igmp interface interface-name static],
[edit protocols igmp interface interface-name static]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Specify the IGMP multicast group address and (optionally) the source address for the multicast group being statically configured on an interface.

NOTE: You must specify a unique address for each group.

The remaining statements are explained separately.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Enabling IGMP Static Group Membership
**group-ranges**

**Syntax**

```plaintext
group-ranges {
    destination-ip-prefix</prefix-length>;
}
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name protocols pim rp bidirectional address address],
[edit logical-systems logical-system-name protocols pim rp embedded-rp],
[edit logical-systems logical-system-name routing-instances instance-name protocols pim rp bidirectional address address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp embedded-rp],
[edit protocols pim rp bidirectional address address],
[edit protocols pim rp embedded-rp],
[edit protocols pim rp local family (inet | inet6)],
[edit protocols pim rp static address address],
[edit routing-instances instance-name protocols pim rp bidirectional address address],
[edit routing-instances routing-instance-name protocols pim rp embedded-rp],
[edit routing-instances routing-instance-name protocols pim rp local family (inet | inet6)],
[edit routing-instances routing-instance-name protocols pim rp static address address]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional RP addresses introduced in Junos OS Release 12.1.

**Description**

Configure the address ranges of the multicast groups for which this routing device can be a rendezvous point (RP).

**Default**

The routing device is eligible to be the RP for all IPv4 or IPv6 groups (224.0.0.0/4 or FF70::/12 to FFF0::/12).

**Options**

`destination-ip-prefix</prefix-length>`—Addresses or address ranges for which this routing device can be an RP.

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring Local PIM RPs in the Multicast Protocols Feature Guide for Routing Devices
- Configuring PIM Embedded RP for IPv6 in the Multicast Protocols Feature Guide for Routing Devices
- Example: Configuring Bidirectional PIM
hello-interval (Protocols PIM)

Syntax

```
hello-interval seconds;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols pim interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim interface interface-name],
[edit protocols pim interface interface-name],
[edit routing-instances routing-instance-name protocols pim interface interface-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Specify how often the routing device sends PIM hello packets out of an interface.

Options

- **seconds**—Length of time between PIM hello packets.
  - Range: 0 through 255
  - Default: 30 seconds

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- hold-time on page 3352
- Modifying the PIM Hello Interval
**hold-time (Protocols PIM)**

**Syntax**

```
hold-time seconds;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols pim rp bidirectional address address],
[edit logical-systems logical-system-name routing-instances instance-name protocols pim rp bidirectional address address],
[edit protocols pim rp bidirectional address address],
[edit protocols pim rp local family (inet | inet6)],
[edit routing-instances instance-name protocols pim rp bidirectional address address],
[edit routing-instances routing-instance-name protocols pim rp local family (inet | inet6)]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional RP addresses introduced in Junos OS Release 12.1.

**Description**

Specify the time period for which a neighbor is to consider the sending routing device (this routing device) to be operative (up).

**Options**

- **seconds**—Hold time.
  - **Range:** 0 through 255
  - **Default:** 150 seconds

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Local PIM RPs in the Multicast Protocols Feature Guide for Routing Devices
- Example: Configuring Bidirectional PIM
### igmp-snooping

**Syntax**

```plaintext
igmp-snooping {
    traceoptions {
        file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
        flag flag <flag-modifier>;
    }
    vlan (all | vlan-name) {
        data-forwarding {
            source {
                groups group-prefix;
            }
            receiver {
                source-vlans vlan-list;
                install;
            }
        }
        disable;
        immediate-leave;
        interface (all | interface-name) {
            multicast-router-interface;
            static {
                group ip-address;
            }
        }
        proxy {
            source-address ip-address;
        }
        robust-count number;
        version version;
    }
}
```

**Hierarchy Level**

```
[edit protocols]
```

**Release Information**

Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description**

Configure IGMP snooping. The factory default configuration enables IGMP snooping on all VLANs.

The remaining statements are explained separately.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring IGMP Snooping on EX Series Switches
- Configuring IGMP Snooping (CLI Procedure)
### immediate-leave (Protocols IGMP)

**Syntax**

immediate-leave;

**Hierarchy Level**

[edit logical-systems logical-system-name protocols igmp]
[edit protocols igmp interface interface-name]

**Release Information**

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

The immediate leave setting is useful for minimizing the leave latency of IGMP memberships. When this setting is enabled, the routing device leaves the multicast group immediately after the last host leaves the multicast group.

Starting in Junos OS Release 9.3, both IGMP version 2 and IGMP version 3 do host tracking when the `immediate-leave` statement is configured. This means that the multicast group leaves only when the last host leaves. The routing device keeps track of the hosts that send join messages. This allows IGMP to determine when the last host sends a leave message for the multicast group.

When the immediate leave setting is enabled, the device removes an interface from the forwarding-table entry without first sending IGMP group-specific queries to the interface. The interface is pruned from the multicast tree for the multicast group specified in the IGMP leave message. The immediate leave setting ensures optimal bandwidth management for hosts on a switched network, even when multiple multicast groups are being used simultaneously.

When immediate leave is disabled and one host sends a leave group message, the routing device first sends a group query to determine if another receiver responds. If no receiver responds, the routing device removes all hosts on the interface from the multicast group.

Immediate leave is disabled by default for both IGMP version 2 and IGMP version 3.

**Note:** Although host tracking is enabled for IGMPv2 and MLDv1 when you enable immediate leave, use immediate leave with these versions only when there is one host on the interface. The reason is that IGMPv2 and MLDv1 use a report suppression mechanism whereby only one host on an interface sends a group join report in response to a membership query. The other interested hosts suppress their reports. The purpose of this mechanism is to avoid a flood of reports for the same group. But it also interferes with host tracking, because the routing device only knows about the one interested host and does not know about the others.

**Required Privilege Level**

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.
Related Documentation

• Specifying Immediate-Leave Host Removal for IGMP

immediate-leave (IGMP Snooping)

Syntax
immediate-leave;

Hierarchy Level
[edit protocols igmp-snooping vlan (all | vlan-name)]

Release Information
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Configure IGMP snooping immediate leave for the specified VLAN. When you configure immediate leave, host tracking is enabled, which allows the switch to track the hosts that send membership reports. The switch can then determine when the last host on an interface leaves the multicast group and immediately stop forwarding multicast traffic to the interface.

Configuring immediate leave reduces the amount of time it takes for the switch to stop sending multicast traffic to an interface when the last host leaves the group. When immediate leave is disabled, the switch no longer tracks hosts. Instead, whenever it receives a leave report from a host, it sends out a group-specific query to all hosts. If it does not receive any membership reports on the interface in response to the group-specific query within a set interval, it stops forwarding multicast traffic to the interface.

NOTE: Immediate leave is supported for both IGMP version 2 (IGMPv2) and IGMPv3. However, with IGMPv2, we recommend that you configure immediate leave only when there is only one IGMP host on an interface. In IGMPv2, only one host on an interface sends a membership report in response to a general query—any other interested hosts suppress their reports. Report suppression avoids a flood of reports for the same group, but it also interferes with host tracking because the switch knows only about one interested host on the interface at any given time.

Default
The immediate-leave feature is disabled.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring IGMP Snooping on EX Series Switches
• Configuring IGMP Snooping (CLI Procedure)
import (Protocols PIM Bootstrap)

Syntax
import [ policy-names ];

Hierarchy Level
[edit logical-systems logical-system-name protocols pim rp bootstrap (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp bootstrap (inet | inet6)],
[edit protocols pim rp bootstrap (inet | inet6)],
[edit routing-instances routing-instance-name protocols pim rp bootstrap (inet | inet6)]

Release Information
Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Apply one or more import policies to control incoming PIM bootstrap messages.

Options
policy-names—Name of one or more import policies.

Required Privilege
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Configuring PIM Bootstrap Properties for IPv4
• Configuring PIM Bootstrap Properties for IPv4 or IPv6
• export (Protocols PIM Bootstrap) on page 3345
**import (Protocols PIM)**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>import [ policy-names ];</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit logical-systems logical-system-name protocols pim], [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim], [edit protocols pim], [edit routing-instances routing-instance-name protocols pim]</td>
</tr>
<tr>
<td>Description</td>
<td>Apply one or more policies to routes being imported into the routing table from PIM. Use the <code>import</code> statement to filter PIM join messages and prevent them from entering the network.</td>
</tr>
<tr>
<td>Options</td>
<td><code>policy-names</code>—Name of one or more policies.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• <em>Filtering Incoming PIM Join Messages</em></td>
</tr>
</tbody>
</table>
infinity

Syntax  infinity [ policy-names ];

Hierarchy Level  [edit logical-systems logical-system-name protocols pim spt-threshold],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim spt-threshold],
[edit protocols pim spt-threshold],
[edit routing-instances routing-instance-name protocols pim spt-threshold]

Release Information  Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Apply one or more policies to set the SPT threshold to infinity for a source-group address pair. Use the infinity statement to prevent the last-hop routing device from transitioning from the RPT rooted at the RP to an SPT rooted at the source for that source-group address pair.

Options  policy-names—Name of one or more policies.

Required Privilege Level  routing—to view this statement in the configuration.
 routing-control—to add this statement to the configuration.

Related Documentation  • Example: Configuring the PIM SPT Threshold Policy
interface (IGMP Snooping)

Syntax

interface (all | interface-name) {
  multicast-router-interface;
  static {
    group ip-address;
  }
}

Hierarchy Level

[edit protocols igmp-snooping vlan (all | vlan-name)]

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description

For IGMP snooping, configure an interface as either a multicast-router interface or as a static member of a multicast group.

Options

all—All interfaces in the VLAN.

interface-name—Name of the interface.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring IGMP Snooping on EX Series Switches
- Configuring IGMP Snooping (CLI Procedure)
- show igmp-snooping vlans
interface (Protocols PIM)

Syntax

```plaintext
interface (Protocols PIM) (all | interface-name) {
    accept-remote-source;
    disable;
    bfd-liveness-detection {
        authentication {
            algorithm algorithm-name;
            key-chain key-chain-name;
            loose-check;
        }
        detection-time {
            threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (0 | 1 | automatic);
    }
    bidirectional {
        df-election {
            backoff-period milliseconds;
            offer-period milliseconds;
            robustness-count number;
        }
    }
    family (inet | inet6) {
        bfd-liveness-detection {
            authentication {
                algorithm algorithm-name;
                key-chain key-chain-name;
                loose-check;
            }
            detection-time {
                threshold milliseconds;
            }
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (0 | 1 | automatic);
        }
        disable;
    }
    hello-interval seconds;
}
```
mode (bidirectional-sparse | bidirectional-sparse-dense | dense | sparse | sparse-dense);
neighbor-policy [ policy-names ];
override-interval milliseconds;
priority number;
propagation-delay milliseconds;
reset-tracking-bit;
version version;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
[edit protocols pim],
[edit routing-instances routing-instance-name protocols pim]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Enable PIM on an interface and configure interface-specific properties.

Options

interface-name—Name of the interface. Specify the full interface name, including the physical and logical address components. To configure all interfaces, you can specify all.

The remaining statements are explained separately.

Required Privilege
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• PIM on Aggregated Interfaces
interface (Protocols IGMP)

Syntax

```
interface interface-name {
    disable;
    (accounting | no-accounting);
    group-limit limit;
    group-policy [ policy-names ];
    immediate-leave;
    oif-map map-name;
    passive;
    promiscuous-mode;
    ssm-map ssm-map-name;
    ssm-map-policy ssm-map-policy-name;
    static {
        group multicast-group-address {
            exclude;
            group-count number;
            group-increment increment;
            source ip-address {
                source-count number;
                source-increment increment;
            }
        }
    }
    version version;
}
```

Hierarchy Level

[edit logical-systems logical-system-name protocols igmp],
[edit protocols igmp]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Enable IGMP on an interface and configure interface-specific properties.

Options

- `interface-name`—Name of the interface. Specify the full interface name, including the physical and logical address components. To configure all interfaces, you can specify all.

  The remaining statements are explained separately.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Enabling IGMP
join-load-balance

Syntax

```
join-load-balance {
    automatic;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
[edit protocols pim],
[edit routing-instances routing-instance-name protocols pim]
```

Release Information

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Enable load balancing of PIM join messages across interfaces and routing devices.

Options

automatic—Enables automatic load balancing of PIM join messages. When a new interface or neighbor is introduced into the network, ECMP joins are redistributed with minimal disruption to traffic.

Required Privilege Level

- routing—to view this statement in the configuration.
- routing-control—to add this statement to the configuration.

Related Documentation

- Example: Configuring PIM Make-Before-Break Join Load Balancing
- Configuring PIM Join Load Balancing
- `clear pim join-distribution` in the Junos OS Operational Mode Commands
local

Syntax

```
local {
    disable;
    address address;
    family (inet | inet6) {
        disable;
        address address;
        anycast-pim {
            local-address address;
            rp-set {
                address address <forward-msdp-sa>;
            }
        }
        group-ranges {
            destination-ip-prefix <prefix-length>;
        }
        hold-time seconds;
        override;
        priority number;
    }
    group-ranges {
        destination-ip-prefix <prefix-length>;
    }
    hold-time seconds;
    override;
    priority number;
}
```

Hierarchy Level

- `[edit logical-systems logical-system-name protocols pim rp]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp]`
- `[edit protocols pim rp]`
- `[edit routing-instances routing-instance-name protocols pim rp]`

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
The remaining statements are explained separately.

Description

Configure the routing device's RP properties.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Local PIM RPs
## local-address (Protocols PIM)

**Syntax**

```
local-address address;
```

**Hierarchy Level**

- `[edit logical-systems logical-system-name protocols pim rp local family (inet inet6) anycast-pim]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp local family (inet inet6) anycast-pim]`
- `[edit protocols pim rp local family (inet inet6) anycast-pim]`
- `[edit routing-instances routing-instance-name protocols pim rp local family (inet inet6) anycast-pim]`

**Release Information**

- Statement introduced in Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure the routing device local address for the anycast rendezvous point (RP). If this statement is omitted, the router ID is used as this address.

**Options**

- `address`—Anycast RP IPv4 or IPv6 address, depending on `family` configuration.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- *Example: Configuring PIM Anycast With or Without MSDP*
mapping-agent-election

Syntax  (mapping-agent-election | no-mapping-agent-election);

Hierarchy Level  [edit logical-systems logical-system-name protocols pim rp auto-rp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp auto-rp],
[edit protocols pim rp auto-rp],
[edit routing-instances routing-instance-name protocols pim rp auto-rp]

Release Information  Statement introduced in Junos OS Release 7.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Configure the routing device mapping announcements as a mapping agent.

Options  mapping-agent-election—Mapping agents do not announce mappings when receiving mapping messages from a higher-addressed mapping agent.

no-mapping-agent-election—Mapping agents always announce mappings and do not perform mapping agent election.

Default: mapping-agent-election

Required Privilege  routing—To view this statement in the configuration.
Level routing-control—To add this statement to the configuration.

Related Documentation  • Configuring PIM Auto-RP
maximum-rps

Syntax  maximum-rps limit;

Hierarchy Level  [edit logical-systems logical-system-name protocols pim rp embedded-rp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp embedded-rp],
[edit protocols pim rp embedded-rp],
[edit routing-instances routing-instance-name protocols pim rp embedded-rp]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description  Limit the number of RPs that the routing device acknowledges.

Options  limit—Number of RPs.
  Range:  1 through 500
  Default:  100

Required Privilege  routing—To view this statement in the configuration.
  routing-control—To add this statement to the configuration.

Related Documentation  • Configuring PIM Embedded RP for IPv6
mode (Protocols PIM)

Syntax
mode (bidirectional-sparse | bidirectional-sparse-dense | dense | sparse | sparse-dense);

Hierarchy Level
[edit logical-systems logical-system-name protocols pim interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim interface interface-name],
[edit protocols pim interface interface-name],
[edit routing-instances routing-instance-name protocols pim interface interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
bidirectional-sparse and bidirectional-sparse-dense options introduced in Junos OS Release 12.1.

Description
Configure the PIM mode on the interface.

Options
The choice of PIM mode is closely tied to controlling how groups are mapped to PIM modes, as follows:

- **bidirectional-sparse**—Use if all multicast groups are operating in bidirectional, sparse, or SSM mode.
- **bidirectional-sparse-dense**—Use if multicast groups, except those that are specified in the dense-groups statement, are operating in bidirectional, sparse, or SSM mode.
- **dense**—Use if all multicast groups are operating in dense mode.
- **sparse**—Use if all multicast groups are operating in sparse mode or SSM mode.
- **sparse-dense**—Use if multicast groups, except those that are specified in the dense-groups statement, are operating in sparse mode or SSM mode.

Default: Sparse mode

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Configuring PIM Dense Mode Properties in the Multicast Protocols Feature Guide for Routing Devices
- Configuring PIM Sparse-Dense Mode Properties in the Multicast Protocols Feature Guide for Routing Devices
- Example: Configuring Bidirectional PIM
**multicast-router-interface (IGMP Snooping)**

**Syntax**

```
multicast-router-interface;
```

**Hierarchy Level**

```
[edit bridge-domains bridge-domain-name protocols igmp-snooping interface interface-name],
[edit bridge-domains bridge-domain-name protocols igmp-snooping vlan vlan-id interface interface-name],
[edit protocols igmp-snooping vlan (all | vlan-name) interface (all | interface-name)]
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name protocols igmp-snooping interface interface-name],
[edit routing-instances routing-instance-name bridge-domains bridge-domain-name protocols vlan vlan-id igmp-snooping interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description**

Statically configure the interface as an IGMP snooping multicast-router interface—that is, an interface that faces toward a multicast router or other IGMP querier.

---

**NOTE:** If the specified interface is a trunk port, the interface becomes a multicast-routing device interface for all VLANs configured on the trunk port. In addition, all unregistered multicast packets, whether they are IPv4 or IPv6 packets, are forwarded to the multicast routing device interface, even if the interface is configured as a multicast routing device interface only for IGMP snooping.

Configure an interface as a bridge interface toward other multicast routing devices.

**Default**

The interface can either be a host-side or multicast-routing device interface.

**Required Privilege Level**

route—To view this statement in the configuration.
route-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring IGMP Snooping on EX Series Switches
- Example: Configuring IGMP Snooping
- Configuring IGMP Snooping (CLI Procedure)
- IGMP Snooping in MC-LAG Active-Active on MX Series Routers Overview
- host-only-interface
- show igmp-snooping membership on page 3453
neighbor-policy

Syntax

neighbor-policy [ policy-names ];

Hierarchy Level

[edit logical-systems logical-system-name protocols pim interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim interface interface-name],
[edit protocols pim interface interface-name],
[edit routing-instances routing-instance-name protocols pim interface interface-name]

Release Information

Statement introduced in Junos OS Release 8.2.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Apply a PIM interface-level policy to filter neighbor IP addresses.

Options

policy-name—Name of the policy that filters neighbor IP addresses.

Required Privilege

routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

Related Documentation

• Configuring Interface-Level PIM Neighbor Policies
pim

Syntax

```
pim {
  disable;
  assert-timeout seconds;
  dense-groups {
    addresses;
  }
  dr-election-on-p2p;
  export;
  family (inet | inet6) {
    disable;
  }
  graceful-restart {
    disable;
    no-bidirectional-mode;
    restart-duration seconds;
  }
  import [ policy-names ];
  interface interface-name {
    family (inet | inet6) {
      disable;
    }
    bfd-liveness-detection {
      authentication {
        algorithm algorithm-name;
        key-chain key-chain-name;
        loose-check;
        detection-time {
          threshold milliseconds;
        }
      }
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (0 | 1 | automatic);
    }
    accept-remote-source;
    disable;
    bidirectional {
      df-election {
        backoff-period milliseconds;
        offer-period milliseconds;
        robustness-count number;
      }
    }
    family (inet | inet6) {
      disable;
    }
    hello-interval seconds;
  }
```
mode (bidirectional-sparse | bidirectional-sparse-dense | dense | sparse | sparse-dense);
neighbor-policy [ policy-names ];
override-interval milliseconds;
priority number;
propagation-delay milliseconds;
reset-tracking-bit;
version version;
}
join-load-balance;
jjoin-prune-timeout;
mdt {
data-mdt-reuse;
group-range multicast-prefix;
threshold {
  group group-address {
    source source-address {
      rate threshold-rate;
    }
  }
}
tunnel-limit limit;
}
}
mvpn {
  autodiscovery {
    inet-mdt;
  }
}
nonstop-routing;
override-interval milliseconds;
propagation-delay milliseconds;
reset-tracking-bit;
rib-group group-name;
rp {
  auto-rp {
    (announce | discovery | mapping);

    (mapping-agent-election | no-mapping-agent-election);
  }
}
bidirectional {
  address address {
    group-ranges {
      destination-ip-prefix</prefix-length>;
    }
  }
  hold-time seconds;
priority number;
}
}
bootstrap {
  family (inet | inet6) {
    export [ policy-names ];
    import [ policy-names ];
priority number;
  }
  bootstrap-import [ policy-names ];
  bootstrap-export [ policy-names ];
bootstrap-priority number;
dr-register-policy [ policy-names ];
embedded-rp [ 
group-ranges [ 
    destination-ip-prefix</prefix-length>];
]  
maximum-rps limit;
]
group-rp-mapping [ 
    family (inet | inet6) { 
        log-interval seconds;  
        maximum limit;  
        threshold value;  
    }
]  
log-interval seconds;  
maximum limit;  
threshold value;  
]  
local [ 
    family (inet | inet6) { 
        address address;  
        anycast-pim [ 
            rp-set { 
                address address <forward-msdp-sa>;
            }  
            disable;  
            local-address address;
        }  
        group-ranges [ 
            destination-ip-prefix</prefix-length>];
    ]  
    hold-time seconds;  
    override;  
    priority number;  
]  
register-limit [ 
    family (inet | inet6) { 
        log-interval seconds;  
        maximum limit;  
        threshold value;  
    }
]  
log-interval seconds;  
maximum limit;  
threshold value;  
]  
rp-register-policy [ policy-names ];
spt-threshold [ 
    infinity [ policy-names ];
]
static [ 
    address address [ 
}
override;

version version;
group-ranges {
    destination-ip-prefix</prefix-length>;
}
}
}
}
}
rpf-selection {
group group-address{
    sourcesource-address{
        next-hop next-hop-address;
    }
    wildcard-source {
        next-hop next-hop-address;
    }
}
}

prefix-list prefix-list-addresses {
    source source-address {
        next-hop next-hop-address;
    }
    wildcard-source {
        next-hop next-hop-address;
    }
}
}

sglimit {
    family (inet | inet6) {
        log-interval seconds;
        maximum limit;
        threshold value;
    }
    log-interval seconds;
    maximum limit;
    threshold value;
}
}

traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}

tunnel-devices [ mt-fpc/pic/port ];
}

Hierarchy Level
[edit logical-systems logical-system-name protocols],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols],
[edit protocols],
[edit routing-instances routing-instance-name protocols]

Release Information
Statement introduced before Junos OS Release 7.4.
family statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Enable PIM on the routing device.
The remaining statements are explained separately.

Default
PIM is disabled on the routing device.

Required Privilege
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Data MDTs and Provider Tunnels Operating in Any-Source Multicast Mode
• Configuring PIM Dense Mode Properties
• Configuring PIM Sparse-Dense Mode Properties

priority (PIM Interfaces)

Syntax
priority number;

Hierarchy Level
[edit logical-systems logical-system-name protocols pim interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim interface interface-name],
[edit protocols pim interface interface-name],
[edit routing-instances routing-instance-name protocols pim interface interface-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure the routing device's likelihood to be elected as the designated router.

Options
number—Routing device's priority for becoming the designated router. A higher value corresponds to a higher priority.
Range: 0 through a 32-bit number
Default: 1

Required Privilege
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Interface Priority for PIM Designated Router Selection
**priority (Bootstrap)**

**Syntax**

```
priority number;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols pim rp bootstrap (inet | inet6)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp bootstrap (inet | inet6)],
[edit protocols pim rp bootstrap (inet | inet6)],
[edit routing-instances routing-instance-name protocols pim rp bootstrap (inet | inet6)]
```

**Release Information**

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Configure the routing device’s likelihood to be elected as the bootstrap router.

**Options**

`number`—Routing device’s priority for becoming the bootstrap router. A higher value corresponds to a higher priority.

- **Range:** 0 through a 32-bit number
- **Default:** 0 (The routing device has the least likelihood of becoming the bootstrap router and sends packets with a priority of 0.)

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring PIM Bootstrap Properties for IPv4](#)
- [Configuring PIM Bootstrap Properties for IPv4 or IPv6](#)
- [bootstrap-priority on page 3338](#)
priority (PIM RPs)

**Syntax**

```
priority number;
```

**Hierarchy Level**

```
[edit logical-systems logical-system-name protocols pim rp bidirectional address address],
[edit logical-systems logical-system-name routing-instances instance-name protocols pim rp bidirectional address address],
[edit protocols pim rp bidirectional address address],
[edit protocols pim rp local family (inet | inet6)],
[edit routing-instances instance-name protocols pim rp bidirectional address address],
[edit routing-instances routing-instance-name protocols pim rp local family (inet | inet6)]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional RP addresses introduced in Junos OS Release 12.1.

**Description**

For PIM-SM, configure this routing device’s priority for becoming an RP.

For bidirectional PIM, configure this RP address’ priority for becoming an RP.

The bootstrap router uses this field when selecting the list of candidate rendezvous points to send in the bootstrap message. A smaller number increases the likelihood that the routing device or RP address becomes the RP. A priority value of 0 means that bootstrap router can override the group range being advertised by the candidate RP.

**Options**

- `number`—Priority for becoming an RP. A lower value corresponds to a higher priority.
  - **Range:** 0 through 255
  - **Default:** 1

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Local PIM RPs in the Multicast Protocols Feature Guide for Routing Devices
- Example: Configuring Bidirectional PIM
query-interval (Protocols IGMP)

Syntax

query-interval seconds;

Hierarchy Level

[edit logical-systems logical-system-name protocols igmp],
[edit protocols igmp]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Specify how often the querier routing device sends general host-query messages.

Options

seconds—Time interval.
Range: 1 through 1024
Default: 125 seconds

Required Privilege

Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Modifying the IGMP Host-Query Message Interval
• query-last-member-interval (Protocols IGMP) on page 3379
• query-response-interval (Protocols IGMP) on page 3380
query-last-member-interval (Protocols IGMP)

Syntax

```
query-last-member-interval seconds;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols igmp],
[edit protocols igmp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Specify how often the querier routing device sends group-specific query messages.

Options

seconds—Time interval, in fractions of a second or seconds.

Range:
0.1 through 0.9, then in 1-second intervals 1 through 999999

Default: 1 second

Required Privilege

Level: routing—To view this statement in the configuration.
        routing-control—To add this statement to the configuration.

Related Documentation

- Modifying the IGMP Last-Member Query Interval
- query-interval (Protocols IGMP) on page 3378
- query-response-interval (Protocols IGMP) on page 3380
query-response-interval (Protocols IGMP)

Syntax

query-response-interval seconds;

Hierarchy Level
[edit logical-systems logical-system-name protocols igmp],
[edit protocols igmp]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Specify how long the querier routing device waits to receive a response to a host-query message from a host.

Options
seconds—The query response interval must be less than the query interval.
Range: 1 through 1024
Default: 10 seconds

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Modifying the IGMP Query Response Interval
• query-interval (Protocols IGMP) on page 3378
• query-last-member-interval (Protocols IGMP) on page 3379
receiver

Syntax  
receiver {  
  source-vlans vlan-list;  
install;  
}  

Hierarchy Level  
[edit protocols igmp-snooping vlan (all | vlan-name) data-forwarding]

Release Information  
- Statement introduced in Junos OS Release 9.6 for EX Series switches.  
- Statement introduced in Junos OS Release 12.3 for the QFX Series.

Description  
Configure a VLAN as a multicast receiver VLAN of the multicast VLAN (MVLAN).  
The remaining statements are explained separately.

Default  
Disabled

Required Privilege Level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

Related Documentation  
- Example: Configuring Multicast VLAN Registration  
- Configuring Multicast VLAN Registration (CLI Procedure)
restart-duration (Protocols PIM)

Syntax

restart-duration seconds;

Hierarchy Level

[edit logical-systems logical-system-name protocols pim graceful-restart],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim graceful-restart],
[edit protocols pim graceful-restart],
[edit routing-instances routing-instance-name protocols pim graceful-restart]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure the duration of the graceful restart interval.

Options

seconds—Time that the routing device waits (in seconds) to complete PIM sparse mode graceful restart.
Range: 30 through 300
Default: 60

Required Privilege

Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Configuring PIM Sparse Mode Graceful Restart
### rib-group (Protocols PIM)

**Syntax**

```
rib-group {
    inet group-name;
    inet6 group-name;
}
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols pim],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
- [edit protocols pim],
- [edit routing-instances routing-instance-name protocols pim]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Associate a routing table group with PIM.

**Options**

- `table-name`—Name of the routing table. The name must be one that you defined with the `rib-groups` statement at the [edit routing-options] hierarchy level.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring a Dedicated PIM RPF Routing Table
robust-count (IGMP Snooping)

Syntax

```
robust-count number;
```

Hierarchy Level

```
[edit protocols igmp-snooping vlan (all | vlan-name)]
```

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description

Configure the number of queries the switch sends before removing a multicast group from the multicast forwarding table. We recommend that the robust count be set to the same value on all multicast routers and switches in the VLAN.

Default

The default is the value of the `robust-count` statement configured for IGMP. The default for the IGMP `robust-count` statement is 2.

Options

- `number`—Number of queries the switch sends before timing out a multicast group.
  - Range: 2 through 10

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring IGMP Snooping (CLI Procedure)

---

robust-count (Protocols IGMP)

Syntax

```
robust-count number;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols igmp],
[edit protocols igmp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Tune the expected packet loss on a subnet. This factor is used to calculate the group member interval, other querier present interval, and last-member query count.

Options

- `number`—Robustness variable.
  - Range: 2 through 10
  - Default: 2

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Modifying the IGMP Robustness Variable
rp

Syntax  rp {
    auto-rp {
        (announce | discovery | mapping);
        (mapping-agent-election | no-mapping-agent-election);
    }
    bidirectional {
        address address {
            group-ranges {
                destination-ip-prefix</prefix-length>;
            }
            hold-time seconds;
            priority number;
        }
    }
    bootstrap {
        family (inet | inet6) {
            export [ policy-names ];
            import [ policy-names ];
            priority number;
        }
        bootstrap-export [ policy-names ];
        bootstrap-import [ policy-names ];
        bootstrap-priority number;
        dr-register-policy [ policy-names ];
        embedded-rp {
            group-ranges {
                destination-ip-prefix</prefix-length>;
            }
            maximum-rps limit;
        }
        group-rp-mapping {
            family (inet | inet6) {
                log-interval seconds;
                maximum limit;
                threshold value;
            }
        }
        log-interval seconds;
        maximum limit;
        threshold value;
    }
    local {
        family (inet | inet6) {
            disable;
            address address;
            anycast-pim {
                local-address address;
                address address <forward-msdp-sa>;
                rp-set {
                    ...
} 

  group-ranges {
    destination-ip-prefix</prefix-length>;
  }

  hold-time seconds;
  override;
  priority number;
}

  register-limit {
    family (inet | inet6) {
      log-interval seconds;
      maximum limit;
      threshold value;
    }
  }

  log-interval seconds;
  maximum limit;
  threshold value;
}

  register-probe-time register-probe-time;
}

  rp-register-policy [policy-names];

  static {
    address address {
      override;
      version version;
      group-ranges {
        destination-ip-prefix</prefix-length>;
      }
    }
  }

Hierarchy Level
[edit logical-systems logical-system-name protocols pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
[edit protocols pim],
[edit routing-instances routing-instance-name protocols pim]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure the routing device as an actual or potential RP. A routing device can be an RP for more than one group.

The remaining statements are explained separately.

Default
If you do not include the rp statement, the routing device can never become the RP.

Required Privilege
routing—to view this statement in the configuration.

Level
routing-control—to add this statement to the configuration.
Related Documentation

- Understanding PIM Sparse Mode

rp-register-policy

Syntax

rp-register-policy [ policy-names ];

Hierarchy Level

- [edit logical-systems logical-system-name protocols pim rp],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
- [edit protocols pim rp],
- [edit routing-instances routing-instance-name protocols pim rp]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Apply one or more policies to control incoming PIM register messages.

Options

- policy-names—Name of one or more import policies.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Register Message Filters on a PIM RP and DR
- dr-register-policy on page 3343
rp-set

Syntax

rp-set {
  address address <forward-msdp-sa>;
}

Hierarchy Level

[edit logical-systems logical-system-name protocols pim local family (inet | inet6) anycast-pim],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim local family (inet | inet6) anycast-pim],
[edit protocols pim local family (inet | inet6) anycast-pim],
[edit routing-instances routing-instance-name protocols pim local family (inet | inet6) anycast-pim]

Release Information

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure a set of rendezvous point (RP) addresses for anycast RP. You can configure up to 15 RPs.

The remaining statements are explained separately.

Required Privilege

Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

• Example: Configuring PIM Anycast With or Without MSDP
source (Protocols IGMP)

Syntax

```plaintext
source ip-address {
    source-count number;
    source-increment increment;
}
```

Hierarchy Level

[edit logical-systems logical-system-name protocols igmp interface interface-name static group multicast-group-address],
[edit protocols igmp interface interface-name static group multicast-group-address]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description

Specify the IP version 4 (IPv4) unicast source address for the multicast group being statically configured on an interface.

Options

`ip-address`—IPv4 unicast address.

The remaining statements are explained separately.

Required Privilege

Level: routing—to view this statement in the configuration.
Level: routing-control—to add this statement to the configuration.

Related Documentation

• Enabling IGMP Static Group Membership
source-vlans

Syntax
source-vlans vlan-list;

Hierarchy Level
[edit protocols igmp-snooping vlan (all | vlan-name) data-forwarding receiver]

Release Information
Statement introduced in Junos OS Release 9.6 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for the QFX Series.

Description
Specify a list of multicast VLANs (MVLANs) from which this multicast receiver VLAN receives multicast traffic. Either all of these MVLANs must be in proxy mode or none of them can be in proxy mode.

Default
Disabled

Options
vlan-list—Names of the MVLANs.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring Multicast VLAN Registration
• Configuring Multicast VLAN Registration (CLI Procedure)
spt-threshold

Syntax

```plaintext
spt-threshold { infinity [ policy-names ]; }
```

Hierarchy Level

- `edit logical-systems logical-system-name protocols pim`
- `edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim`
- `edit protocols pim`
- `edit routing-instances routing-instance-name protocols pim`

Release Information

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Set the SPT threshold to infinity for a source-group address pair. Last-hop multicast routing devices running PIM sparse mode can forward the same stream of multicast packets onto the same LAN through an RPT rooted at the RP or an SPT rooted at the source. By default, last-hop routing devices transition to a direct SPT to the source. You can configure this routing device to set the SPT transition value to infinity to prevent this transition for any source-group address pair.

The remaining statements are explained separately.

Required Privilege Level

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation

- Example: Configuring the PIM SPT Threshold Policy
### ssm-map (Protocols IGMP)

**Syntax**

```
ssm-map ssm-map-name;
```

**Hierarchy Level**

[edit logical-systems logical-system-name protocols igmp interface interface-name],
[edit protocols igmp interface interface-name]

**Release Information**

Statement introduced in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Apply an SSM map to an IGMP interface.

**Options**

- `ssm-map-name`—Name of SSM map.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring SSM Mapping

### static (IGMP Snooping)

**Syntax**

```
static {  
    group ip-address;
  }
```

**Hierarchy Level**

[edit protocols igmp-snooping vlan (all | vlan-name) interface (all | interface-name)]

**Release Information**

Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description**

Statically define multicast groups on an interface.

The remaining statement is explained separately.

**Default**

No multicast groups are statically defined.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring IGMP Snooping (CLI Procedure)
- show igmp-snooping membership on page 3453
static (Protocols PIM)

Syntax
static {
  address address {
    group-ranges {
      destination-ip-prefix</prefix-length>;
    }
    override:
    version version;
  }
}

Hierarchy Level
[edit logical-systems logical-system-name protocols pim rp],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp],
[edit protocols pim rp],
[edit routing-instances routing-instance-name protocols pim rp]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description
Configure static RP addresses. The default static RP address is 224.0.0.0/4. To configure other addresses, include one or more address statements. You can configure a static RP in a logical system only if the logical system is not directly connected to a source.

For each static RP address, you can optionally specify the PIM version and the groups for which this address can be the RP. The default PIM version is version 1.

The remaining statements are explained separately.

Required Privilege
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- Configuring the Static PIM RP Address on the Non-RP Routing Device
**static (Protocols IGMP)**

**Syntax**

```plaintext
static {
  group multicast-group-address {
    exclude;
    group-count number;
    group-increment increment;
    source ip-address {
      source-count number;
      source-increment increment;
    }
  }
}
```

**Hierarchy Level**

- [edit logical-systems logical-system-name protocols igmp interface interface-name]
- [edit protocols igmp interface interface-name]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**

Test multicast forwarding on an interface without a receiver host.

The `static` statement simulates IGMP joins on a routing device statically on an interface without any IGMP hosts. It is supported for both IGMPv2 and IGMPv3 joins. This statement is especially useful for testing multicast forwarding on an interface without a receiver host.

**NOTE:** To prevent joining too many groups accidentally, the `static` statement is not supported with the `interface all` statement.

The remaining statements are explained separately.

**Required Privilege Level**

- routing and trace—To view this statement in the configuration.
- routing-control and trace-control—To add this statement to the configuration.

**Related Documentation**

- [Enabling IGMP Static Group Membership](#)
traceoptions (Protocols PIM)

Syntax

```
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

- [edit logical-systems logical-system-name protocols pim],
- [edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim],
- [edit protocols pim],
- [edit routing-instances routing-instance-name protocols pim]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Configure PIM tracing options.
To specify more than one tracing operation, include multiple `flag` statements.

Default

The default PIM trace options are those inherited from the routing protocol’s `traceoptions` statement included at the `[edit routing-options]` hierarchy level.

Options

- `disable`—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as `all`.

  - `file filename`—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`. We recommend that you place tracing output in the `pim-log` file.

  - `files number`—(Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum number of files, you must also include the `size` statement to specify the maximum file size.

  - `Range:` 2 through 1000 files
  - `Default:` 2 files

  - `flag flag`—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements.

PIM Tracing Flags

- `assert`—Assert messages

- `bidirectional-df-election`—Bidirectional PIM designated-forwarder (DF) election events
- **bootstrap**—Bootstrap messages
- **cache**—Packets in the PIM sparse mode routing cache
- **graft**—Graft and graft acknowledgment messages
- **hello**—Hello packets
- **join**—Join messages
- **mt**—Multicast tunnel messages
- **nsr-synchronization**—Nonstop active routing (NSR) synchronization messages
- **packets**—All PIM packets
- **prune**—Prune messages
- **register**—Register and register stop messages
- **rp**—Candidate RP advertisements
- **all**—All tracing operations
- **general**—A combination of the **normal** and **route** trace operations
- **normal**—All normal operations

**Default:** If you do not specify this option, only unusual or abnormal operations are traced.
- **policy**—Policy operations and actions
- **route**—Routing table changes
- **state**—State transitions
- **task**—Interface transactions and processing
- **timer**—Timer usage

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:
- **detail**—Detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

**no-stamp**—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

**Default:** If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.
no-world-readable—(Optional) Do not allow users to read the log file.

replace—(Optional) Replace an existing trace file if there is one.

**Default:** If you do not include this option, tracing output is appended to an existing trace file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file.0`. When `trace-file` again reaches this size, `trace-file.0` is renamed `trace-file.1` and `trace-file` is renamed `trace-file.0`. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you must also include the `files` statement to specify the maximum number of trace files.

**Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

**Range:** 0 KB through the maximum file size supported on your system

**Default:** 1 MB

world-readable—(Optional) Allow any user to read the log file.

**Required Privilege Level**
- **routing and trace**—To view this statement in the configuration.
- **routing-control and trace-control**—To add this statement to the configuration.

**Related Documentation**
- *Configuring PIM Trace Options*
- *Tracing DVMRP Protocol Traffic*
- *Tracing MSDP Protocol Traffic*
- *Configuring PIM Trace Options*
traceoptions (Protocols IGMP)

Syntax
traceoptions {
  file filename <files number> <size> <world-readable | no-world-readable>;  
  flag flag <flag-modifier> <disable>;
}

Hierarchy Level
[edit logical-systems logical-system-name protocols igmp],  
[edit protocols igmp]

Release Information
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Configure IGMP tracing options.

To specify more than one tracing operation, include multiple flag statements.

To trace the paths of multicast packets, use the mtrace command.

Default
The default IGMP trace options are those inherited from the routing protocols traceoptions statement included at the [edit routing-options] hierarchy level.

Options
disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.

file filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log. We recommend that you place tracing output in the file igmp-log.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also include the size statement to specify the maximum file size.

Range: 2 through 1000 files

Default: 2 files

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.

IGMP Tracing Flags
- leave—Leave group messages (for IGMP version 2 only).
- mtrace—Mtrace packets. Use the mtrace command to troubleshoot the software.
- packets—All IGMP packets.
• **query**—IGMP membership query messages, including general and group-specific queries.

• **report**—Membership report messages.

**Global Tracing Flags**

• **all**—All tracing operations

• **general**—A combination of the **normal** and **route** trace operations

• **normal**—All normal operations

**Default:** If you do not specify this option, only unusual or abnormal operations are traced.

• **policy**—Policy operations and actions

• **route**—Routing table changes

• **state**—State transitions

• **task**—Interface transactions and processing

• **timer**—Timer usage

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

• **detail**—Detailed trace information

• **receive**—Packets being received

• **send**—Packets being transmitted

**no-stamp**—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

**Default:** If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

**no-world-readable**—(Optional) Do not allow users to read the log file.

**replace**—(Optional) Replace an existing trace file if there is one.

**Default:** If you do not include this option, tracing output is appended to an existing trace file.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When **trace-file** again reaches this size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
If you specify a maximum file size, you must also include the `files` statement to specify the maximum number of trace files.

**Syntax:**  `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

**Range:** 10 KB through the maximum file size supported on your system

**Default:** 1 MB

`world-readable`—(Optional) Allow any user to read the log file.

**Required Privilege**
- **Level:** routing and trace—To view this statement in the configuration.
- routing-control and trace-control—To add this statement to the configuration.

**Related Documentation**
- *Tracing IGMP Protocol Traffic*
traceoptions (IGMP Snooping)

Syntax

```
traceoptions {
    file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier>;
}
```

Hierarchy Level

[edit protocols igmp-snooping]

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description

Define tracing operations for IGMP snooping.

Default

The traceoptions feature is disabled by default.

Options

- **file** `filename`—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

- **files number**—(Optional) Maximum number of trace files, including the active trace file. When a trace file reaches its maximum size, its contents are archived into a compressed file named `filename.0` and the trace file is emptied. When the trace file reaches its maximum size again, the `filename.0` archive file is renamed `filename.1` and a new `filename.0` archive file is created from the contents of the trace file. This process continues until the maximum number of trace files is reached, at which point the system starts overwriting the oldest archive file each time the trace file is archived. If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

  Range: 2 through 1000

  Default: 10 files

- **flag** `flag`—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

  - all—All tracing operations.
  - general—Trace general IGMP snooping protocol events.
  - krt—Trace communication over routing socket.
  - leave—Trace leave group messages (IGMPv2 and IGMPv3 only).
  - nexthop—Trace nexthop-related events.
  - normal—Trace normal IGMP snooping protocol events. If you do not specify this flag, only unusual or abnormal operations are traced.
  - packets—Trace all IGMP packets.
  - policy—Trace policy processing.
  - query—Trace IGMP membership query messages.
  - report—Trace membership report messages.
- **route**—Trace routing information.
- **state**—Trace IGMP state transitions.
- **task**—Trace routing protocol task processing.
- **timer**—Trace routing protocol timer processing.
- **vlan**—Trace VLAN-related events.

**flag-modifier**—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers per flag:

- **detail**—Provide detailed trace information
- **disable**—Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.
- **receive**—Packets being received.
- **send**—Packets being transmitted.

**no-stamp**—(Optional) Omit the timestamp at the beginning of each line in the trace file.

**no-world-readable**—(Optional) Restrict file access to the user who created the file.

**replace**—(Optional) Replace an existing trace file if there is one. If you do not include this option, tracing output is appended to an existing trace file.

**size**—(Optional) Maximum size of each trace file, in bytes, kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches its maximum size, it is zipped and renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum size, you also must specify a maximum number of files with the `files` option.

**Syntax:** `x` to specify bytes, `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

**Range:** 10240 through 4294967295 bytes

**Default:** 128 KB

**world-readable**—(Optional) Allow unrestricted file access.

**Required Privilege Level**
- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**
- Configuring IGMP Snooping Tracing Operations (CLI Procedure) on page 3325
version (Protocols IGMP)

**Syntax**  
version version;

**Hierarchy Level**  
[edit logical-systems logical-system-name protocols igmp interface interface-name].  
[edit protocols igmp interface interface-name]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**  
Specify the version of IGMP.

**Options**  
version—IGMP version number.  
Range: 1, 2, or 3  
Default: IGMP version 2

**Required Privilege**  
level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**  
• Changing the IGMP Version

version (IGMP Snooping)

**Syntax**  
version number;

**Hierarchy Level**  
[edit protocols igmp-snooping vlan (all | vlan-name)]

**Release Information**  
Statement introduced in Junos OS Release 11.1 for EX Series switches.  
Statement introduced in Junos OS Release 12.1 for the QFX Series.

**Description**  
Specify the IGMP version for the IGMP general query that the switch sends to hosts when  
an interface comes up. The configured IGMP version affects only the version of the general  
queries sent by a switch. It does not affect the version of IGMP messages that the switch  
can snoop. For example, if the switch is configured for IGMP version 1 (IGMPv1), it can  
snoop IGMPv2 and IGMPv3 messages.

**Default**  
If you do not configure the version statement, the default is IGMPv2.

**Options**  
version—IGMP version number.  
Range: 1 through 3

**Required Privilege**  
level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**  
• Configuring IGMP Snooping (CLI Procedure)  
• Configuring IGMP Snooping
version (PIM)

Syntax

```
version version;
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols pim interface interface-name],
[edit logical-systems logical-system-name protocols pim rp static address address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim interface interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols pim rp static address address],
[edit protocols pim interface interface-name],
[edit protocols pim rp static address address],
[edit routing-instances routing-instance-name protocols pim interface interface-name],
[edit routing-instances routing-instance-name protocols pim rp static address address]
```

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Specify the version of PIM.

Options

- **version**—PIM version number.
  - Range: 1 or 2
  - Default: PIMv1 for rendezvous point (RP) mode (at the [edit protocols pim rp static address address] hierarchy level). PIMv2 for interface mode (at the [edit protocols pim interface interface-name] hierarchy level).

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Enabling PIM Sparse Mode
- Configuring PIM Dense Mode Properties
- Configuring PIM Sparse-Dense Mode Properties
vlan (IGMP Snooping)

Syntax

```
vlan (all | vlan-name) {
  data-forwarding {
    source {
      groups group-prefix;
    }
    receiver {
      source-vlans vlan-list;
      install;
    }
  }
  disable;
  immediate-leave;
  interface (all | interface-name) {
    multicast-router-interface;
    static {
      group ip-address;
    }
    proxy {
      source-address ip-address;
    }
    robust-count number;
    version version;
  }
}
```

Hierarchy Level
[edit protocols igmp-snooping]

Release Information
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated with enhanced (CLI completion feature) functionality in Junos OS Release 9.5 for EX Series switches.

Description
Configure IGMP snooping parameters for a VLAN.

When the `vlan` configuration statement is used without the `disable` statement, IGMP snooping is enabled on the specified VLAN or on all VLANs.

NOTE: You cannot configure IGMP snooping on a secondary VLAN.

Default
If the `vlan` statement is not included in the configuration, IGMP snooping is disabled.

Options
- **all**—All VLANs on the switch
- **vlan-name**—Name of a VLAN.

TIP: When you configure IGMP snooping parameters using the `vlan all` statement, any VLAN that is not individually configured for IGMP snooping
inherits the vlan all configuration. Any VLAN that is individually configured for IGMP snooping, on the other hand, inherits none of its configuration from vlan all. Any parameters that are not explicitly defined for the individual VLAN assume their default values, not the values specified in the vlan all configuration.

For example, in the following configuration:

```plaintext
protocols {
    igmp-snooping {
        vlan all {
            robust-count 8;
        }
        vlan employee {
            interface ge-0/0/8.0 {
                static {
                    group 239.0.10.3
                }
            }
        }
    }
}
```

all VLANs, except employee, have a robust count of 8. Because employee has been individually configured, its robust count value is not determined by the value set under vlan all. Instead, its robust count is the default value of 2.

The remaining statements are explained separately.

**Required Privilege**
- **Level**
  - routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring IGMP Snooping on EX Series Switches
- Configuring IGMP Snooping (CLI Procedure)
- show igmp-snooping vlans
CHAPTER 65

Administration

- Routine Monitoring on page 3407
- Operational Commands on page 3412

Routine Monitoring

- Monitoring IGMP Snooping on page 3407
- Verifying IGMP Snooping (CLI Procedure) on page 3410

Monitoring IGMP Snooping

**Purpose**  
Use the monitoring feature to view status and information about IGMP snooping configuration on your EX Series switch.

**Action**  
To display IGMP snooping details in the J-Web interface, select Monitor > Switching > IGMP Snooping.

To display IGMP snooping details in the CLI, enter the following commands:

- `show igmp-snooping route`
- `show igmp-snooping statistics`
- `show igmp-snooping vlans`

**NOTE:** On EX4300 switches, to display IGMP snooping details in the CLI, enter the following commands:

- `show igmp snooping interface`
- `show igmp snooping statistics`
- `show multicast snooping next-hops`
- `show multicast snooping route`

**Meaning**  
Table 402 on page 3408 summarizes the IGMP snooping details displayed.
### Table 402: Summary of IGMP Snooping Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IGMP Snooping Monitor</strong></td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN for which IGMP snooping is enabled.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Indicates the interfaces configured as switching interfaces that are associated with the multicast router.</td>
</tr>
<tr>
<td>Groups</td>
<td>Indicates the number of the multicast groups learned by the VLAN.</td>
</tr>
<tr>
<td>Learning Domain</td>
<td>Learning domain for snooping.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is supported only on EX4300 switches.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>Frequency (in seconds) with which the router sends membership queries when it is the querier.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is supported only on EX4300 switches.</td>
</tr>
<tr>
<td>Query Response Interval</td>
<td>Time (in seconds) that the router waits for a response to a general query.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is supported only on EX4300 switches.</td>
</tr>
<tr>
<td>Last Member Query Interval</td>
<td>Time (in seconds) that the router waits for a report in response to a group-specific query.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is supported only on EX4300 switches.</td>
</tr>
<tr>
<td>Robustness Count</td>
<td>Number of times the router retries a query.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is supported only on EX4300 switches.</td>
</tr>
<tr>
<td>MRouters</td>
<td>Specifies the multicast router.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is not supported on EX4300 switches.</td>
</tr>
<tr>
<td>Receivers</td>
<td>Specifies the multicast receiver.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is not supported on EX4300 switches.</td>
</tr>
<tr>
<td><strong>Interface Details</strong></td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td>Name of the interface.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is only supported on EX4300 switches.</td>
</tr>
<tr>
<td>State</td>
<td>Operating state of the interface. Values are Up or Down.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is only supported on EX4300 switches.</td>
</tr>
<tr>
<td>Group count</td>
<td>Number of groups on the interface.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is only supported on EX4300 switches.</td>
</tr>
</tbody>
</table>
Table 402: Summary of IGMP Snooping Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immediate Leave</td>
<td>State of immediate leave. Values are On or Off.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is only supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Router Interface</td>
<td>Router interfaces that are part of this learning domain.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is only supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>IGMP Route Information</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN for which IGMP snooping is enabled.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>Indicates the multicast groups learned by the VLAN.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Next-Hop</td>
<td>Specifies the next hop assigned by the switch after performing the route lookup.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Statistics</td>
<td></td>
</tr>
<tr>
<td>Packets per Vlan</td>
<td>Displays the number of packets sent or received, or the number of received errors.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Global</td>
<td>Displays the statistics name and statistics count. The statistics names are:</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Multicast Snooping Nexthops</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Next-hop identifier of the prefix. The identifier is returned by the routing device’s Packet Forwarding Engine.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Reference Count</td>
<td>Number of cache entries that are using this next hop.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Kernel Reference Count</td>
<td>Kernel reference count for the next hop.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
</tr>
</tbody>
</table>
Verifying IGMP Snooping (CLI Procedure)

Internet Group Management Protocol (IGMP) snooping constrains the flooding of IPv4 multicast traffic on VLANs on a switch. This topic describes how to verify IGMP snooping operation on the switch.

It covers:

- Verifying IGMP Snooping Memberships on page 3410
- Viewing IGMP Snooping Statistics on page 3411
- Viewing IGMP Snooping Routing Information on page 3411

Verifying IGMP Snooping Memberships

Purpose

Determine group memberships, multicast-router interfaces, host IGMP versions, and the current values of timeout counters.

Action

Enter the following command:

```
user@switch> show igmp-snooping membership detail
VLAN: vlan2 Tag: 2 (Index: 3)
  Router interfaces:
    ge-1/0/0.0 dynamic Uptime: 00:14:24 timeout: 253
    Group: 225.0.0.1
    ge-1/0/17.0 259 Last reporter: 13.0.0.90 Receiver count: 1
    Uptime: 00:00:19 timeout: 259 Flags: <V3-hosts>
    Include source: 10.2.11.5, 10.2.11.12
```

Meaning

The switch has multicast membership information for one VLAN on the switch, vlan2. IGMP snooping might be enabled on other VLANs, but the switch does not have any multicast membership information for them. The following information is provided:

- Information on the multicast-router interfaces for the VLAN—in this case, ge-1/0/0.0. The multicast-router interface has been learned by IGMP snooping, as indicated by the dynamic value. The timeout value shows how many seconds from now the interface

Table 402: Summary of IGMP Snooping Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downstream Interface</td>
<td>Interface names associated with each multicast next-hop ID.</td>
</tr>
</tbody>
</table>

**NOTE:** This option is supported only on EX4300 switches.
will be removed from the multicast forwarding table if the switch does not receive IGMP queries or Protocol Independent Multicast (PIM) updates on the interface.

- Information about the group memberships for the VLAN:
  - Currently, the VLAN has membership in only one multicast group, 225.0.0.1.
  - The host or hosts that have reported membership in the group are on interface ge-1/0/17.0. The last host that reported membership in the group has address 13.0.0.90. The number of hosts belonging to the group on the interface is shown in the Receiver count field, which is displayed only when host tracking is enabled if immediate leave is configured on the VLAN.
  - The Uptime field shows that the multicast group has been active on the interface for 19 seconds. The interface group membership will time out in 259 seconds if no hosts respond to membership queries during this interval. The Flags field shows the lowest version of IGMP used by a host that is currently a member of the group, which in this case is IGMP version 3 (IGMPv3).
  - Because the interface has IGMPv3 hosts on it, the source addresses from which the IGMPv3 hosts want to receive group multicast traffic are shown (addresses 10.2.11.5 and 10.2.11.12). The timeout value for the interface group membership is derived from the largest timeout value for all sources addresses for the group.

**Viewing IGMP Snooping Statistics**

**Purpose**
Display IGMP snooping statistics, such as number of IGMP queries, reports, and leaves received and how many of these IGMP messages contained errors.

**Action**
Enter the following command:

```
user@switch> show igmp-snooping statistics
```

Bad length: 0  Bad checksum: 0  Invalid interface: 0
Not local: 0  Receive unknown: 0  Timed out: 0

<table>
<thead>
<tr>
<th>IGMP Type</th>
<th>Received</th>
<th>Transmitted</th>
<th>Recv Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries:</td>
<td>74295</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reports:</td>
<td>18148423</td>
<td>0</td>
<td>16333523</td>
</tr>
<tr>
<td>Leaves:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Meaning**
The output shows how many IGMP messages of each type—Queries, Reports, Leaves—the switch received or transmitted on interfaces on which IGMP snooping is enabled. For each message type, it also shows the number of IGMP packets the switch received that had errors—for example, packets that do not conform to the IGMPv1, IGMPv2, or IGMPv3 standards. If the Recv Errors count increases, verify that the hosts are compliant with IGMP standards. If the switch is unable to recognize the IGMP message type for a packet, it counts the packet under Receive unknown.

**Viewing IGMP Snooping Routing Information**

**Purpose**
Display the next-hop information maintained in the multicast forwarding table.
**Action**
Enter the following command:

```
user@switch> show igmp-snooping route detail
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Group</th>
<th>Next-hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>v100</td>
<td>224.0.0.0, *</td>
<td>1323</td>
</tr>
<tr>
<td></td>
<td>Interfaces: ge-0/0/0.0</td>
<td></td>
</tr>
<tr>
<td>v100</td>
<td>226.0.0.1, *</td>
<td>1322</td>
</tr>
<tr>
<td></td>
<td>Interfaces: ge-0/0/0.0, ge-0/0/1.0, ge-0/0/47.0</td>
<td></td>
</tr>
</tbody>
</table>

**Meaning**
The output shows the next-hop interfaces for a given multicast group on a VLAN. For example, route 226.0.0.1 on v100 has next-hop interfaces ge-0/0/0.0, ge-0/0/1.0, and ge-0/0/47.0.

**Related Documentation**
- clear igmp-snooping membership on page 3418
- clear igmp-snooping statistics on page 3419
- *Example: Configuring IGMP Snooping on EX Series Switches*
- *Configuring IGMP Snooping (CLI Procedure)*

**Operational Commands**
clear igmp membership

**Syntax**
```
clear igmp membership
  <group address-range>
  <interface interface-name>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**
```
clear igmp membership
  <group address-range>
  <interface interface-name>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Clear Internet Group Management Protocol (IGMP) group members.

**Options**
- **none**—Clear all IGMP members on all interfaces and for all address ranges.
- **group address-range**—(Optional) Clear all IGMP members that are in a particular address range. An example of a range is `224.2/16`. If you omit the destination prefix length, the default is `/32`.
- **interface interface-name**—(Optional) Clear all IGMP group members on an interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**
```
clear
```

**Related Documentation**
- show igmp group on page 3442
- show igmp interface on page 3446

**List of Sample Output**
- clear igmp membership on page 3413
- clear igmp membership interface on page 3414
- clear igmp membership group on page 3414

**Output Fields**
See show igmp group for an explanation of output fields.

**Sample Output**
```
clear igmp membership

The following sample output displays IGMP group information before and after the clear igmp membership command is entered:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group</th>
<th>Last Reported</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/0</td>
<td>224.2.127.253</td>
<td>10.1.128.1</td>
<td>186</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>224.2.127.254</td>
<td>10.1.128.1</td>
<td>186</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>239.255.255.255</td>
<td>10.1.128.1</td>
<td>187</td>
</tr>
</tbody>
</table>
```

Copyright © 2013, Juniper Networks, Inc.
so-0/0/0  224.1.127.255  10.1.128.1  188
local    224.0.0.6       (null)                0
local    224.0.0.5       (null)                0
local    224.2.127.254   (null)                0
local    239.255.255.255 (null)                0
local    224.0.0.2       (null)                0
local    224.0.0.13      (null)                0

user@host> clear igmp membership
Clearing Group Membership Info for so-0/0/0
Clearing Group Membership Info for so-1/0/0
Clearing Group Membership Info for so-2/0/0

user@host> show igmp group
Interface   Group           Last Reported   Timeout
so-0/0/0    224.2.127.253   10.1.128.1          210
so-0/0/0    239.255.255.255 10.1.128.1          210
so-0/0/0    224.1.127.255   10.1.128.1          215
so-0/0/0    224.2.127.254   10.1.128.1          216
local      224.0.0.6       (null)                0
local      224.0.0.5       (null)                0
local      224.2.127.254   (null)                0
local      239.255.255.255 (null)                0
local      224.0.0.2       (null)                0
local      224.0.0.13      (null)                0

user@host> clear igmp membership interface
Clearing Group Membership Info for so-0/0/0

user@host> show igmp group
Interface   Group           Last Reported   Timeout
local      224.0.0.6       (null)                0
local      224.0.0.5       (null)                0
local      224.2.127.254   (null)                0
local      239.255.255.255 (null)                0
local      224.0.0.2       (null)                0
local      224.0.0.13      (null)                0

user@host> clear igmp membership group
Clearing Group Membership Info for so-0/0/0

user@host> show igmp group
Interface   Group           Last Reported   Timeout
local      224.0.0.6       (null)                0
local      224.0.0.5       (null)                0
local      224.2.127.254   (null)                0
local      239.255.255.255 (null)                0
local      224.0.0.2       (null)                0
local      224.0.0.13      (null)                0

user@host> show igmp group

### clear igmp membership group 239.225/16

Clearing Group Membership Range 239.225.0.0/16 on so-0/0/0
Clearing Group Membership Range 239.225.0.0/16 on so-1/0/0
Clearing Group Membership Range 239.225.0.0/16 on so-2/0/0

### show igmp group

<table>
<thead>
<tr>
<th>Interface</th>
<th>Group</th>
<th>Last Reported</th>
<th>Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>so-0/0/0</td>
<td>224.1.127.255</td>
<td>10.1.128.1</td>
<td>231</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>224.2.127.254</td>
<td>10.1.128.1</td>
<td>233</td>
</tr>
<tr>
<td>so-0/0/0</td>
<td>224.2.127.253</td>
<td>10.1.128.1</td>
<td>236</td>
</tr>
<tr>
<td>local</td>
<td>224.0.0.6</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>224.0.0.5</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>224.2.127.254</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>239.255.255.255</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>224.0.0.2</td>
<td>(null)</td>
<td>0</td>
</tr>
<tr>
<td>local</td>
<td>224.0.0.13</td>
<td>(null)</td>
<td>0</td>
</tr>
</tbody>
</table>
clear igmp statistics

Syntax
<interface interface-name>
logical-system (all | logical-system-name)>

Syntax (EX Series Switches)
clear igmp statistics
<interface interface-name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Clear Internet Group Management Protocol (IGMP) statistics.

Options
none—Clear IGMP statistics on all interfaces.
interface interface-name—(Optional) Clear IGMP statistics for the specified interface only.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
Level
clear

Related Documentation
• show igmp statistics on page 3450

List of Sample Output
clear igmp statistics on page 3416

Output Fields
See show igmp statistics for an explanation of output fields.

Sample Output
clear igmp statistics

The following sample output displays IGMP statistics information before and after the clear igmp statistics command is entered:

user@host> show igmp statistics
IGMP packet statistics for all interfaces
IGMP Message type   Received   Sent  Rx errors
Membership Query    8883      459         0
V1 Membership Report 0       0          0
DVMRP     19784     35476        0
PIM V1      18310         0         0
Cisco Trace      0        0          0
V2 Membership Report 0      0          0
Group Leave     0        0          0
Mtrace Response 0        0          0
Mtrace Request  0        0          0
Domain Wide Report 0       0          0
V3 Membership Report 0     0          0
Other Unknown types                                  0
IGMP v3 unsupported type                             0
IGMP v3 source required for SSM                     0
IGMP v3 mode not applicable for SSM                 0

IGMP Global Statistics
Bad Length                                          0
Bad Checksum                                        0
Bad Receive If                                      0
Rx non-local                                        1227

user@host> clear igmp statistics
user@host> show igmp statistics
IGMP packet statistics for all interfaces

IGMP Message type     Received  Sent  Rx errors
Membership Query       0         0     0
V1 Membership Report   0         0     0
DVMRP                  0         0     0
PIM V1                 0         0     0
Cisco Trace            0         0     0
V2 Membership Report   0         0     0
Group Leave            0         0     0
Mtrace Response        0         0     0
Mtrace Request         0         0     0
Domain Wide Report     0         0     0
V3 Membership Report   0         0     0
Other Unknown types    0         0     0
IGMP v3 unsupported type                                0
IGMP v3 source required for SSM                        0
IGMP v3 mode not applicable for SSM                    0
IGMP Global Statistics
Bad Length                                          0
Bad Checksum                                        0
Bad Receive If                                      0
Rx non-local                                        0

Copyright © 2013, Juniper Networks, Inc.
### clear igmp-snooping membership

**Syntax**
```plaintext
clear igmp-snooping membership
<vlan vlan-name>
```

**Release Information**
Command introduced in Junos OS Release 9.1 for EX Series switches.

**Description**
Clear IGMP snooping dynamic membership information from the multicast forwarding table.

**Options**
- **none**—Clear dynamic membership information for all VLANs.
- **vlan vlan-name**—(Optional) Clear dynamic membership information for the specified VLAN.

**Required Privilege Level**
- view

**Related Documentation**
- show igmp-snooping membership on page 3453
- clear igmp-snooping statistics on page 3419

**List of Sample Output**
clear igmp-snooping membership on page 3418

**Sample Output**
clear igmp-snooping membership
```
user@switch> clear igmp-snooping membership vlan employee-vlan
```
### clear igmp-snooping statistics

**Syntax**
```plaintext
clear igmp-snooping statistics
```

**Release Information**
Command introduced in Junos OS Release 9.1 for EX Series switches.

**Description**
Clear IGMP snooping statistics.

**Required Privilege Level**
`view`

**Related Documentation**
- [show igmp-snooping statistics on page 3458](#)
- [clear igmp-snooping membership on page 3418](#)

**List of Sample Output**
`clear igmp-snooping statistics on page 3419`

**Sample Output**
clear igmp-snooping statistics

```
user@switch> clear igmp-snooping statistics
```
clear multicast bandwidth-admission

Syntax clear multicast bandwidth-admission
    <group group-address>
    <inet | inet6>
    <instance instance-name>
    <interface interface-name>
    <source source-address>

Release Information
Command introduced in Junos OS Release 8.3.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Reapply IP multicast bandwidth admissions.

Options
none—Reapply multicast bandwidth admissions for all IPv4 forwarding entries in the master routing instance.

group group-address—(Optional) Reapply multicast bandwidth admissions for the specified group.

inet—(Optional) Reapply multicast bandwidth admission settings for IPv4 flows.

inet6—(Optional) Reapply multicast bandwidth admission settings for IPv6 flows.

instance instance-name—(Optional) Reapply multicast bandwidth admission settings for the specified instance. If you do not specify an instance, the command applies to the master routing instance.

interface interface-name—(Optional) Examines the corresponding outbound interface in the relevant entries and acts as follows:
- If the interface is congested, and it was admitted previously, it is removed.
- If the interface was rejected previously, the clear multicast bandwidth-admission command enables the interface to be admitted as long as enough bandwidth exists on the interface.
- If you do not specify an interface, issuing the clear multicast bandwidth-admission command readmits any previously rejected interface for the relevant entries as long as enough bandwidth exists on the interface.

To manually reject previously admitted outbound interfaces, you must specify the interface.

source source-address—(Optional) Use with the group option to reapply multicast bandwidth admission settings for the specified (source, group) entry.

Required Privilege
Level clear
When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear multicast bandwidth-admission

user@host> clear multicast bandwidth-admission
```
clear multicast scope

Syntax

```
clear multicast scope
  <inet | inet6>
  <interface interface-name>
  <logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and the QFX Series)

```
clear multicast scope
  <inet | inet6>
  <interface interface-name>
```

Release Information

Command introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 option introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear IP multicast scope statistics.

Options

- `none`—(Same as `logical-system all`) Clear multicast scope statistics.
- `inet`—(Optional) Clear multicast scope statistics for IPv4 family addresses.
- `inet6`—(Optional) Clear multicast scope statistics for IPv6 family addresses.
- `interface interface-name`—(Optional) Clear multicast scope statistics on a specific interface.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

`clear`

Related Documentation

- `show multicast scope` on page 3483

List of Sample Output

- `clear multicast scope` on page 3422

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear multicast scope

user@host> clear multicast scope
```
clear multicast sessions

**Syntax**

```plaintext
clear multicast sessions
<logical-system (all | logical-system-name)>
<regular-expression>
```

**Syntax (EX Series Switch and the QFX Series)**

```plaintext
clear multicast sessions
<regular-expression>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Clear IP multicast sessions.

**Options**

- `none`—(Same as `logical-system all`) Clear multicast sessions.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.
- `regular-expression`—(Optional) Clear only multicast sessions that contain the specified regular expression.

**Required Privilege Level**

`clear`

**Related Documentation**

- [show multicast sessions on page 3485](#)

**List of Sample Output**

- [clear multicast sessions on page 3423](#)

**Output Fields**

When you enter this command, you are provided feedback on the status of your request.

**Sample Output**

```plaintext
clear multicast sessions

user@host> clear multicast sessions
```

---

Copyright © 2013, Juniper Networks, Inc.
clear multicast statistics

Syntax

```
clear multicast statistics
<inet | inet6>
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and the QFX Series)

```
clear multicast statistics
<inet | inet6>
<instance instance-name>
<interface interface-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Clear IP multicast statistics.

Options

```
none—Clear multicast statistics for all supported address families on all interfaces.
inet—(Optional) Clear multicast statistics for IPv4 family addresses.
inet6—(Optional) Clear multicast statistics for IPv6 family addresses.
instance instance-name—(Optional) Clear multicast statistics for the specified instance.
interface interface-name—(Optional) Clear multicast statistics on a specific interface.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.
```

Required Privilege Level clear

Related Documentation

- `show multicast statistics`

List of Sample Output

`clear multicast statistics on page 3424`

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear multicast statistics

user@host> clear multicast statistics
```
### clear pim join

**Syntax**

```
clear pim join
<group-address>
<bidirectional | dense | sparse>
<exact>
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
<rp ip-address/prefix | source ip-address/prefix>
<sg | star-g>
```

**Syntax (EX Series Switch and the QFX Series)**

```
clear pim join
<group-address>
<dense | sparse>
<exact>
<inet | inet6>
<instance instance-name>
<rp ip-address/prefix | source ip-address/prefix>
<sg | star-g>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- *inet6* and *instance* options introduced in Junos OS Release 10.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Multiple new filter options introduced in Junos OS Release 13.2.

**Description**

Clear the Protocol Independent Multicast (PIM) join and prune states.

**Options**

- **none**—Clear the PIM join and prune states for all groups, family addresses, and instances.
- **group-address**—(Optional) Clear the PIM join and prune states for a group address.
- **bidirectional | dense | sparse**—(Optional) Clear PIM bidirectional mode, dense mode, or sparse and source-specific multicast (SSM) mode entries.
- **exact**—(Optional) Clear only the group that exactly matches the specified group address.
- **inet | inet6**—(Optional) Clear the PIM entries for IPv4 or IPv6 family addresses, respectively.
- **instance instance-name**—(Optional) Clear the entries for a specific PIM-enabled routing instance.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.
- **rp ip-address/prefix | source ip-address/prefix**—(Optional) Clear the PIM entries with a specified rendezvous point (RP) address and prefix or with a specified source address and prefix. You can omit the prefix.
- **sg | star-g**—(Optional) Clear PIM *(S,G)* or *(G)* entries.
The `clear pim join` command cannot be used to clear the PIM join and prune state on a backup Routing Engine when nonstop active routing is enabled.

**Required Privilege Level**
clear

**Related Documentation**
- show pim join on page 3496

**List of Sample Output**
clear pim join on page 3426
clear pim join inet6 on page 3426
clear pim join inet6 star-g on page 3426

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear pim join

```
user@host> clear pim join
Cleared 8 Join/Prune states
```

clear pim join inet6

```
user@host> clear pim join inet6
Cleared 4 Join/Prune states
```

clear pim join inet6 star-g

```
user@host> clear pim join inet6 star-g
Cleared 1 Join/Prune states
```
clear pim register

**Syntax**
```
clear pim register
<inet | inet6>
<instance instance-name>
<interface interface-name>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**
```
clear pim register
<inet | inet6>
<instance instance-name>
<interface interface-name>
```

**Syntax (PTX Series)**
```
clear pim register
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Release Information**
Command introduced in Junos OS Release 7.6.
Command introduced in Junos OS Release 9.0 for EX Series switches.
*inet6* and *instance* options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Clear Protocol Independent Multicast (PIM) register message counters.

**Options**
- **none**—Clear PIM register message counters for all family addresses, instances, and interfaces.
- **inet | inet6**—(Optional) Clear PIM register message counters for IPv4 or IPv6 family addresses, respectively.
- **instance instance-name**—(Optional) Clear register message counters for a specific PIM-enabled routing instance.
- **interface interface-name**—(Optional) Clear PIM register message counters for a specific interface.
- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**
The `clear pim register` command cannot be used to clear the PIM register state on a backup Routing Engine when nonstop active routing is enabled.

**Required Privilege Level**
clear

**Related Documentation**
- show pim statistics on page 3524

**List of Sample Output**
clear pim register on page 3428

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.
Sample Output

clear pim register

  user@host> clear pim register
clear pim statistics

**Syntax**

`clear pim statistics`  
`<inet | inet6>`  
`<instance instance-name>`  
`<interface interface-name>`  
`<logical-system (all | logical-system-name)>`

**Syntax (EX Series Switch and the QFX Series)**

`clear pim statistics`  
`<inet | inet6>`  
`<instance instance-name>`  
`<interface interface-name>`

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
`inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Clear Protocol Independent Multicast (PIM) statistics.

**Options**

`none`—Clear PIM statistics for all family addresses, instances, and interfaces.  
`<inet | inet6>`—(Optional) Clear PIM statistics for IPv4 or IPv6 family addresses, respectively.  
`instance instance-name`—(Optional) Clear statistics for a specific PIM-enabled routing instance.  
`interface interface-name`—(Optional) Clear PIM statistics for a specific interface.  
`logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Additional Information**

The `clear pim statistics` command cannot be used to clear the PIM statistics on a backup Routing Engine when nonstop active routing is enabled.

**Required Privilege Level**

`clear`

**Related Documentation**

- `show pim statistics` on page 3524

**List of Sample Output**

`clear pim statistics` on page 3429

**Output Fields**

See `show pim statistics` for an explanation of output fields.

**Sample Output**

clear pim statistics

The following sample output displays PIM statistics before and after the `clear pim statistics` command is entered:
```
user@host> show pim statistics
PIM statistics on all interfaces:

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>2111</td>
<td>4222</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>14200</td>
<td>13115</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PIM statistics summary for all interfaces:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown type</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>V1 Unknown type</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown Version</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neighbor unknown</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bad Length</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx Intf disabled</td>
<td>2007</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx V1 Require V2</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx Register not RP</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP Filtered Source</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown Reg Stop</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx Join/Prune no state</td>
<td>1040</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rx Graft/Graft Ack no state</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

user@host> clear pim statistics
user@host> show pim statistics
PIM statistics on all interfaces:

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

...```
**mtrace**

**Syntax**

```
mtrace source
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 9.5 for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Command introduced in Junos OS Release 12.3 for the PTX Series.

**Description**

Display trace information about an IP multicast path.

**Options**

- `source`—Source hostname or address.

- `logical-system (logical-system-name)`—(Optional) Perform this operation on a logical system.

- `routing-instance routing-instance-name`—(Optional) Trace a particular routing instance.

**Additional Information**

The `mtrace` command for multicast traffic is similar to the `traceroute` command used for unicast traffic. Unlike `traceroute`, `mtrace` traces traffic backwards, from the receiver to the source.

**Required Privilege Level**

`view`

**List of Sample Output**

`mtrace source on page 3433`

**Output Fields**

Table 403 on page 3431 describes the output fields for the `mtrace` command. Output fields are listed in the approximate order in which they appear.

**Table 403: mtrace Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mtrace from</td>
<td>IP address of the receiver.</td>
</tr>
<tr>
<td>to</td>
<td>IP address of the source.</td>
</tr>
<tr>
<td>via group</td>
<td>IP address of the multicast group (if any).</td>
</tr>
<tr>
<td>Querying full reverse path</td>
<td>Indicates the full reverse path query has begun.</td>
</tr>
<tr>
<td>number-of-hops</td>
<td>Number of hops from the source to the named router or switch.</td>
</tr>
<tr>
<td>router-name</td>
<td>Name of the router or switch for this hop.</td>
</tr>
<tr>
<td>address</td>
<td>Address of the router or switch for this hop.</td>
</tr>
</tbody>
</table>
Table 403: mtrace Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>Protocol used (for example, PIM).</td>
</tr>
<tr>
<td>Round trip time</td>
<td>Average round-trip time, in milliseconds (ms).</td>
</tr>
<tr>
<td>total ttl of</td>
<td>Time-to-live (TTL) threshold.</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Sample Output
mtrace source

user@host$ mtrace 192.1.4.2
Mtrace from 192.1.4.2 to 192.1.1.2 via group 0.0.0.0
Querying full reverse path... * *
  0  routerA.lab.mycompany.net (192.1.1.2)
  -1  routerB.lab.mycompany.net (192.1.2.2)  PIM  thresh^ 1
  -2  routerC.lab.mycompany.net (192.1.3.2)  PIM  thresh^ 1
  -3  hostA.lab.mycompany.net (192.1.4.2)
Round trip time 2 ms; total ttl of 2 required.
mtrace from-source

Syntax

mtrace from-source source source
<brief | detail>
<extra-hops extra-hops>
<group group>
<interval interval>
<loop>
<max-hops max-hops>
<max-queries max-queries>
<multicast-response | unicast-response>
<no-resolve>
<no-router-alert>
=response response>
<routing-instance routing-instance-name>
<ttl ttl>
<wait-time wait-time>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display trace information about an IP multicast path from a source to this router or switch.
If you specify a group address with this command, Junos OS returns additional information,
such as packet rates and losses.

Options

brief | detail—(Optional) Display the specified level of output.
extra-hops extra-hops—(Optional) Number of hops to take after reaching a nonresponsive
router. You can specify a number between 0 and 255.
group group—(Optional) Group address for which to trace the path. The default group
address is 0.0.0.0.
interval interval—(Optional) Number of seconds to wait before gathering statistics again.
The default value is 10 seconds.
loop—(Optional) Loop indefinitely, displaying rate and loss statistics.
max-hops max-hops—(Optional) Maximum hops to trace toward the source. The range
of values is 0 through 255. The default value is 32 hops.
max-queries max-queries—(Optional) Maximum number of query attempts for any hop.
The range of values is 1 through 32. The default is 3.
multicast-response—(Optional) Always request the response using multicast.
no-resolve—(Optional) Do not attempt to display addresses symbolically.
no-router-alert—(Optional) Do not use the router-alert IP option.
response response—(Optional) Send trace response to a host or multicast address.
routing-instance routing-instance-name—(Optional) Trace a particular routing instance.

source source—Source hostname or address.

ttl ttl—(Optional) IP time-to-live (TTL) value. You can specify a number between 0 and 255. Local queries to the multicast group use a value of 1. Otherwise, the default value is 127.

unicast-response—(Optional) Always request the response using unicast.

wait-time wait-time—(Optional) Number of seconds to wait for a response. The default value is 3.

Required Privilege Level view

List of Sample Output mtrace from-source on page 3436

Output Fields Table 404 on page 3435 describes the output fields for the mtrace from-source command. Output fields are listed in the approximate order in which they appear.

Table 404: mtrace from-source Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mtrace from</td>
<td>IP address of the receiver.</td>
</tr>
<tr>
<td>to</td>
<td>IP address of the source.</td>
</tr>
<tr>
<td>via group</td>
<td>IP address of the multicast group (if any).</td>
</tr>
<tr>
<td>Querying full reverse path</td>
<td>Indicates the full reverse path query has begun.</td>
</tr>
<tr>
<td>number-of-hops</td>
<td>Number of hops from the source to the named router or switch.</td>
</tr>
<tr>
<td>router-name</td>
<td>Name of the router or switch for this hop.</td>
</tr>
<tr>
<td>address</td>
<td>Address of the router or switch for this hop.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol used (for example, PIM).</td>
</tr>
<tr>
<td>Round trip time</td>
<td>Average round-trip time, in milliseconds (ms).</td>
</tr>
<tr>
<td>total ttl of</td>
<td>Time-to-live (TTL) threshold.</td>
</tr>
<tr>
<td>source</td>
<td>Source address.</td>
</tr>
<tr>
<td>Response Dest</td>
<td>Response destination address.</td>
</tr>
<tr>
<td>Overall</td>
<td>Average packet rate for all traffic at each hop.</td>
</tr>
</tbody>
</table>
Table 404: mtrace from-source Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packet Statistics for Traffic From</strong></td>
<td>Number of packets lost, number of packets sent, percentage of packets lost, and average packet rate at each hop.</td>
</tr>
<tr>
<td><strong>Receiver</strong></td>
<td>IP address receiving the multicast.</td>
</tr>
<tr>
<td><strong>Query source</strong></td>
<td>IP address sending the mtrace query.</td>
</tr>
</tbody>
</table>

Sample Output

mtrace from-source

user@host> mtrace from-source source 192.1.4.2 group 225.1.1.1
Mtrace from 192.1.4.2 to 192.1.1.2 via group 225.1.1.1
Querying full reverse path... * *
   0  routerA.lab.mycompany.net (192.1.1.2)
   -1 routerB.lab.mycompany.net (192.1.2.2)  PIM  thresh^ 1
   -2 routerC.lab.mycompany.net (192.1.3.2)  PIM  thresh^ 1
   -3 hostA.lab.mycompany.net (192.1.4.2)
Round trip time 2 ms; total ttl of 2 required.

Waiting to accumulate statistics...Results after 10 seconds:

<table>
<thead>
<tr>
<th>Source</th>
<th>Response</th>
<th>Dest</th>
<th>Overall</th>
<th>Packet Statistics For Traffic From 192.1.4.2 To 225.1.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.1.2.1</td>
<td>v</td>
<td>__/</td>
<td>rtt 2 ms</td>
<td>Rate Lost/Sent = Pct Rate</td>
</tr>
<tr>
<td>192.1.3.2</td>
<td>v</td>
<td>^</td>
<td>ttl 2</td>
<td>0/0 = -- 0 pps</td>
</tr>
<tr>
<td>192.1.4.1</td>
<td>v</td>
<td>___</td>
<td>ttl 3</td>
<td>0/0 = 0 pps</td>
</tr>
<tr>
<td>192.1.1.2</td>
<td>v</td>
<td>___</td>
<td>ttl 3</td>
<td>0/0 = 0 pps</td>
</tr>
</tbody>
</table>

Receiver  Query Source
**mtrace monitor**

**Syntax**

mtrace monitor

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Listen passively for IP multicast responses. To exit the mtrace monitor command, type Ctrl+c.

**Options**

none—Trace the master instance.

**Required Privilege Level**

view

**List of Sample Output**

mtrace monitor on page 3438

**Output Fields**

Table 405 on page 3437 describes the output fields for the mtrace monitor command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mtrace query at</td>
<td>Date and time of the query.</td>
</tr>
<tr>
<td>by</td>
<td>Address of the host issuing the query.</td>
</tr>
<tr>
<td>resp to</td>
<td>Response destination.</td>
</tr>
<tr>
<td>qid</td>
<td>Query ID number.</td>
</tr>
<tr>
<td>packet from...to</td>
<td>IP address of the query source and default group destiny.</td>
</tr>
<tr>
<td>from...to</td>
<td>IP address of the multicast source and the response address.</td>
</tr>
<tr>
<td>via group</td>
<td>IP address of the group to trace.</td>
</tr>
<tr>
<td>mxhop</td>
<td>Maximum hop setting.</td>
</tr>
</tbody>
</table>
Sample Output

mtrace monitor

```plaintext
user@host> mtrace monitor
Mtrace query at Oct 22 13:36:14 by 192.1.3.2, resp to 224.0.1.32, qid 74a5b8 packet from 192.1.3.2 to 224.0.0.2 from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:17 by 192.1.3.2, resp to 224.0.1.32, qid 1d07ba packet from 192.1.3.2 to 224.0.0.2 from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:20 by 192.1.3.2, resp to same, qid 2feald packet from 192.1.3.2 to 224.0.0.2 from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)

Mtrace query at Oct 22 13:36:30 by 192.1.3.2, resp to same, qid 7c88ad packet from 192.1.3.2 to 224.0.0.2 from 192.1.3.2 to 192.1.3.38 via group 224.1.1.1 (mxhop=60)
```

Copyright © 2013, Juniper Networks, Inc.
mtrace to-gateway

**Syntax**

```
mtrace to-gateway gateway gateway
       <brief | detail>
       <extra-hops extra-hops>
       <group group>
       <interface interface-name>
       <interval interval>
       <loop>
       <max-hops max-hops>
       <max-queries max-queries>
       <multicast-response | unicast-response>
       <no-resolve>
       <no-router-alert>
       <response response>
       <routing-instance routing-instance-name>
       < ttl ttl>
       <unicast-response>
       <wait-time wait-time>
```  

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display trace information about a multicast path from this router or switch to a gateway router or switch.

**Options**

- `gateway gateway`—Send the trace query to a gateway multicast address.
- `brief | detail`—(Optional) Display the specified level of output.
- `extra-hops extra-hops`—(Optional) Number of hops to take after reaching a nonresponsive router or switch. You can specify a number between 0 and 255.
- `group group`—(Optional) Group address for which to trace the path. The default group address is 0.0.0.0.
- `interface interface-name`—(Optional) Source address for sending the trace query.
- `interval interval`—(Optional) Number of seconds to wait before gathering statistics again. The default value is 10.
- `loop`—(Optional) Loop indefinitely, displaying rate and loss statistics.
- `max-hops max-hops`—(Optional) Maximum hops to trace toward the source. You can specify a number between 0 and 255. The default value is 32.
- `max-queries max-queries`—(Optional) Maximum number of query attempts for any hop. You can specify a number between 0 and 255. The default value is 3.
- `no-resolve`—(Optional) Do not attempt to display addresses symbolically.
no-router-alert—(Optional) Do not use the router-alert IP option.

response response—(Optional) Send trace response to a host or multicast address.

routing-instance routing-instance-name—(Optional) Trace a particular routing instance.

ttl ttl—(Optional) IP time-to-live value. You can specify a number between 0 and 225.
Local queries to the multicast group use TTL 1. Otherwise, the default value is 127.

unicast-response—(Optional) Always request the response using unicast.

wait-time wait-time—(Optional) Number of seconds to wait for a response. The default value is 3.

**Required Privilege**

view

**List of Sample Output**

mtrace to-gateway on page 3440

Table 406 on page 3440 describes the output fields for the mtrace to-gateway command. Output fields are listed in the approximate order in which they appear.

**Table 406: mtrace to-gateway Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mtrace from</td>
<td>IP address of the receiver.</td>
</tr>
<tr>
<td>to</td>
<td>IP address of the source.</td>
</tr>
<tr>
<td>via group</td>
<td>IP address of the multicast group (if any).</td>
</tr>
<tr>
<td>Querying full reverse path</td>
<td>Indicates the full reverse path query has begun.</td>
</tr>
<tr>
<td>number-of-hops</td>
<td>Number of hops from the source to the named router or switch.</td>
</tr>
<tr>
<td>router-name</td>
<td>Name of the router or switch for this hop.</td>
</tr>
<tr>
<td>address</td>
<td>Address of the router or switch for this hop.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol used (for example, PIM).</td>
</tr>
<tr>
<td>Round trip time</td>
<td>Average round-trip time, in milliseconds (ms).</td>
</tr>
<tr>
<td>total ttl of</td>
<td>Time-to-live (TTL) threshold.</td>
</tr>
</tbody>
</table>

**Sample Output**

mtrace to-gateway

user@host> mtrace to-gateway gateway 192.1.3.2 group 225.1.1.1 interface 192.1.1.73 brief

Mtrace from 192.1.1.73 to 192.1.1.2 via group 225.1.1.1
Querying full reverse path... * *
  
  0  routerA.lab.mycompany.net (192.1.1.2)
-1  routerA.lab.mycompany.net (192.1.1.2)  PIM  thresh^ 1
-2  routerB.lab.mycompany.net (192.1.2.2)  PIM  thresh^ 1
-3  routerC.lab.mycompany.net (192.1.3.2)  PIM  thresh^ 1

Round trip time 2 ms; total ttl of 3 required.
show igmp group

Syntax
show igmp group
<br/>&lt;brief | detail&gt;
<br/>&lt;group-name&gt;
<br/>&lt;logical-system (all | logical-system-name)&gt;

Syntax (EX Series Switch and the QFX Series)
show igmp group
<br/>&lt;brief | detail&gt;
<br/>&lt;group-name&gt;

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display Internet Group Management Protocol (IGMP) group membership information.

Options
none—Display standard information about membership for all IGMP groups.
brief | detail—(Optional) Display the specified level of output.
group-name—(Optional) Display group membership for the specified IP address only.
logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
view

Related Documentation
• clear igmp membership on page 3413

List of Sample Output
show igmp group (Include Mode) on page 3443
show igmp group (Exclude Mode) on page 3444
show igmp group brief on page 3444
show igmp group detail on page 3444

Output Fields
Table 407 on page 3442 describes the output fields for the show igmp group command. Output fields are listed in the approximate order in which they appear.

Table 407: show igmp group Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface that received the IGMP membership report. A name of local indicates that the local routing device joined the group itself.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group Mode</td>
<td>Mode the SSM group is operating in: Include or Exclude.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source</td>
<td>Source address.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 407: show igmp group Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source timeout</td>
<td>Time remaining until the group traffic is no longer forwarded. The timer is refreshed when a listener in include mode sends a report. A group in exclude mode or configured as a static group displays a zero timer.</td>
<td>detail</td>
</tr>
<tr>
<td>Last reported by</td>
<td>Address of the host that last reported membership in this group.</td>
<td>All levels</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time remaining until the group membership is removed.</td>
<td>brief none</td>
</tr>
<tr>
<td>Group timeout</td>
<td>Time remaining until a group in exclude mode moves to include mode. The timer is refreshed when a listener in exclude mode sends a report. A group in include mode or configured as a static group displays a zero timer.</td>
<td>detail</td>
</tr>
<tr>
<td>Type</td>
<td>Type of group membership:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- Dynamic—Host reported the membership.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Static—Membership is configured.</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Output

**show igmp group (Include Mode)**

```
user@host> show igmp group
Interface: t1-0/1/0.0
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.2
    Last reported by: 10.9.5.2
    Timeout: 24 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.3
    Last reported by: 10.9.5.2
    Timeout: 24 Type: Dynamic
  Group: 232.1.1.1
    Group mode: Include
    Source: 10.0.0.4
    Last reported by: 10.9.5.2
    Timeout: 24 Type: Dynamic
  Group: 232.1.1.2
    Group mode: Include
    Source: 10.0.0.4
    Last reported by: 10.9.5.2
    Timeout: 24 Type: Dynamic
  Group: 224.0.0.2
    Source: 0.0.0.0
    Last reported by: Local
    Timeout: 0 Type: Dynamic
  Group: 224.0.0.22
    Source: 0.0.0.0
```
show igmp group (Exclude Mode)

user@host> show igmp group
Interface: t1-0/1/0.0
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
Group: 224.0.0.2
Source: 0.0.0.0
Last reported by: Local
Timeout: 0 Type: Dynamic
Group: 224.0.0.22
Source: 0.0.0.0
Last reported by: Local
Timeout: 0 Type: Dynamic

show igmp group brief

The output for the `show igmp group brief` command is identical to that for the `show igmp group` command.

show igmp group detail

user@host> show igmp group detail
Interface: t1-0/1/0.0
Group: 232.1.1.1
  Group mode: Include
  Source: 10.0.0.2
  Source timeout: 12
  Last reported by: 10.9.5.2
  Group timeout: 0 Type: Dynamic
Group: 232.1.1.1
  Group mode: Include
  Source: 10.0.0.3
  Source timeout: 12
  Last reported by: 10.9.5.2
  Group timeout: 0 Type: Dynamic
Group: 232.1.1.1
  Group mode: Include
  Source: 10.0.0.4
  Source timeout: 12
  Last reported by: 10.9.5.2
  Group timeout: 0 Type: Dynamic
Group: 232.1.1.2
  Group mode: Include
  Source: 10.0.0.4
  Source timeout: 12
  Last reported by: 10.9.5.2
  Group timeout: 0 Type: Dynamic
Interface: t1-0/1/1.0
Interface: ge-0/2/2.0
Interface: ge-0/2/0.0
Interface: local
Group: 224.0.0.2
  Group mode: Exclude
  Source: 0.0.0.0
  Source timeout: 0
Last reported by: Local
Group timeout: 0 Type: Dynamic
Group: 224.0.0.22
Group mode: Exclude
Source: 0.0.0.0
Source timeout: 0
Last reported by: Local
Group timeout: 0 Type: Dynamic
show igmp interface

Syntax

show igmp interface
<brief | detail>
<interface-name>
logical-system (all | logical-system-name)>

Syntax (EX Series Switches and the QFX Series)

show igmp interface
<brief | detail>
<interface-name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display information about Internet Group Management Protocol (IGMP)-enabled interfaces.

Options
none—Display standard information about all IGMP-enabled interfaces.

brief | detail—(Optional) Display the specified level of output.

interface-name—(Optional) Display information about the specified IGMP-enabled interface only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege
Level
view

Related Documentation

• clear igmp membership on page 3413

List of Sample Output

show igmp interface on page 3448
show igmp interface brief on page 3448
show igmp interface detail on page 3449
show igmp interface <interface-name> on page 3449

Output Fields
Table 408 on page 3446 describes the output fields for the show igmp interface command. Output fields are listed in the approximate order in which they appear.

Table 408: show igmp interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Querier</td>
<td>Address of the routing device that has been elected to send membership queries.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface: Up or Down.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 408: show igmp interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSM Map Policy</td>
<td>Name of the source-specific multicast (SSM) map policy that has been applied to the IGMP interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Timeout</td>
<td>How long until the IGMP querier is declared to be unreachable, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Version</td>
<td>IGMP version being used on the interface: 1, 2, or 3.</td>
<td>All levels</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group limit</td>
<td>Maximum number of groups allowed on the interface. Any joins requested after the limit is reached are rejected.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group threshold</td>
<td>Configured threshold at which a warning message is generated. This threshold is based on a percentage of groups received on the interface. If the number of groups received reaches the configured threshold, the device generates a warning message.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group log-interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
<td>All levels</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>State of the immediate leave option:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• On—Indicates that the router removes a host from the multicast group as soon as the router receives a leave group message from a host associated with the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—Indicates that after receiving a leave group message, instead of removing a host from the multicast group immediately, the router sends a group query to determine if another receiver responds.</td>
<td></td>
</tr>
<tr>
<td>Promiscuous Mode</td>
<td>State of the promiscuous mode option:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• On—Indicates that the router can accept IGMP reports from subnetworks that are not associated with its interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—Indicates that the router can accept IGMP reports only from subnetworks that are associated with its interfaces.</td>
<td></td>
</tr>
<tr>
<td>Passive</td>
<td>State of the passive mode option:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• On—Indicates that the router can run IGMP on the interface but not send or receive control traffic such as IGMP reports, queries, and leaves.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Off—Indicates that the router can run IGMP on the interface and send or receive control traffic such as IGMP reports, queries, and leaves.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The passive statement enables you to selectively activate up to two out of a possible three available query or control traffic options. When enabled, the following options appear after the on state declaration:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• send-general-query—The interface sends general queries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• send-group-query—The interface sends group-specific and group-source-specific queries.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• allow-receive—The interface receives control traffic.</td>
<td></td>
</tr>
<tr>
<td>OIF map</td>
<td>Name of the OIF map (if configured) associated with the interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 408: show igmp interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSM map</td>
<td>Name of the source-specific multicast (SSM) map (if configured) used on the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Configured Parameters</strong></td>
<td>Information configured by the user:</td>
<td>All levels</td>
</tr>
<tr>
<td>• IGMP Query Interval—Interval (in seconds) at which this router sends membership queries when it is the querier.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IGMP Query Response Interval—Time (in seconds) that the router waits for a report in response to a general query.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IGMP Last Member Query Interval—Time (in seconds) that the router waits for a report in response to a group-specific query.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IGMP Robustness Count—Number of times the router retries a query.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Derived Parameters</strong></td>
<td>Derived information:</td>
<td>All levels</td>
</tr>
<tr>
<td>• IGMP Membership Timeout—Timeout period (in seconds) for group membership. If no report is received for these groups before the timeout expires, the group membership is removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IGMP Other Querier Present Timeout—Time (in seconds) that the router waits for the IGMP querier to send a query.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

```bash
show igmp interface

user@host> show igmp interface
Interface: at-0/3/1.0
   Querier: 10.111.30.1
   State:    Up Timeout:    None Version:  2 Groups:      4
   SSM Map Policy: ssm-policy-A
Interface: so-1/0/0.0
   Querier: 10.111.10.1
   State:    Up Timeout:    None Version:  2 Groups:      2
   SSM Map Policy: ssm-policy-B
Interface: so-1/0/1.0
   Querier: 10.111.20.1
   State:    Up Timeout:    None Version:  2 Groups:      4
   SSM Map Policy: ssm-policy-C
Immediate Leave: On
Promiscuous Mode: Off

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Derived Parameters:
IGMP Membership Timeout: 260.0
IGMP Other Querier Present Timeout: 255.0
```

show igmp interface brief

The output for the show igmp interface brief command is identical to that for the show igmp interface command. For sample output, see show igmp interface on page 3448.
show igmp interface detail

The output for the `show igmp interface detail` command is identical to that for the `show igmp interface` command. For sample output, see `show igmp interface` on page 3448.

```
show igmp interface <interface-name>
```

```
user@host# show igmp interface ge-3/2/0.0
Interface: ge-3/2/0.0
    Querier: 20.1.1.1
    State: Up Timeout: None Version: 3 Groups: 1
    Group limit: 8
    Group threshold: 60
    Group log-interval: 10
    Immediate leave: Off
    Promiscuous mode: Off
```
show igmp statistics

Syntax

show igmp statistics

Syntax (EX Series Switch and the QFX Series)

show igmp statistics

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display Internet Group Management Protocol (IGMP) statistics.

Options

none—Display IGMP statistics for all interfaces.

brief | detail—(Optional) Display the specified level of output.

interface interface-name—(Optional) Display IGMP statistics about the specified interface only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

Related Documentation

• clear igmp statistics on page 3416

List of Sample Output

show igmp statistics on page 3451
show igmp statistics interface on page 3452

Output Fields

Table 409 on page 3450 describes the output fields for the show igmp statistics command. Output fields are listed in the approximate order in which they appear.

Table 409: show igmp statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP packet statistics</td>
<td>Heading for IGMP packet statistics for all interfaces or for the specified interface name.</td>
</tr>
</tbody>
</table>
Table 409: show igmp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Message type</td>
<td>Summary of IGMP statistics:</td>
</tr>
<tr>
<td></td>
<td>• Membership Query—Number of membership queries sent and received.</td>
</tr>
<tr>
<td></td>
<td>• V1 Membership Report—Number of version 1 membership reports sent and received.</td>
</tr>
<tr>
<td></td>
<td>• DVMRP—Number of DVMRP messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• PIM V1—Number of PIM version 1 messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Cisco Trace—Number of Cisco trace messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• V2 Membership Report—Number of version 2 membership reports sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Group Leave—Number of group leave messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Mtrace Response—Number of Mtrace response messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Mtrace Request—Number of Mtrace request messages sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Domain Wide Report—Number of domain-wide reports sent or received.</td>
</tr>
<tr>
<td></td>
<td>• V3 Membership Report—Number of version 3 membership reports sent or received.</td>
</tr>
<tr>
<td></td>
<td>• Other Unknown types—Number of unknown message types received.</td>
</tr>
<tr>
<td></td>
<td>• IGMP v3 unsupported type—Number of messages received with unknown and unsupported IGMP version 3 message types.</td>
</tr>
<tr>
<td></td>
<td>• IGMP v3 source required for SSM—Number of IGMP version 3 messages received that contained no source.</td>
</tr>
<tr>
<td></td>
<td>• IGMP v3 mode not applicable for SSM—Number of IGMP version 3 messages received that did not contain a mode applicable for source-specific multicast (SSM).</td>
</tr>
<tr>
<td>Received</td>
<td>Number of messages received.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of messages sent.</td>
</tr>
<tr>
<td>Rx errors</td>
<td>Number of received packets that contained errors.</td>
</tr>
</tbody>
</table>

IGMP Global Statistics: Summary of IGMP statistics for all interfaces.

- **Bad Length**—Number of messages received with length errors so severe that further classification could not occur.
- **Bad Checksum**—Number of messages received with a bad IP checksum. No further classification was performed.
- **Bad Receive If**—Number of messages received on an interface not enabled for IGMP.
- **Rx non-local**—Number of messages received from senders that are not local.
- **Timed out**—Number of groups that timed out as a result of not receiving an explicit leave message.
- **Rejected Report**—Number of reports dropped because of the IGMP group policy.
- **Total Interfaces**—Number of interfaces configured to support IGMP.

Sample Output

```
show igmp statistics
IGMP packet statistics for all interfaces
IGMP Message type        Received Sent  Rx errors
Membership Query          8883    459    0
V1 Membership Report      0       0      0
```
<table>
<thead>
<tr>
<th>Message Type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Query</td>
<td></td>
<td>230</td>
<td></td>
</tr>
<tr>
<td>V1 Membership Report</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**IGMP Global Statistics**

- Bad Length: 0
- Bad Checksum: 0
- Bad Receive If: 0
- Rx non-local: 1227
- Timed out: 0
- Rejected Report: 0
- Total Interfaces: 2

**show igmp statistics interface**

```
user@host> show igmp statistics interface fe-1/0/1.0
IGMP interface packet statistics for fe-1/0/1.0
IGMP Message type    Received  Sent  Rx errors
Membership Query      0        230  0
V1 Membership Report  0        0    0
```
show igmp-snooping membership

Syntax

show igmp-snooping membership
  <brief | detail>
  <interface interface-name>
  <vlan (vlan-id | vlan-name)>

Release Information

Command introduced in Junos OS Release 9.1 for EX Series switches.

Description

Display the multicast group membership information maintained by IGMP snooping.

Options

none—Display the multicast group membership information about all VLANs on which IGMP snooping is enabled.

brief | detail—(Optional) Display the specified level of output. The default is brief.

interface interface-name—(Optional) Display the multicast group membership information about the specified interface.

vlan (vlan-id | vlan-name)—(Optional) Display the multicast group membership for the specified VLAN.

Required Privilege

Level view

Related Documentation

- show igmp-snooping route on page 3456
- show igmp-snooping statistics on page 3458
- show igmp-snooping vlans
- Verifying IGMP Snooping (CLI Procedure) on page 3410
- Configuring IGMP Snooping (CLI Procedure)

List of Sample Output

show igmp-snooping membership on page 3454
show igmp-snooping membership detail on page 3454
show igmp-snooping membership vlan detail on page 3455

Output Fields

Table 410 on page 3453 lists the output fields for the show igmp-snooping membership command. Output fields are listed in the approximate order in which they appear.

Table 410: show igmp-snooping membership Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Name of the VLAN.</td>
<td>All</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Interfaces that are members of the listed multicast group.</td>
<td>All</td>
</tr>
<tr>
<td>Tag</td>
<td>Numerical identifier of the VLAN.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 410: show igmp-snooping membership Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router interfaces</td>
<td>List of information about multicast-router interfaces:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Name of the multicast-router interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>static</strong> or <strong>dynamic</strong>—Whether the multicast-router interface is static or dynamic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Uptime</strong>—For static interfaces, amount of time since the interface was configured as a multicast-router interface or since the interface last flapped. For dynamic interfaces, amount of time since the first query was received on the interface or since the interface last flapped.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>timeout</strong>—Seconds remaining before a dynamic multicast-router interface times out.</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td>IP multicast address of the multicast group.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>The following information is provided for the multicast group:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Name of the interface belonging to the multicast group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Last reporter</strong>—Last host to report membership for the multicast group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Receiver count</strong>—Number of hosts on the interface that are members of the multicast group. This field appears only if <strong>immediate-leave</strong> is configured on the VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Uptime</strong>—Length of time (in hours, minutes, and seconds) a multicast group has been active on the interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>timeout</strong>—Time (in seconds) left until the entry for the multicast group is removed from the multicast group if no membership reports are received on the interface. This counter is reset to its maximum value when a membership report is received.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Flags</strong>—The lowest IGMP version in use by a host that is a member of the group on the interface. If the flag <strong>static</strong> is included, the interface has been configured as static member of the multicast group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>include source</strong>—Multicast source addresses of all IGMPv3 membership reports received for the group on the interface.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

```bash
show igmp-snooping membership

user@switch> show igmp-snooping membership
VLAN: vlan24
  224.1.1.1      *
      Interfaces: ge-0/0/0.0
  224.1.1.100    *
      Interfaces: ge-0/0/0.0
  225.1.1.100    *
      Interfaces: ge-0/0/0.0

show igmp-snooping membership detail

user@switch> show igmp-snooping membership detail
VLAN: vlan2 Tag: 2 (Index: 3)
  Router interfaces:
```

Copyright © 2013, Juniper Networks, Inc.
show igmp-snooping membership vlan detail

user@switch> show igmp-snooping membership vlan vlan700 detail
VLAN: vlan700 Tag: 700 (Index: 52)
  Router interfaces:
    ae2.0 dynamic Uptime: 16:53:13 timeout: 245
  Group: 230.150.10.1
  ge-0/0/1.0 Last reporter: 100.2.188.201
    Uptime: 17:00:52 timeout: 237 Flags: <V2-hosts>
  ge-0/0/0.0 Last reporter: 100.2.188.202
    Uptime: 17:00:50 timeout: 243 Flags: <V2-hosts>
show igmp-snooping route

Syntax

```
show igmp-snooping route
  <brief | detail>
  <ethernet-switching | inet>
  <vlan (vlan-id | vlan-name)>
```

Release Information

Command introduced in Junos OS Release 9.1 for EX Series switches.

Description

Display IGMP snooping route information.

Options

- `none`—Display route information for all VLANs on which IGMP snooping is enabled.
- `brief | detail`—(Optional) Display the specified level of output. The default is `brief`.
- `ethernet-switching`—(Optional) Display information on Layer 2 multicast routes. This is the default.
- `inet`—(Optional) Display information for Layer 3 multicast routes.
- `vlan (vlan-id | vlan-name)`—(Optional) Display route information for the specified VLAN.

Required Privilege

`view`

Related Documentation

- `show igmp-snooping membership` on page 3453
- `show igmp-snooping statistics` on page 3458
- `show igmp-snooping vlans`
- `Verifying IGMP Snooping (CLI Procedure)` on page 3410
- `Configuring IGMP Snooping (CLI Procedure)`

List of Sample Output

- `show igmp-snooping route vlan v18` on page 3457
- `show igmp-snooping route detail` on page 3457
- `show igmp-snooping route inet detail` on page 3457

Output Fields

Table 411 on page 3456 lists the output fields for the `show igmp-snooping route` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Routing table ID for virtual routing instances.</td>
</tr>
<tr>
<td>Routing Table</td>
<td>Routing table ID for virtual routing instances.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Name of the VLAN on which IGMP snooping is enabled.</td>
</tr>
<tr>
<td>Group</td>
<td>Multicast IPv4 group address.</td>
</tr>
</tbody>
</table>
### Table 411: show igmp-snooping route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-hop</td>
<td>ID associated with the next-hop device.</td>
</tr>
<tr>
<td>Routing next-hop</td>
<td>ID associated with the Layer 3 next-hop device.</td>
</tr>
<tr>
<td>Interface or Interfaces</td>
<td>Name of the interface or interfaces in the VLAN associated with the multicast group.</td>
</tr>
<tr>
<td>Layer 2 next-hop</td>
<td>ID associated with the Layer 2 next-hop device.</td>
</tr>
</tbody>
</table>

#### Sample Output

**show igmp-snooping route vlan v18**

```plaintext
user@switch> show igmp-snooping route vlan v18
VLAN    Group          Next-hop
vlan18  224.0.0.0, *  
vlan18  225.20.20.1, * 1539
```

**show igmp-snooping route detail**

```plaintext
user@switch> show igmp-snooping route detail
VLAN    Group          Next-hop
default 224.0.0.0, *  
vlant100 224.0.0.0, *  1332
  Interfaces: ge-1/0/1.0
VLAN    Group          Next-hop
vlant100 226.0.0.1, *  1334
  Interfaces: ge-1/0/1.0, ge-5/0/30.0
```

**show igmp-snooping route inet detail**

```plaintext
user@switch> show igmp-snooping route inet detail
Routing table: 0
Group: 229.0.0.1, 171.2.60.100
  Routing next-hop: 3448
    vlan.100
      Interface: vlan.100, VLAN: vlan100, Layer 2 next-hop: 3343
```
show igmp-snooping statistics

**Syntax**
show igmp-snooping statistics

**Release Information**
Command introduced in Junos OS Release 9.1 for EX Series switches.

**Description**
Display IGMP snooping statistics.

**Required Privilege Level**
view

**Related Documentation**
- clear igmp-snooping statistics on page 3419
- show igmp-snooping membership on page 3453
- show igmp-snooping route on page 3456
- show igmp-snooping vlans
- Verifying IGMP Snooping (CLI Procedure) on page 3410
- Configuring IGMP Snooping (CLI Procedure)

**List of Sample Output**
show igmp-snooping statistics on page 3459

**Output Fields**
Table 412 on page 3458 lists the output fields for the show igmp-snooping statistics command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad length</td>
<td>IGMP packet has illegal or bad length.</td>
</tr>
<tr>
<td>Bad checksum</td>
<td>IGMP or IP checksum is incorrect.</td>
</tr>
<tr>
<td>Invalid interface</td>
<td>Packet was received through an invalid interface.</td>
</tr>
<tr>
<td>Not local</td>
<td>Not used—always 0.</td>
</tr>
<tr>
<td>Receive unknown</td>
<td>Unknown IGMP type.</td>
</tr>
<tr>
<td>Timed out</td>
<td>Not used—always 0.</td>
</tr>
<tr>
<td>IGMP Type</td>
<td>Type of IGMP message (Query, Report, Leave, or Other).</td>
</tr>
<tr>
<td>Received</td>
<td>Number of IGMP packets received.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Number of IGMP packets transmitted.</td>
</tr>
<tr>
<td>Recv Errors</td>
<td>Number of packets received that did not conform to the IGMP version 1 (IGMPv1), IGMPv2, or IGMPv3 standards.</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
Sample Output

```
show igmp-snooping statistics
```

```
user@switch>  show igmp-snooping statistics
Bad length: 0  Bad checksum: 0  Invalid interface: 0
Not local: 0  Receive unknown: 0  Timed out: 0

<table>
<thead>
<tr>
<th>IGMP Type</th>
<th>Received</th>
<th>Transmitted</th>
<th>Recv Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries:</td>
<td>74295</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reports:</td>
<td>18148423</td>
<td>0</td>
<td>16333523</td>
</tr>
<tr>
<td>Leaves:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
**show multicast flow-map**

**Syntax**

```
show multicast flow-map
  <brief | detail>
  <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**

```
show multicast flow-map
  <brief | detail>
```

**Release Information**

- Command introduced in Junos OS Release 8.2.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display configuration information about IP multicast flow maps.

**Options**

- `none` — Display configuration information about IP multicast flow maps on all systems.
- `brief | detail` — (Optional) Display the specified level of output.
- `logical-system (all | logical-system-name)` — (Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege**

```
view
```

**List of Sample Output**

- `show multicast flow-map on page 3461`
- `show multicast flow-map detail on page 3461`

**Output Fields**

Table 413 on page 3460 describes the output fields for the `show multicast flow-map` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Levels of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the flow map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Policy</td>
<td>Name of the policy associated with the flow map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Cache-timeout</td>
<td>Cache timeout value assigned to the flow map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Bandwidth setting associated with the flow map.</td>
<td>All levels</td>
</tr>
<tr>
<td>Adaptive</td>
<td>Whether or not adaptive mode is enabled for the flow map.</td>
<td>none</td>
</tr>
<tr>
<td>Flow-map</td>
<td>Name of the flow map.</td>
<td>detail</td>
</tr>
<tr>
<td>Adaptive Bandwidth</td>
<td>Whether or not adaptive mode is enabled for the flow map.</td>
<td>detail</td>
</tr>
<tr>
<td>Redundant Sources</td>
<td>Redundant sources defined for the same destination group.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Sample Output
show multicast flow-map

```
user@host> show multicast flow-map
Instance: master

<table>
<thead>
<tr>
<th>Name</th>
<th>Policy</th>
<th>Cache timeout</th>
<th>Bandwidth</th>
<th>Adaptive</th>
</tr>
</thead>
<tbody>
<tr>
<td>map2</td>
<td>policy2</td>
<td>never</td>
<td>2000000</td>
<td>no</td>
</tr>
<tr>
<td>map1</td>
<td>policy1</td>
<td>60 seconds</td>
<td>2000000</td>
<td>no</td>
</tr>
</tbody>
</table>
```

Sample Output
show multicast flow-map detail

```
user@host> show multicast flow-map detail
Instance: master
Flow-map: map1

<table>
<thead>
<tr>
<th>Policy</th>
<th>Cache Timeout</th>
<th>Bandwidth</th>
<th>Adaptive Bandwidth</th>
<th>Redundant Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy1</td>
<td>600 seconds</td>
<td>2000000</td>
<td>yes</td>
<td>11.11.11.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11.11.11.12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11.11.11.13</td>
</tr>
</tbody>
</table>
```
**show multicast interface**

**Syntax**
show multicast interface  
<logical-system (all | logical-system-name)>

**Syntax (EX Series Switch and the QFX Series)**
show multicast interface

**Release Information**
Command introduced in Junos OS Release 8.3.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Display bandwidth information about IP multicast interfaces.

**Options**
none—Display all interfaces that have multicast configured.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
view

**List of Sample Output**
show multicast interface on page 3463

**Output Fields**
Table 414 on page 3462 describes the output fields for the show multicast interface command. Output fields are listed in the approximate order in which they appear.

**Table 414: show multicast interface Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the multicast interface.</td>
</tr>
<tr>
<td>Maximum bandwidth (bps)</td>
<td>Maximum bandwidth setting, in bits per second, for this interface.</td>
</tr>
<tr>
<td>Remaining bandwidth (bps)</td>
<td>Amount of bandwidth, in bits per second, remaining on the interface.</td>
</tr>
</tbody>
</table>
| Mapped bandwidth deduction (bps)  | Amount of bandwidth, in bits per second, used by any flows that are mapped to the interface.  
**NOTE:** Adding the mapped bandwidth deduction value to the local bandwidth deduction value results in the total deduction value for the interface.  
This field does not appear in the output when the no QoS adjustment feature is disabled. |
### Table 414: show multicast interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local bandwidth deduction (bps)</td>
<td>Amount of bandwidth, in bits per second, used by any mapped flows that are traversing the interface.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Adding the mapped bandwidth deduction value to the local bandwidth deduction value results in the total deduction value for the interface.</td>
</tr>
<tr>
<td></td>
<td>This field does not appear in the output when the no QoS adjustment feature is disabled.</td>
</tr>
<tr>
<td>Reverse OIF mapping</td>
<td>State of the reverse OIF mapping feature (on or off).</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This field does not appear in the output when the no QoS adjustment feature is disabled.</td>
</tr>
<tr>
<td>Reverse OIF mapping no QoS adjustment</td>
<td>State of the no QoS adjustment feature (on or off) for interfaces that are using reverse OIF mapping.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This field does not appear in the output when the no QoS adjustment feature is disabled.</td>
</tr>
<tr>
<td>Leave timer</td>
<td>Amount of time a mapped interface remains active after the last mapping ends.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This field does not appear in the output when the no QoS adjustment feature is disabled.</td>
</tr>
<tr>
<td>No QoS adjustment</td>
<td>State (on) of the no QoS adjustment feature when this feature is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This field does not appear in the output when the no QoS adjustment feature is disabled.</td>
</tr>
</tbody>
</table>

**Sample Output**

```text
show multicast interface

user@host> show multicast interface

Interface                Maximum bandwidth (bps) Remaining bandwidth (bps)
fe-0/0/3                                10000000                         0
fe-0/0/3.210                            10000000                        -2000000
fe-0/0/3.220                            100000000                     -10000000
fe-0/0/3.230                            20000000                      18000000
fe-0/0/2.200                            100000000                     100000000
```

**Copyright © 2013, Juniper Networks, Inc.**
**show multicast mrinfo**

**Syntax**
```
show multicast mrinfo
<host>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**
Display configuration information about IP multicast networks, including neighboring multicast router addresses.

**Options**
- `none`—Display configuration information about all multicast networks.
- `host`—(Optional) Display configuration information about a particular host. Replace `host` with a hostname or IP address.

**Required Privilege Level**
`view`

**List of Sample Output**
`show multicast mrinfo on page 3465`

**Output Fields**
Table 415 on page 3464 describes the output fields for the `show multicast mrinfo` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-address</td>
<td>Query address, hostname (DNS name or IP address of the source address), and multicast protocol version or the software version of another vendor.</td>
</tr>
<tr>
<td>ip-address-1→ip-address-2</td>
<td>Queried router interface address and directly attached neighbor interface address, respectively.</td>
</tr>
<tr>
<td>(name or ip-address)</td>
<td>Name or IP address of neighbor.</td>
</tr>
<tr>
<td>[metric/threshold/type/flags]</td>
<td>Neighbor’s multicast profile:</td>
</tr>
<tr>
<td></td>
<td>• metric—Always has a value of 1, because <code>mrinfo</code> queries the directly connected interfaces of a device.</td>
</tr>
<tr>
<td></td>
<td>• threshold—Multicast threshold time-to-live (TTL). The range of values is 0 through 255.</td>
</tr>
<tr>
<td></td>
<td>• type—Multicast connection type: <code>pim</code> or <code>tunnel</code>.</td>
</tr>
<tr>
<td></td>
<td>• flags—Flags for this route:</td>
</tr>
<tr>
<td></td>
<td>• querier—Queried router is the designated router for the neighboring session.</td>
</tr>
<tr>
<td></td>
<td>• leaf—Link is a leaf in the multicast network.</td>
</tr>
<tr>
<td></td>
<td>• down—Link status indicator.</td>
</tr>
</tbody>
</table>
Sample Output

show multicast mrinfo

user@host> show multicast mrinfo 10.35.4.1
10.35.4.1 (10.35.4.1) [version 12.0]:
  192.168.195.166 -> 0.0.0.0 (local) [1/0/pim/querier/leaf]
  10.38.20.1 -> 0.0.0.0 (local) [1/0/pim/querier/leaf]
  10.47.1.1 -> 10.47.1.2 (10.47.1.2) [1/5/pim]
  0.0.0.0 -> 0.0.0.0 (local) [1/0/pim/down]
**show multicast next-hops**

**Syntax**

```
show multicast next-hops
   <brief | detail>
   <identifier-number>
   <inet | inet6>
   <logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**

```
show multicast next-hops
   <brief | detail>
   <identifier-number>
   <inet | inet6>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`inet6` option introduced in Junos OS Release 10.0 for EX Series switches.
`detail` option display of next-hop ID number introduced in Junos OS Release 11.1 for M Series and T Series routers and EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.

**Description**

Display the entries in the IP multicast next-hop table.

**Options**

- **none**—Display standard information about all entries in the multicast next-hop table for all supported address families.
- **brief | detail**—(Optional) Display the specified level of output.
  
  When you include the `detail` option on M Series and T Series routers and EX Series switches, the downstream interface name includes the next-hop ID number in parentheses, in the form `fe-0/1/2.0-(1048574)` where 1048574 is the next-hop ID number.

- **identifier-number**—(Optional) Show a particular next hop by ID number. The range of values is 1 through 65,535.

- **inet | inet6**—(Optional) Display entries for IPv4 or IPv6 family addresses, respectively.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

view

**List of Sample Output**

- show multicast next-hops on page 3467
- show multicast next-hops (Bidirectional PIM on page 3467
- show multicast next-hops brief on page 3468
- show multicast next-hops detail on page 3468

**Output Fields**

Table 416 on page 3467 describes the output fields for the `show multicast next-hops` command. Output fields are listed in the approximate order in which they appear.
Table 416: show multicast next-hops Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family</td>
<td>Protocol family (such as INET).</td>
</tr>
<tr>
<td>ID</td>
<td>Next-hop identifier of the prefix. The identifier is returned by the routing device's Packet Forwarding Engine.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of cache entries that are using this next hop.</td>
</tr>
<tr>
<td>KRefcount</td>
<td>Kernel reference count for the next hop.</td>
</tr>
<tr>
<td>Downstream interface</td>
<td>Interface names associated with each multicast next-hop ID.</td>
</tr>
<tr>
<td>Incoming interface list</td>
<td>List of interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.</td>
</tr>
</tbody>
</table>

Sample Output

show multicast next-hops

```
user@host> show multicast next-hops
Family: INET
ID      Refcount  KRefcount Downstream interface
262142          4          2 so-1/0/0.0
262143          2          1 mt-1/1/0.49152
262148          2          1 mt-1/1/0.32769
```

show multicast next-hops (Bidirectional PIM)

```
user@host> show multicast next-hops
Family: INET
ID      Refcount  KRefcount Downstream interface
2097151            8         4 ge-0/0/1.0

Family: INET6
ID      Refcount  KRefcount Downstream interface
2097157            2         1 ge-0/0/1.0

Family: Incoming interface list
ID      Refcount  KRefcount Downstream interface
513                5         2 lo0.0  ge-0/0/1.0
514                5         2 lo0.0  ge-0/0/1.0  xe-4/1/0.0
515                3         1 lo0.0  ge-0/0/1.0  xe-4/1/0.0
544                1         0 lo0.0  xe-4/1/0.0
```
show multicast next-hops brief

The output for the show multicast next-hops brief command is identical to that for the show multicast next-hops command. For sample output, see show multicast next-hops on page 3467.

show multicast next-hops detail

```
user@host> show multicast next-hops detail  
Family: INET  
ID          Refcount KRefcount Downstream interface  
1048577         2             1 fe-0/1/2.0-(1048574)   
                 ge-0/2/3.0-(1048576)
```
show multicast pim-to-igmp-proxy

Syntax

show multicast pim-to-igmp-proxy
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)

show multicast pim-to-igmp-proxy
<instance instance-name>

Release Information
Command introduced in Junos OS Release 9.6 for EX Series switches.
instance option introduced in Junos OS Release 10.3.
instance option introduced in Junos OS Release 10.3 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description
Display configuration information about PIM-to-IGMP message translation, also known as PIM-to-IGMP proxy.

Options

none—Display configuration information about PIM-to-IGMP message translation for all routing instances.

instance instance-name—(Optional) Display configuration information about PIM-to-IGMP message translation for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level
view

Related Documentation
• Configuring PIM-to-IGMP and PIM-to-MLD Message Translation

List of Sample Output

show multicast pim-to-igmp-proxy on page 3470
show multicast pim-to-igmp-proxy instance on page 3470

Output Fields
Table 417 on page 3469 describes the output fields for the show multicast pim-to-igmp-proxy command. Output fields are listed in the order in which they appear.

Table 417: show multicast pim-to-igmp-proxy Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Routing instance. Default instance is master (inet.0 routing table).</td>
</tr>
<tr>
<td>Proxy state</td>
<td>State of PIM-to-IGMP message translation, also known as PIM-to-IGMP proxy, on the configured upstream interfaces: enabled or disabled.</td>
</tr>
<tr>
<td>interface-name</td>
<td>Name of upstream interface (no more than two allowed) on which PIM-to-IGMP message translation is configured.</td>
</tr>
</tbody>
</table>
Sample Output

show multicast pim-to-igmp-proxy

user@host> show multicast pim-to-igmp-proxy
Instance: master Proxy state: enabled
ge-0/1/0.1
ge-0/1/0.2

show multicast pim-to-igmp-proxy instance

user@host> show multicast pim-to-igmp-proxy instance VPN-A
Instance: VPN-A Proxy state: enabled
ge-0/1/0.1
**Syntax**

```
show multicast pim-to-mld-proxy
<instance instance-name>
<logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**

```
show multicast pim-to-mld-proxy
<instance instance-name>
```

**Release Information**

- Command introduced in Junos OS Release 9.6 for EX Series switches.
- `instance` option introduced in Junos OS Release 10.3.
- `instance` option introduced in Junos OS Release 10.3 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display configuration information about PIM-to-MLD message translation, also known as PIM-to-MLD proxy.

**Options**

- `none`—Display configuration information about PIM-to-MLD message translation for all routing instances.

- `instance instance-name`—(Optional) Display configuration information about PIM-to-MLD message translation for a specific multicast instance.

- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

`view`

**List of Sample Output**

- `show multicast pim-to-mld-proxy` on page 3472
- `show multicast pim-to-mld-proxy instance` on page 3472

**Output Fields**

Table 418 on page 3471 describes the output fields for the `show multicast pim-to-mld-proxy` command. Output fields are listed in the order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy state</td>
<td>State of PIM-to-MLD message translation, also known as PIM-to-MLD proxy, on the configured upstream interfaces: <code>enabled</code> or <code>disabled</code>.</td>
</tr>
<tr>
<td><code>interface-name</code></td>
<td>Name of upstream interface (no more than two allowed) on which PIM-to-MLD message translation is configured.</td>
</tr>
</tbody>
</table>
Sample Output

show multicast pim-to-mld-proxy

user@host> show multicast pim-to-mld-proxy
Instance: master Proxy state: enabled
ge-0/5/0.1
ge-0/5/0.2

show multicast pim-to-mld-proxy instance

user@host> show multicast pim-to-mld-proxy instance VPN-A
Instance: VPN-A Proxy state: enabled
ge-0/5/0.1
show multicast route

Syntax

show multicast route
   <brief | detail | extensive | summary>
   <active | all | inactive>
   <group group>
   <inet | inet6>
   <instance instance name>
   <logical-system (all | logical-system-name)>
   <regular-expression>
   <source-prefix source-prefix>

Syntax (EX Series Switch and the QFX Series)

show multicast route
   <brief | detail | extensive | summary>
   <active | all | inactive>
   <group group>
   <inet | inet6>
   <instance instance name>
   <regular-expression>
   <source-prefix source-prefix>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.

Description

Display the entries in the IP multicast forwarding table. You can display similar information with the show route table inet.1 command.

Options

none—Display standard information about all entries in the multicast forwarding table for all routing instances.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

active | all | inactive—(Optional) Display all active entries, all entries, or all inactive entries, respectively, in the multicast forwarding table.

group group—(Optional) Display the cache entries for a particular group.

inet | inet6—(Optional) Display multicast forwarding table entries for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Display entries in the multicast forwarding table for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

regular-expression—(Optional) Display information about the multicast forwarding table entries that match a UNIX OS-style regular expression.
**source-prefix source-prefix**—(Optional) Display the cache entries for a particular source prefix.

**Required Privilege**  
view

**Level**

**List of Sample Output**  
show multicast route on page 3475  
show multicast route (Bidirectional PIM) on page 3476  
show multicast route brief on page 3476  
show multicast route detail on page 3476  
show multicast route extensive (Bidirectional PIM) on page 3477  
show multicast route instance <instance-name> on page 3478  
show multicast route summary on page 3478

**Output Fields**  
Table 419 on page 3474 describes the output fields for the **show multicast route** command. Output fields are listed in the approximate order in which they appear.

**Table 419: show multicast route Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>family</td>
<td>IPv4 address family (<strong>INET</strong>) or IPv6 address family (<strong>INET6</strong>).</td>
<td>All levels</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>For any-source multicast routes, for example for bidirectional PIM, the group address includes the prefix length.</td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Prefix and length of the source as it is in the multicast forwarding table.</td>
<td>All levels</td>
</tr>
<tr>
<td>Incoming interface list</td>
<td>List of interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.</td>
<td>All levels</td>
</tr>
<tr>
<td>Upstream interface</td>
<td>Name of the interface on which the packet with this source prefix is expected to arrive.</td>
<td>All levels</td>
</tr>
<tr>
<td>Downstream interface list</td>
<td>List of interface names to which the packet with this source prefix is forwarded.</td>
<td>All levels</td>
</tr>
<tr>
<td>Number of outgoing interfaces</td>
<td>Total number of outgoing interfaces for each (S,G) entry.</td>
<td>extensive</td>
</tr>
<tr>
<td>Session description</td>
<td>Name of the multicast session.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Statistics</td>
<td>Rate at which packets are being forwarded for this source and group entry (in Kbps and pps), and number of packets that have been forwarded to this prefix. If one or more of the kilobits per second packet forwarding statistic queries fails or times out, the statistics field displays <strong>Forwarding statistics are not available.</strong></td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> On QFX Series switches, this field does not report valid statistics.</td>
<td></td>
</tr>
<tr>
<td>Next-hop ID</td>
<td>Next-hop identifier of the prefix. The identifier is returned by the routing device’s Packet Forwarding Engine and is also displayed in the output of the <strong>show multicast nexthops</strong> command.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
### Table 419: show multicast route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming interface list ID</td>
<td>For bidirectional PIM, incoming interface list identifier.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>Identifiers for interfaces that accept incoming traffic. Only shown for routes that do not use strict RPF-based forwarding, for example for bidirectional PIM.</td>
<td></td>
</tr>
<tr>
<td>Upstream protocol</td>
<td>The protocol that maintains the active multicast forwarding route for this group or source.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>When the <code>show multicast route extensive</code> command is used with the <code>display-origin-protocol</code> option, the field name is only <code>Protocol</code> and not <code>Upstream Protocol</code>. However, this field also displays the protocol that installed the active route.</td>
<td></td>
</tr>
<tr>
<td>Route type</td>
<td>Type of multicast route. Values can be (S,G) or (*,G).</td>
<td>summary</td>
</tr>
<tr>
<td>Route state</td>
<td>Whether the group is Active or Inactive.</td>
<td>summary extensive</td>
</tr>
<tr>
<td>Route count</td>
<td>Number of multicast routes.</td>
<td>summary</td>
</tr>
<tr>
<td>Forwarding state</td>
<td>Whether the prefix is pruned or forwarding.</td>
<td>extensive</td>
</tr>
<tr>
<td>Cache lifetime/timeout</td>
<td>Number of seconds until the prefix is removed from the multicast forwarding table. A value of <code>never</code> indicates a permanent forwarding entry. A value of <code>forever</code> indicates routes that do not have keepalive times.</td>
<td>extensive</td>
</tr>
<tr>
<td>Wrong incoming interface notifications</td>
<td>Number of times that the upstream interface was not available.</td>
<td>extensive</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time since the creation of a multicast route.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

### Sample Output

`show multicast route`

```bash
user@host> show multicast route
Family: INET

Group: 228.0.0.0
  Source: 10.255.14.144/32
  Upstream interface: local
  Downstream interface list:
    so-1/0/0.0

Group: 239.1.1.1
  Source: 10.255.14.144/32
  Upstream interface: local
  Downstream interface list:
    so-1/0/0.0

Group: 239.1.1.1
  Source: 10.255.70.15/32
```
Upstream interface: so-1/0/0.0
Downstream interface list:
  mt-1/1/0.1081344

Family: INET6

**show multicast route (Bidirectional PIM)**

```
user@host> show multicast route
Family: INET

Group: 224.1.1.0/24
  Source: *
  Incoming interface list:
    lo0.0 ge-0/0/1.0
  Downstream interface list:
    ge-0/0/1.0

Group: 224.1.3.0/24
  Source: *
  Incoming interface list:
    lo0.0 ge-0/0/1.0 xe-4/1/0.0
  Downstream interface list:
    ge-0/0/1.0

Group: 225.1.1.0/24
  Source: *
  Incoming interface list:
    lo0.0 ge-0/0/1.0
  Downstream interface list:
    ge-0/0/1.0

Group: 225.1.3.0/24
  Source: *
  Incoming interface list:
    lo0.0 ge-0/0/1.0 xe-4/1/0.0
  Downstream interface list:
    ge-0/0/1.0
Family: INET6
```

**show multicast route brief**

The output for the *show multicast route brief* command is identical to that for the *show multicast route* command. For sample output, see *show multicast route on page 3475* or *show multicast route (Bidirectional PIM) on page 3476*.

**show multicast route detail**

```
user@host> show multicast route detail
Family: INET

Group: 228.0.0.0
  Source: 10.255.14.144/32
  Upstream interface: local
  Downstream interface list:
    so-1/0/0.0
  Session description: Unknown
  Statistics: 8 kbps, 100 pps, 45272 packets
  Next-hop ID: 262142
  Upstream protocol: PIM
```
show multicast route extensive (Bidirectional PIM)

user@host> show multicast route extensive
Family: INET

Group: 224.1.1.0/24
Source: *
   Incoming interface list:
     lo0.0 ge-0/0/1.0
   Downstream interface list:
     ge-0/0/1.0
   Number of outgoing interfaces: 1
   Session description: NOB Cross media facilities
   Statistics: 0 kbps, 0 pps, 0 packets
   Next-hop ID: 2097153
   Incoming interface list ID: 585
   Upstream protocol: PIM
   Route state: Active
   Forwarding state: Forwarding
   Cache lifetime/timeout: forever
   Wrong incoming interface notifications: 0

Group: 224.1.3.0/24
Source: *
   Incoming interface list:
     lo0.0 ge-0/0/1.0 xe-4/1/0.0
   Downstream interface list:
     ge-0/0/1.0
   Number of outgoing interfaces: 1
   Session description: NOB Cross media facilities
   Statistics: 0 kbps, 0 pps, 0 packets
   Next-hop ID: 2097153
   Incoming interface list ID: 589
   Upstream protocol: PIM
   Route state: Active
   Forwarding state: Forwarding
   Cache lifetime/timeout: forever
   Wrong incoming interface notifications: 0
Family: INET6

show multicast route instance <instance-name>

user@host> show multicast route instance v1 extensive
Instance: v1 Family: INET

Group: 224.1.1.1
Source: (null)/0
Upstream interface: fe-1/3/0.111
Downstream interface list:
  lt-0/3/0.42 lt-0/3/0.46 lt-0/3/0.43
Number of outgoing interfaces: 3

Group: 224.1.1.2
Source: (null)/0
Upstream interface: fe-1/3/0.111
Downstream interface list:
  lt-0/3/0.42 lt-0/3/0.46 lt-0/3/0.43
Number of outgoing interfaces: 3

Group: 224.1.1.3
Source: (null)/0
Upstream interface: fe-1/3/0.111
Downstream interface list:
  lt-0/3/0.42 lt-0/3/0.46 lt-0/3/0.43
Number of outgoing interfaces: 3

Instance: v1 Family: INET6

show multicast route summary

user@host> show multicast route summary
Instance: master Family: INET

<table>
<thead>
<tr>
<th>Route type</th>
<th>Route state</th>
<th>Route count</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S,G)</td>
<td>Active</td>
<td>2</td>
</tr>
<tr>
<td>(S,G)</td>
<td>Inactive</td>
<td>3</td>
</tr>
</tbody>
</table>

Instance: master Family: INET6
**show multicast rpf**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show multicast rpf &lt;inet</td>
<td>inet6&gt; &lt;instance instance-name&gt; &lt;logical-system (all</td>
</tr>
</tbody>
</table>

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Options**

none—Display RPF calculation information for all supported address families.

inet | inet6—(Optional) Display the RPF calculation information for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Display information about multicast RPF calculations for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

prefix—(Optional) Display the RPF calculation information for the specified prefix.

summary—(Optional) Display a summary of all multicast RPF information.

**Required Privilege**

view

**List of Sample Output**

- show multicast rpf on page 3480
- show multicast rpf inet6 on page 3481
- show multicast rpf prefix on page 3482
- show multicast rpf summary on page 3482
Output Fields  
Table 420 on page 3480 describes the output fields for the `show multicast rpf` command. Output fields are listed in the approximate order in which they appear.

### Table 420: show multicast rpf Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance. (Displayed when multicast is configured within a routing instance.)</td>
</tr>
<tr>
<td>Source prefix</td>
<td>Prefix and length of the source as it exists in the multicast forwarding table.</td>
</tr>
<tr>
<td>Protocol</td>
<td>How the route was learned.</td>
</tr>
<tr>
<td>Interface</td>
<td>Upstream RPF interface.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Upstream RPF neighbor.</td>
</tr>
</tbody>
</table>

**NOTE:** The displayed interface information does not apply to bidirectional PIM RP addresses. This is because the `show multicast rpf` command does not take into account equal-cost paths or the designated forwarder. For accurate upstream RPF interface information, always use the `show pim join extensive` command when bidirectional PIM is configured.

**NOTE:** The displayed neighbor information does not apply to bidirectional PIM. This is because the `show multicast rpf` command does not take into account equal-cost paths or the designated forwarder. For accurate upstream RPF neighbor information, always use the `show pim join extensive` command when bidirectional PIM is configured.

---

### Sample Output

show multicast rpf

```
user@host> show multicast rpf
Multicast RPF table: inet.0, 12 entries

0.0.0.0/0
  Protocol: Static

10.255.14.132/32
  Protocol: Direct
  Interface: lo0.0

10.255.245.91/32
  Protocol: IS-IS
  Interface: so-1/1/1.0
  Neighbor: 192.168.195.21

127.0.0.1/32
  Inactive
  Neighbor: 172.16.0.0/12
  Protocol: Static
  Interface: fxp0.0
```
192.168.0.0/16
Protocol: Static
Interface: fxp0.0
192.168.14.0/24
Protocol: Direct
Interface: fxp0.0
192.168.14.132/32
Protocol: Local
192.168.195.20/30
Protocol: Direct
Interface: so-1/1/1.0
192.168.195.22/32
Protocol: Local
192.168.195.36/30
Protocol: IS-IS
Interface: so-1/1/1.0
Neighbor: 192.168.195.21

show multicast rpf inet6

user@host> show multicast rpf inet6
Multicast RPF table: inet6.0, 12 entries
::10.255.14.132/128
   Protocol: Direct
   Interface: lo0.0

::10.255.245.91/128
   Protocol: IS-IS
   Interface: so-1/1/1.0
   Neighbor: fe80::2a0:a5ff:fe28:2e8c

::192.168.195.20/126
   Protocol: Direct
   Interface: so-1/1/1.0

::192.168.195.22/128
   Protocol: Local

::192.168.195.36/126
   Protocol: IS-IS
   Interface: so-1/1/1.0
   Neighbor: fe80::2a0:a5ff:fe28:2e8c

::192.168.195.76/126
   Protocol: Direct
   Interface: fe-2/2/0.0

::192.168.195.77/128
   Protocol: Local
```
fe80::/64
Protocol: Direct
Interface: so-1/1/1.0

fe80::290:69ff:fe0c:993a/128
Protocol: Local

fe80::2a0:a5ff:fe12:84f/128
Protocol: Direct
Interface: lo0.0

ff02::2/128
Protocol: PIM

ff02::d/128
Protocol: PIM

show multicast rpf prefix

user@host> show multicast rpf ff02::/16
Multicast RPF table: inet6.0, 13 entries

ff02::2/128
Protocol: PIM

ff02::d/128
Protocol: PIM

...

show multicast rpf summary

user@host> show multicast rpf summary
Multicast RPF table: inet.0, 16 entries
Multicast RPF table: inet6.0, 12 entries
```
show multicast scope

Syntax

show multicast scope
<inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)

show multicast scope
<inet | inet6>
<instance instance-name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display administratively scoped IP multicast information.

Options

none—Display standard information about administratively scoped multicast information for all supported address families in all routing instances.

inet | inet6—(Optional) Display scoped multicast information for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Display administratively scoped information for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

List of Sample Output

show multicast scope on page 3484
show multicast scope inet on page 3484
show multicast scope inet6 on page 3484

Output Fields

Table 421 on page 3483 describes the output fields for the show multicast scope command. Output fields are listed in the approximate order in which they appear.

Table 421: show multicast scope Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope name</td>
<td>Name of the multicast scope.</td>
</tr>
<tr>
<td>Group Prefix</td>
<td>Range of multicast groups that are scoped.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface that is the boundary of the administrative scope.</td>
</tr>
<tr>
<td>Resolve Rejects</td>
<td>Number of kernel resolve rejects.</td>
</tr>
</tbody>
</table>
## Sample Output

### show multicast scope

```
user@host> show multicast scope
Scope name | Group Prefix | Interface  | Rejects
---|---|---|---
232-net    | 232.232.0.0/16 | fe-0/0/0.1 | 0
local      | 239.255.0.0/16 | fe-0/0/0.1 | 0
local      | ff05::/16 | fe-0/0/0.1 | 0
larry      | ff05::1234/128 | fe-0/0/0.1 | 0
```

### show multicast scope inet

```
user@host> show multicast scope inet
Scope name | Group Prefix | Interface  | Rejects
---|---|---|---
232-net    | 232.232.0.0/16 | fe-0/0/0.1 | 0
local      | 239.255.0.0/16 | fe-0/0/0.1 | 0
```

### show multicast scope inet6

```
user@host> show multicast scope inet6
Scope name | Group Prefix | Interface  | Rejects
---|---|---|---
local      | ff05::/16 | fe-0/0/0.1 | 0
larry      | ff05::1234/128 | fe-0/0/0.1 | 0
```
show multicast sessions

**Syntax**

show multicast sessions

*briefer | detail | extensive>*

*<logical-system (all | logical-system-name)*>*  

*<regular-expression>*

**Syntax (EX Series Switch and the QFX Series)**

show multicast sessions

*briefer | detail | extensive>*  

*<regular-expression>*

**Release Information**

Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display information about announced IP multicast sessions.

**Options**

none—Display standard information about all multicast sessions for all routing instances.

*briefer | detail | extensive*—(Optional) Display the specified level of output.

*logical-system (all | logical-system-name)*—(Optional) Perform this operation on all logical systems or on a particular logical system.

*regular-expression*—(Optional) Display information about announced sessions that match a UNIX-style regular expression.

**Required Privilege Level**

view

**List of Sample Output**

show multicast sessions on page 3486
show multicast sessions regular-expression detail on page 3486

**Output Fields**

Table 422 on page 3485 describes the output fields for the show multicast sessions command. Output fields are listed in the approximate order in which they appear.

**Table 422: show multicast sessions Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session-name</td>
<td>Name of the known announced multicast sessions.</td>
</tr>
</tbody>
</table>
Sample Output

show multicast sessions

user@host> show multicast sessions
1-Department of Biological Sciences, LSU
... Monterey Bay - DockCam
Monterey Bay - JettyCam
Monterey Bay - StandCam
Monterey DockCam
Monterey DockCam / ROV cam
... NASA TV (MPEG-1)
... UO Broadcast - NASA Videos - 25 Years of Progress
UO Broadcast - NASA Videos - Journey through the Solar System
UO Broadcast - NASA Videos - Life in the Universe
UO Broadcasts OPB’s Oregon Story
UO DOD News Clips
UO Medical Management of Biological Casualties (1)
UO Medical Management of Biological Casualties (2)
UO Medical Management of Biological Casualties (3)
... 376 active sessions.

show multicast sessions regular-expression detail

user@host> show multicast sessions "NASA TV" detail
SDP Version: 0 Originated by: -0128.223.83.33
Session: NASA TV (MPEG-1)
Description: NASA television in MPEG-1 format, provided by Private University.
Please contact the UO if you have problems with this feed.
Email: Your Name Here <multicast@lists.private.edu>
Phone: Your Name Here <888/555-1212>
Bandwidth: AS:1000
Start time: permanent
Stop time: none
Attribute: type:broadcast
Attribute: tool:IP/TV Content Manager 3.4.14
Attribute: live:capture:1
Attribute: x-iptv-capture:mpls
Media: video 54302 RTP/AVP 32 31 96 97
Connection Data: 224.2.231.45 ttl 127
Attribute: quality:8
Attribute: framerate:30
Attribute: rtpmap:96 WBIH/90000
Attribute: rtpmap:97 MP4V-ES/90000
Attribute: x-iptv-svr:video 128.223.91.191 live
Attribute: fmtp:32 type=mpeg1
Media: audio 28848 RTP/AVP 14 0 96 3 5 97 98 99 100 101 102 10 11 103 104 105 106
Connection Data: 224.2.145.37 ttl 127
Attribute: rtpmap:96 X-WAVE/8000
Attribute: rtpmap:97 L8/8000/2
Attribute: rtpmap:98 L8/8000
Attribute: rtpmap:99 L8/22050/2
Attribute: rtpmap:100 L8/22050
Attribute: rtpmap:101 L8/11025/2
Attribute: rtpmap:102 L8/11025
Attribute: rtpmap:103 L16/22050/2
Attribute: rtpmap:104 L16/22050

1 matching sessions.
show multicast usage

Syntax

```
show multicast usage
  <brief | detail>
  <inet | inet6>
  <instance instance-name>
  <logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and the QFX Series)

```
show multicast usage
  <brief | detail>
  <inet | inet6>
  <instance instance-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

Display usage information about the 10 most active Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM) groups.

Options

none—Display multicast usage information for all supported address families for all routing instances.

brief | detail—(Optional) Display the specified level of output.

inet | inet6—(Optional) Display usage information for IPv4 or IPv6 family addresses, respectively.

instance instance-name—(Optional) Display information about the most active DVMRP or PIM groups for a specific multicast instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

List of Sample Output

```
show multicast usage on page 3489
show multicast usage brief on page 3489
show multicast usage instance on page 3489
show multicast usage detail on page 3490
```

Output Fields

Table 423 on page 3488 describes the output fields for the show multicast usage command. Output fields are listed in the approximate order in which they appear.

Table 423: show multicast usage Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance. (Displayed when multicast is configured within a routing instance.)</td>
</tr>
</tbody>
</table>
Table 423: show multicast usage Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Group address.</td>
</tr>
<tr>
<td>Sources</td>
<td>Number of sources.</td>
</tr>
<tr>
<td>Packets</td>
<td>Number of packets that have been forwarded to this prefix. If one or more of the packets forwarded statistic queries fails or times out, the packets field displays unavailable.</td>
</tr>
<tr>
<td>Bytes</td>
<td>Number of bytes that have been forwarded to this prefix. If one or more of the packets forwarded statistic queries fails or times out, the bytes field displays unavailable.</td>
</tr>
<tr>
<td>Prefix</td>
<td>IP address.</td>
</tr>
<tr>
<td>/len</td>
<td>Prefix length.</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of multicast groups.</td>
</tr>
</tbody>
</table>

Sample Output

show multicast usage

user@host> show multicast usage
Group           Sources Packets              Bytes
228.0.0.0       1       52847                4439148
239.1.1.1       2       13450                1125530

Prefix          /len Groups Packets              Bytes
10.255.14.144   /32  2      66254                5561304
10.255.70.15    /32  1      43                   3374...

show multicast usage brief

The output for the show multicast usage brief command is identical to that for the show multicast usage command. For sample output, see show multicast usage on page 3489.

show multicast usage instance

user@host> show multicast usage instance VPN-A
Group           Sources Packets              Bytes
224.0.1.40      1       13                   624
224.0.1.40      1       13                   624

Prefix          /len Groups Packets              Bytes
192.168.195.34  /32  1      5538                509496
10.255.14.30    /32  1      13                   624
...
### show multicast usage detail

```
show multicast usage detail

<table>
<thead>
<tr>
<th>Group</th>
<th>Sources</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.0.0.0</td>
<td>1</td>
<td>53159</td>
<td>4465356</td>
</tr>
<tr>
<td>239.1.1.1</td>
<td>2</td>
<td>13450</td>
<td>1125530</td>
</tr>
<tr>
<td>Source: 10.255.70.15    /32</td>
<td>Packets: 43 Bytes: 3374</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prefix</th>
<th>/len</th>
<th>Groups</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.14.144 /32</td>
<td>2</td>
<td>66566</td>
<td>5587512</td>
<td></td>
</tr>
<tr>
<td>Group: 228.0.0.0</td>
<td></td>
<td>Packets: 53159 Bytes: 4465356</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group: 239.1.1.1</td>
<td></td>
<td>Packets: 13407 Bytes: 1122156</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.255.70.15    /32</td>
<td>1</td>
<td>43</td>
<td>3374</td>
<td></td>
</tr>
<tr>
<td>Group: 239.1.1.1</td>
<td></td>
<td>Packets: 43 Bytes: 3374</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show pim bootstrap

Syntax

show pim bootstrap

<instance instance-name>

<logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)

show pim bootstrap

<instance instance-name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
instance option introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

Description

For sparse mode only, display information about Protocol Independent Multicast (PIM) bootstrap routers.

Options

none—Display PIM bootstrap router information for all routing instances.

instance instance-name—(Optional) Display information about bootstrap routers for a specific PIM-enabled routing instance.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

List of Sample Output

show pim bootstrap on page 3492
show pim bootstrap instance on page 3492

Output Fields

Table 424 on page 3491 describes the output fields for the show pim bootstrap command.
Output fields are listed in the approximate order in which they appear.

Table 424: show pim bootstrap Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>BSR</td>
<td>Bootstrap router.</td>
</tr>
<tr>
<td>Pri</td>
<td>Priority of the routing device as elected to be the bootstrap router.</td>
</tr>
<tr>
<td>Local address</td>
<td>Local routing device address.</td>
</tr>
<tr>
<td>Pri</td>
<td>Local routing device address priority to be elected as the bootstrap router.</td>
</tr>
<tr>
<td>State</td>
<td>Local routing device election state: Candidate, Elected, or Ineligible.</td>
</tr>
</tbody>
</table>
Table 424: show pim bootstrap Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>How long until the local routing device declares the bootstrap router to be unreachable, in seconds.</td>
</tr>
</tbody>
</table>

Sample Output

**show pim bootstrap**

```
user@host> show pim bootstrap
Instance: PIM.master

BSR Pri Local address Pri State Timeout
None 0 10.255.71.46 0 InEligible 0
feco:1:1:1:0:aff:785c 34 feco:1:1:1:0:aff:7c12 0 InEligible 0
```

**show pim bootstrap instance**

```
user@host> show pim bootstrap instance VPN-A
Instance: PIM.VPN-A

BSR Pri Local address Pri State Timeout
None 0 192.168.196.105 0 InEligible 0
```
show pim interfaces

Syntax

```
show pim interfaces
  <inet | inet6>
  <instance (instance-name | all)>
  <logical-system (all | logical-system-name)>
```

Syntax (EX Series Switch and the QFX Series)

```
show pim interfaces
  <inet | inet6>
  <instance (instance-name | all)>
```

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Support for bidirectional PIM added in Junos OS Release 12.1.
- Support for the `instance all` option added in Junos OS Release 12.1.

Description

Display information about the interfaces on which Protocol Independent Multicast (PIM) is configured.

Options

- `none`—Display interface information for all family addresses for the main instance.
- `inet | inet6`—(Optional) Display interface information for IPv4 or IPv6 family addresses, respectively.
- `instance (instance-name | all)`—(Optional) Display information about interfaces for a specific PIM-enabled routing instance or for all routing instances.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

`view`

List of Sample Output

```
show pim interfaces on page 3494
```

Output Fields

Table 425 on page 3493 describes the output fields for the `show pim interfaces` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>Name</td>
<td>Interface name.</td>
</tr>
<tr>
<td>State</td>
<td>State of the interface. The state also is displayed in the <code>show interfaces</code> command.</td>
</tr>
</tbody>
</table>
Table 425: show pim interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>PIM mode running on the interface:</td>
</tr>
<tr>
<td></td>
<td>• B—In bidirectional mode, multicast groups are carried across the network over bidirectional shared trees. This type of tree minimizes PIM routing state, which is especially important in networks with numerous and dispersed senders and receivers.</td>
</tr>
<tr>
<td></td>
<td>• S—In sparse mode, routing devices must join and leave multicast groups explicitly. Upstream routing devices do not forward multicast traffic to this routing device unless this device has sent an explicit request (using a join message) to receive multicast traffic.</td>
</tr>
<tr>
<td></td>
<td>• Dense—Unlike sparse mode, where data is forwarded only to routing devices sending an explicit request, dense mode implements a flood-and-prune mechanism, similar to DVMRP (the first multicast protocol used to support the multicast backbone). (Not supported on QFX Series.)</td>
</tr>
<tr>
<td></td>
<td>• Sparse-Dense—Sparse-dense mode allows the interface to operate on a per-group basis in either sparse or dense mode. A group specified as dense is not mapped to a rendezvous point (RP). Instead, data packets destined for that group are forwarded using PIM-Dense Mode (PIM-DM) rules. A group specified as sparse is mapped to an RP, and data packets are forwarded using PIM-Sparse Mode (PIM-SM) rules. (Not supported on QFX Series.)</td>
</tr>
<tr>
<td></td>
<td>When sparse-dense mode is configured, the output includes both S and D. When bidirectional-sparse mode is configured, the output includes S and B. When bidirectional-sparse-dense mode is configured, the output includes B, S, and D.</td>
</tr>
<tr>
<td>IP</td>
<td>Version number of the address family on the interface: 4 (IPv4) or 6 (IPv6).</td>
</tr>
<tr>
<td>V</td>
<td>PIM version running on the interface: 1 or 2.</td>
</tr>
<tr>
<td>State</td>
<td>State of PIM on the interface:</td>
</tr>
<tr>
<td></td>
<td>• Active—Bidirectional mode is enabled on the interface and on all PIM neighbors.</td>
</tr>
<tr>
<td></td>
<td>• DR—Designated router.</td>
</tr>
<tr>
<td></td>
<td>• NotCap—Bidirectional mode is not enabled on the interface. This can happen when bidirectional PIM is not configured locally, when one of the neighbors is not configured for bidirectional PIM, or when one of the neighbors has not implemented the bidirectional PIM protocol.</td>
</tr>
<tr>
<td></td>
<td>• NotDR—Not the designated router.</td>
</tr>
<tr>
<td></td>
<td>• P2P—Point to point.</td>
</tr>
<tr>
<td>NbrCnt</td>
<td>Number of neighbors that have been seen on the interface.</td>
</tr>
<tr>
<td>JoinCnt(sg)</td>
<td>Number of (s,g) join messages that have been seen on the interface.</td>
</tr>
<tr>
<td>JointCnt(*g)</td>
<td>Number of (*g) join messages that have been seen on the interface.</td>
</tr>
<tr>
<td>DR address</td>
<td>Address of the designated router.</td>
</tr>
</tbody>
</table>

Sample Output

```
show pim interfaces
```

user@host> show pim interfaces

Stat = Status, V = Version, NbrCnt = Neighbor Count,
S = Sparse, D = Dense, B = Bidirectional,
DR = Designated Router, P2P = Point-to-point link,
**Active = Bidirectional is active, NotCap = Not Bidirectional Capable**

<table>
<thead>
<tr>
<th>Name</th>
<th>Stat</th>
<th>Mode</th>
<th>IP V</th>
<th>State</th>
<th>NbrCnt</th>
<th>JoinCnt (sg/*g)</th>
<th>DR address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/3/0.0</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2 NotDR,NotCap</td>
<td>1</td>
<td>0/0</td>
<td>40.0.0.3</td>
</tr>
<tr>
<td>ge-0/3/3.50</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2 DR,NotCap</td>
<td>1</td>
<td>9901/100</td>
<td>50.0.0.2</td>
</tr>
<tr>
<td>ge-0/3/3.51</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2 DR,NotCap</td>
<td>1</td>
<td>0/0</td>
<td>51.0.0.2</td>
</tr>
<tr>
<td>pe-1/2/0.32769</td>
<td>Up</td>
<td>S</td>
<td>4</td>
<td>2 P2P,NotCap</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
</tbody>
</table>
show pim join

Syntax

show pim join
<brief | detail | extensive | summary>
<bidirectional | dense | sparse>
<exact>
/inet | inet6>
<instance instance-name>
<logical-system (all | logical-system-name)>
<range>
<rp ip-address/prefix | source ip-address/prefix>
<sg | star-g>

Syntax (EX Series Switch and the QFX Series)

show pim join
<brief | detail | extensive | summary>
<dense | sparse>
<exact>
/inet | inet6>
<instance instance-name>
<range>
<rp ip-address/prefix | source ip-address/prefix>
<sg | star-g>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
summary option introduced in Junos OS Release 9.6.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Support for bidirectional PIM added in Junos OS Release 12.1.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Multiple new filter options introduced in Junos OS Release 13.2.

Description

Display information about Protocol Independent Multicast (PIM) groups for all PIM modes.

For bidirectional PIM, display information about PIM group ranges (*G-range) for each active bidirectional RP group range, in addition to each of the joined (*G) routes.

Options

none—Display the standard information about PIM groups for all supported family addresses for all routing instances.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

bidirectional | dense | sparse—(Optional) Display information about PIM bidirectional mode, dense mode, or sparse and source-specific multicast (SSM) mode entries.

exact—(Optional) Display information about only the group that exactly matches the specified group address.

inet | inet6—(Optional) Display PIM group information for IPv4 or IPv6 family addresses, respectively.
instance instance-name—(Optional) Display information about groups for the specified PIM-enabled routing instance only.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

range—(Optional) Address range of the group, specified as prefix/prefix-length.

rp ip-address/prefix | source ip-address/prefix—(Optional) Display information about the PIM entries with a specified rendezvous point (RP) address and prefix or with a specified source address and prefix. You can omit the prefix.

sg | star-g—(Optional) Display information about PIM (S,G) or (*,G) entries.

Required Privilege Level
view

Related Documentation
• clear pim join on page 3425

List of Sample Output
show pim join summary on page 3501
show pim join (PIM Sparse Mode) on page 3501
show pim join (Bidirectional PIM) on page 3501
show pim join inet6 on page 3502
show pim join inet6 star-g on page 3502
show pim join instance <instance-name> on page 3502
show pim join detail on page 3503
show pim join extensive (PIM Sparse Mode) on page 3503
show pim join extensive (Bidirectional PIM) on page 3504
show pim join extensive (Bidirectional PIM with a Directly Connected Phantom RP) on page 3505
show pim join instance <instance-name> extensive on page 3506
show pim join extensive (Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 3506
show pim join extensive (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 3507

Output Fields
Table 426 on page 3497 describes the output fields for the show pim join command. Output fields are listed in the approximate order in which they appear.

Table 426: show pim join Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
<td>brief detail extensive summary none</td>
</tr>
<tr>
<td>Family</td>
<td>Name of the address family: inet (IPv4) or inet6 (IPv6).</td>
<td>brief detail extensive summary none</td>
</tr>
<tr>
<td>Route type</td>
<td>Type of multicast route: (S,G) or (*,G).</td>
<td>summary</td>
</tr>
<tr>
<td>Route count</td>
<td>Number of (S,G) routes and number of (*,G) routes.</td>
<td>summary</td>
</tr>
</tbody>
</table>
Table 426: show pim join Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>Rendezvous Point Tree.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>S</td>
<td>Sparse.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>W</td>
<td>Wildcard.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Group</td>
<td>Group address.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Bidirectional group prefix length</td>
<td>For bidirectional PIM, length of the IP prefix for RP group ranges.</td>
<td>All levels</td>
</tr>
<tr>
<td>Source</td>
<td>Multicast source:</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• * (wildcard value)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ipv4-address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ipv6-address</td>
<td></td>
</tr>
<tr>
<td>RP</td>
<td>Rendezvous point for the PIM group.</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td>Flags</td>
<td>PIM flags:</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>• bidirectional—Bidirectional mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• dense—Dense mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rptree—Entry is on the rendezvous point tree.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• sparse—Sparse mode entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• spt—Entry is on the shortest-path tree for the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• wildcard—Entry is on the shared tree.</td>
<td></td>
</tr>
<tr>
<td>Upstream interface</td>
<td>RPF interface toward the source address for the source-specific state (S,G) or toward the rendezvous point (RP) address for the non-source-specific state (*G).</td>
<td>brief detail extensive none</td>
</tr>
<tr>
<td></td>
<td>For bidirectional PIM, <strong>RP Link</strong> means that the interface is directly connected to a subnet that contains a phantom RP address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A pseudo multipoint LDP (M-LDP) interface appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 426: show pim join Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upstream neighbor</strong></td>
<td>Information about the upstream neighbor: Direct, Local, Unknown, or a specific IP address. For bidirectional PIM, Direct means that the interface is directly connected to a subnet that contains a phantom RP address. The multipoint LDP (M-LDP) root appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Upstream state</strong></td>
<td>Information about the upstream interface:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>- <strong>Join to RP</strong>—Sending a join to the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Join to Source</strong>—Sending a join to the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Local RP</strong>—Sending neither join messages nor prune messages toward the RP, because this routing device is the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Local Source</strong>—Sending neither join messages nor prune messages toward the source, because the source is locally attached to this routing device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Prune to RP</strong>—Sending a prune to the rendezvous point.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Prune to Source</strong>—Sending a prune to the source.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** RP group range entries have **None** in the **Upstream state** field because RP group ranges do not trigger actual PIM join messages between routing devices.
### Table 426: show pim join Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Downstream neighbors</strong></td>
<td>Information about downstream interfaces:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Interface—Interface name for the downstream neighbor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A pseudo PIM-SM interface appears for all IGMP-only interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A pseudo multipoint LDP (M-LDP) interface appears on ingress root nodes in M-LDP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>point-to-multipoint LSPs with inband signaling.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interface address—Address of the downstream neighbor.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• State—Information about the downstream neighbor: join or prune.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Flags—PIM join flags: R (RPtree), S (Sparse), W (Wildcard), or zero.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Uptime—Time since the downstream interface joined the group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Time since last Join—Time since the last join message was received from the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>downstream interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Time since last Prune—Time since the last prune message was received from the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>downstream interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Number of downstream interfaces</strong></td>
<td>Total number of outgoing interfaces for each (S,G) entry.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Assert Timeout</strong></td>
<td>Length of time between assert cycles on the downstream interface. Not displayed</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>if the assert timer is null.</td>
<td></td>
</tr>
<tr>
<td><strong>Keepalive timeout</strong></td>
<td>Time remaining until the downstream join state is updated (in seconds). If the</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>downstream join state is not updated before this keepalive timer reaches zero,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the entry is deleted. If there is a directly connected host, <strong>Keepalive timeout</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is Infinity.</td>
<td></td>
</tr>
<tr>
<td><strong>Uptime</strong></td>
<td>Time since the creation of (S,G) or (*,G) state. The uptime is not refreshed</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>every time a PIM join message is received for an existing (S,G) or (*,G) state.</td>
<td></td>
</tr>
<tr>
<td>**Bidirectional accepting</td>
<td>Interfaces on the routing device that forward bidirectional PIM traffic.</td>
<td>extensive</td>
</tr>
<tr>
<td>interfaces**</td>
<td>The reasons for forwarding bidirectional PIM traffic are that the interface is the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>winner of the designated forwarder election (DF Winner), or the interface is the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reverse path forwarding (RPF) interface toward the RP (RPF).</td>
<td></td>
</tr>
</tbody>
</table>
Sample Output

show pim join summary

```
user@host> show pim join summary
Instance: PIM.master Family: INET

Route type         Route count
(s,g)                2
(*,g)                1

Instance: PIM.master Family: INET6
```

show pim join (PIM Sparse Mode)

```
user@host> show pim join
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
  Source: *
  RP: 10.255.14.144
  Flags: sparse,rptree,wildcard
  Upstream interface: Local

Group: 239.1.1.1
  Source: 10.255.14.144
  Flags: sparse,spt
  Upstream interface: Local

Group: 239.1.1.1
  Source: 10.255.70.15
  Flags: sparse,spt
  Upstream interface: so-1/0/0.0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard
```

show pim join (Bidirectional PIM)

```
user@host> show pim join
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 224.1.1.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.13.2
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0

Group: 224.1.3.0
  Bidirectional group prefix length: 24
  Source: *
  RP: 10.10.1.3
  Flags: bidirectional,rptree,wildcard
  Upstream interface: ge-0/0/1.0 (RP Link)

Group: 225.1.1.0
  Bidirectional group prefix length: 24
  Source: *
```
RP: 10.10.13.2
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0

Group: 225.1.3.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join inet6

user@host> show pim join inet6
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: ff04::e000:101
Source: *
RP: ::46.0.0.13
Flags: sparse,rptree,wildcard
Upstream interface: Local

Group: ff04::e000:101
Source: ::1.1.1.1
Flags: sparse
Upstream interface: unknown (no neighbor)

Group: ff04::e800:101
Source: ::1.1.1.1
Flags: sparse
Upstream interface: unknown (no neighbor)

Group: ff04::e800:101
Source: ::1.1.1.2
Flags: sparse
Upstream interface: unknown (no neighbor)

show pim join inet6 star-g

user@host> show pim join inet6 star-g
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: ff04::e000:101
Source: *
RP: ::46.0.0.13
Flags: sparse,rptree,wildcard
Upstream interface: Local

show pim join instance <instance-name>

user@host> show pim join instance VPN-A
Instance: PIM.VPN-A Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 235.1.1.2
Source: *
RP: 10.10.47.100
Flags: sparse,rptree,wildcard
Upstream interface: Local

Group: 235.1.1.2
Source: 192.168.195.74
Flags: sparse,spt
Upstream interface: at-0/3/1.0

Group: 235.1.1.2
Source: 192.168.195.169
Flags: sparse
Upstream interface: so-1/0/1.0

Instance: PIM.VPN-A Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join detail

user@host> show pim join detail
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
Source: *
RP: 10.255.14.144
Flags: sparse,rptree,wildcard
Upstream interface: Local

Group: 239.1.1.1
Source: 10.255.14.144
Flags: sparse,spt
Upstream interface: Local

Group: 239.1.1.1
Source: 10.255.70.15
Flags: sparse,spt
Upstream interface: so-1/0/0.0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join extensive (PIM Sparse Mode)

user@host> show pim join extensive
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 239.1.1.1
Source: *
RP: 10.255.14.144
Flags: sparse,rptree,wildcard
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local RP
Uptime: 00:03:49
Downstream neighbors:
  Interface: so-1/0/0.0
    10.111.10.2 State: Join Flags: SRW Timeout: 174
    Uptime: 00:03:49 Time since last Join: 00:01:49
    Interface: mt-1/1/0.32768
    10.10.47.100 State: Join Flags: SRW Timeout: Infinity
show pim join extensive (Bidirectional PIM)

user@host> show pim join extensive
Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 224.1.1.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.13.2
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0
Upstream neighbor: 10.10.1.2
Upstream state: None
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0 (RPF)
  Interface: lo0.0 (DF Winner)
Number of downstream interfaces: 0
Group: 225.1.1.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.13.2
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0
Upstream neighbor: 10.10.1.2
Upstream state: None
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0     (RPF)
  Interface: lo0.0          (DF Winner)
Downstream neighbors:
  Interface: lt-1/0/10.24
    10.0.24.4 State: Join   RW Timeout: 185
  Interface: lt-1/0/10.23
    10.0.23.3 State: Join   RW Timeout: 184
Number of downstream interfaces: 2

Group: 225.1.3.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)
Upstream neighbor: Direct
Upstream state: Local RP
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0     (RPF)
  Interface: lo0.0          (DF Winner)
  Interface: xe-4/1/0.0     (DF Winner)
Number of downstream interfaces: 0

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

show pim join extensive (Bidirectional PIM with a Directly Connected Phantom RP)

user@host> show pim join extensive
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 224.1.3.0
Bidirectional group prefix length: 24
Source: *
RP: 10.10.1.3
Flags: bidirectional,rptree,wildcard
Upstream interface: ge-0/0/1.0 (RP Link)
Upstream neighbor: Direct
Upstream state: Local RP
Uptime: 00:03:49
Bidirectional accepting interfaces:
  Interface: ge-0/0/1.0     (RPF)
  Interface: lo0.0          (DF Winner)
  Interface: xe-4/1/0.0     (DF Winner)
Number of downstream interfaces: 0
show pim join instance <instance-name> extensive

```
user@host> show pim join instance VPN-A extensive
Instance: PIM.VPN-A Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 235.1.1.2
Source: *
  RP: 10.10.47.100
  Flags: sparse,rptree,wildcard
  Upstream interface: Local
  Upstream neighbor: Local
  Upstream state: Local RP
  Uptime: 00:03:49
  Downstream neighbors:
    Interface: mt-1/1/0.32768
    10.10.47.101 State: Join Flags: SRW Timeout: 156
    Uptime: 00:03:49 Time since last Join: 00:01:49
  Number of downstream interfaces: 1

Group: 235.1.1.2
Source: 192.168.195.74
  Flags: sparse,spt
  Upstream interface: at-0/3/1.0
  Upstream neighbor: 10.111.30.2
  Upstream state: Local RP, Join to Source
  Keepalive timeout: 156
  Uptime: 00:14:52

Group: 235.1.1.2
Source: 192.168.195.169
  Flags: sparse
  Upstream interface: so-1/0/1.0
  Upstream neighbor: 10.111.20.2
  Upstream state: Local RP, Join to Source
  Keepalive timeout: 156
  Uptime: 00:14:52
```

show pim join extensive (Ingress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

```
user@host> show pim join extensive
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 232.1.1.1
Source: 192.168.219.11
  Flags: sparse,spt
  Upstream interface: fe-1/3/1.0
  Upstream neighbor: Direct
  Upstream state: Local Source
  Keepalive timeout:
  Uptime: 11:27:55
  Downstream neighbors:
    Interface: Pseudo-MLDP
    Interface: lt-1/2/0.25
      1.2.5.2 State: Join Flags: S Timeout: Infinity

Group: 232.1.1.2
Source: 192.168.219.11
  Flags: sparse,spt
```
show pim join extensive (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show pim join extensive
Instance: PIM.master Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 227.1.1.1
Source: *
RP: 1.1.1.1
Flags: sparse,rptree,wildcard
Upstream interface: Local
Upstream neighbor: Local
Upstream state: Local RP
Uptime: 11:31:33
Downstream neighbors:
  Interface: fe-1/3/0.0
    192.168.209.9 State: Join Flags: SRW Timeout: Infinity
Uptime: 11:31:33 Time since last Join: 11:31:32

Group: 232.1.1.1
Source: 192.168.219.11
Flags: sparse,spt
Upstream protocol: MLDP
Upstream interface: Pseudo MLDP
Upstream neighbor: MLDP LSP root <1.1.1.2>
Upstream state: Join to Source
Keepalive timeout:
Uptime: 11:31:32
Downstream neighbors:
  Interface: so-0/1/3.0
    192.168.92.9 State: Join Flags: S Timeout: Infinity
    Uptime: 11:31:30 Time since last Join: 11:31:30
Downstream neighbors:
  Interface: fe-1/3/0.0
    192.168.209.9 State: Join Flags: S Timeout: Infinity
    Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 232.1.1.2
Source: 192.168.219.11
Flags: sparse,spt
Upstream protocol: MLDP
Upstream interface: Pseudo MLDP
Upstream neighbor: MLDP LSP root <1.1.1.2>
Upstream state: Join to Source
Keepalive timeout:
Uptime: 11:31:32
Downstream neighbors:
  Interface: so-0/1/3.0
    192.168.92.9 State: Join Flags: S Timeout: Infinity
    Uptime: 11:31:30 Time since last Join: 11:31:30
Downstream neighbors:
  Interface: lt-1/2/0.14
    1.1.4.4 State: Join Flags: S Timeout: 177
    Uptime: 11:30:33 Time since last Join: 00:00:33
Downstream neighbors:
  Interface: fe-1/3/0.0
    192.168.209.9 State: Join Flags: S Timeout: Infinity
    Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 232.1.1.3
Source: 192.168.219.11
Flags: sparse,spt
Upstream protocol: MLDP
Upstream interface: Pseudo MLDP
Upstream neighbor: MLDP LSP root <1.1.1.2>
Upstream state: Join to Source
Keepalive timeout:
Uptime: 11:31:32
Downstream neighbors:
  Interface: fe-1/3/0.0
    192.168.209.9 State: Join Flags: S Timeout: Infinity
    Uptime: 11:31:32 Time since last Join: 11:31:32

Group: 232.2.2.2
Source: 1.2.7.7
Flags: sparse,spt
Upstream protocol: MLDP
Upstream interface: Pseudo MLDP
Upstream neighbor: MLDP LSP root <1.1.1.2>
Upstream state: Join to Source
Keepalive timeout:
Uptime: 11:31:30
Downstream neighbors:
  Interface: so-0/1/3.0
    192.168.92.9 State: Join Flags: S Timeout: Infinity
    Uptime: 11:31:30 Time since last Join: 11:31:30

Instance: PIM.master Family: INET6
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: ff3e::1:2
  Source: abcd::1:2:7:7
  Flags: sparse.spt
  Upstream protocol: MLDP
  Upstream interface: Pseudo MLDP
  Upstream neighbor: MLDP LSP root <1.1.1.2>
  Upstream state: Join to Source
  Keepalive timeout:
  Uptime: 11:31:32

Downstream neighbors:
  Interface: fe-1/3/0.0
    fe80::21f:12ff:fea5:c4db State: Join Flags: S Timeout: Infinity
    Uptime: 11:31:32 Time since last Join: 11:31:32
show pim neighbors

Syntax

show pim neighbors
  <brief | detail>
  <inet | inet6>
  <instance (instance-name | all)>
  <logical-system (all | logical-system-name)>

Syntax (EX Series Switch and the QFX Series)

show pim neighbors
  <brief | detail>
  <inet | inet6>
  <instance (instance-name | all)>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
inet6 and instance options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.
Support for the instance all option added in Junos OS Release 12.1.

Description

Display information about Protocol Independent Multicast (PIM) neighbors.

Options

none—(Same as brief) Display standard information about PIM neighbors for all supported family addresses for the main instance.

brief | detail—(Optional) Display the specified level of output.

inet | inet6—(Optional) Display information about PIM neighbors for IPv4 or IPv6 family addresses, respectively.

instance (instance-name | all)—(Optional) Display information about neighbors for the specified PIM-enabled routing instance or for all routing instances.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

List of Sample Output

show pim neighbors on page 3512
show pim neighbors brief on page 3512
show pim neighbors instance on page 3512
show pim neighbors detail on page 3512
show pim neighbors detail (With BFD) on page 3513

Output Fields

Table 427 on page 3511 describes the output fields for the show pim neighbors command. Output fields are listed in the approximate order in which they appear.
### Table 427: show pim neighbors Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the neighbor is reachable.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbor addr</td>
<td>Address of the neighboring PIM routing device.</td>
<td>All levels</td>
</tr>
<tr>
<td>IP</td>
<td>IP version: 4 or 6.</td>
<td>All levels</td>
</tr>
<tr>
<td>V</td>
<td>PIM version running on the neighbor: 1 or 2.</td>
<td>All levels</td>
</tr>
<tr>
<td>Mode</td>
<td>PIM mode of the neighbor: Sparse, Dense, SparseDense, or Unknown. When the neighbor is running PIM version 2, this mode is always Unknown.</td>
<td>All levels</td>
</tr>
<tr>
<td>Option</td>
<td>Can be one or more of the following:</td>
<td>brief none</td>
</tr>
<tr>
<td></td>
<td>• B—Bidirectional Capable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• H—Hello Option Holdtime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• G—Generation Identifier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• P—Hello Option DR Priority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• L—Hello Option LAN Prune Delay.</td>
<td></td>
</tr>
<tr>
<td>Uptime</td>
<td>Time the neighbor has been operational since the PIM process was last initialized, in the format $dd:hh:mm:ss$ ago for less than a week and $nwnd:hh:mm:ss$ ago for more than a week.</td>
<td>All levels</td>
</tr>
<tr>
<td>Address</td>
<td>Address of the neighboring PIM routing device.</td>
<td>detail</td>
</tr>
<tr>
<td>BFD</td>
<td>Status and operational state of the Bidirectional Forwarding Detection (BFD) protocol on the interface: Enabled, Operational state is up, or Disabled.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option Holdtime</td>
<td>Time for which the neighbor is available, in seconds. The range of values is 0 through 65,535.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Default Holdtime</td>
<td>Default holdtime and the time remaining if the holdtime option is not in the received hello message.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option DR Priority</td>
<td>Designated router election priority. The range of values is 0 through 255.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option Generation ID</td>
<td>9-digit or 10-digit number used to tag hello messages.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option Bi-Directional PIM supported</td>
<td>Neighbor can process bidirectional PIM messages.</td>
<td>detail</td>
</tr>
<tr>
<td>Hello Option LAN Prune Delay</td>
<td>Time to wait before the neighbor receives prune messages, in the format delay $nnn$ ms override $nnn$ ms.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 427: show pim neighbors Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Suppression supported</td>
<td>Neighbor is capable of join suppression.</td>
<td>detail</td>
</tr>
<tr>
<td>Rx Join</td>
<td>Information about joins received from the neighbor.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Group—Group addresses in the join message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Source—Address of the source in the join message.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Timeout—Time for which the join is valid.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show pim neighbors

```
user@host> show pim neighbors
Instance: PIM.master
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority

Interface           IP V Mode     Option      Uptime Neighbor addr
so-1/0/0.0           4 2             HPLG      00:07:10 10.111.10.2
```

show pim neighbors brief

The output for the `show pim neighbors brief` command is identical to that for the `show pim neighbors` command. For sample output, see `show pim neighbors on page 3512`.

show pim neighbors instance

```
user@host> show pim neighbors instance VPN-A
Instance: PIM.VPN-A
B = Bidirectional Capable, G = Generation Identifier,
H = Hello Option Holdtime, L = Hello Option LAN Prune Delay,
P = Hello Option DR Priority

Interface           IP V Mode     Option      Uptime Neighbor addr
at-0/3/1.0           4 2             HPLG      00:07:54 10.111.30.2
mt-1/1/0.32768       4 2             HPLG      00:07:22 10.10.47.101
so-1/0/1.0           4 2             HPLG      00:07:50 10.111.20.2
```

show pim neighbors detail

```
user@host> show pim neighbors detail
Instance: PIM.master
Interface: ge-0/0/1.0

Address: 10.10.1.1, IPv4, PIM v2, Mode: SparseDense, sg Join Count: 0, tsg Join Count: 2
Hello Option Holdtime: 65535 seconds
Hello Option DR Priority: 1
Hello Option Generation ID: 2053759302
Hello Option Bi-Directional PIM supported
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported
```
Address: 10.10.1.2, IPv4, PIM v2, sg Join Count: 0, tsg Join Count: 2
BFD: Disabled
Hello Option Holdtime: 105 seconds 93 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 1734018161
Hello Option Bi-Directional PIM supported
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported

Interface: lo0.0

Address: 10.255.179.246, IPv4, PIM v2, Mode: SparseDense, sg Join Count: 0, tsg Join Count: 0
Hello Option Holdtime: 65535 seconds
Hello Option DR Priority: 1
Hello Option Generation ID: 1997462267
Hello Option Bi-Directional PIM supported
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
Join Suppression supported

show pim neighbors detail (With BFD)

user@host> show pim neighbors detail
Instance: PIM.master
Interface: fe-1/0/0.0
Address: 192.168.11.1, IPv4, PIM v2, Mode: Sparse
Hello Option Holdtime: 65535 seconds
Hello Option DR Priority: 1
Hello Option Generation ID: 836607909
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms

Address: 192.168.11.2, IPv4, PIM v2
BFD: Enabled, Operational state is up
Hello Default Holdtime: 105 seconds 104 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 1907549685
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms

Interface: fe-1/0/1.0
Address: 192.168.12.1, IPv4, PIM v2
BFD: Disabled
Hello Default Holdtime: 105 seconds 80 remaining
Hello Option DR Priority: 1
Hello Option Generation ID: 1971554705
Hello Option LAN Prune Delay: delay 500 ms override 2000 ms
**show pim rps**

**Syntax**
```
show pim rps
<brief | detail | extensive>
<group-address>
/inet | inet6>
<instance instance-name>
/logical-system (all | logical-system-name)>
```

**Syntax (EX Series Switch and the QFX Series)**
```
show pim rps
<brief | detail | extensive>
<group-address>
/inet | inet6>
<instance instance-name>
```

**Release Information**
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.
Support for bidirectional PIM added in Junos OS Release 12.1.

**Description**
Display information about Protocol Independent Multicast (PIM) rendezvous points (RPs).

**Options**

- **none**—Display standard information about PIM RPs for all groups and family addresses for all routing instances.

- **brief | detail | extensive**—(Optional) Display the specified level of output.

- **group-address**—(Optional) Display the RPs for a particular group. If you specify a group address, the output lists the routing device that is the RP for that group.

- **inet | inet6**—(Optional) Display information for IPv4 or IPv6 family addresses, respectively.

- **instance instance-name**—(Optional) Display information about RPs for a specific PIM-enabled routing instance.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**
`view`

**Related Documentation**
- Example: Configuring Bidirectional PIM

**List of Sample Output**
- `show pim rps` on page 3517
- `show pim rps brief` on page 3517
- `show pim rps <group-address> (Bidirectional PIM)` on page 3517
- `show pim rps <group-address> (PIM Dense Mode)` on page 3517
Table 428: show pim rps Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Family or Address family</td>
<td>Name of the address family: inet (IPv4) or inet6 (IPv6).</td>
<td>All levels</td>
</tr>
<tr>
<td>RP address</td>
<td>Address of the rendezvous point.</td>
<td>All levels</td>
</tr>
<tr>
<td>Type</td>
<td>Type of RP:</td>
<td>brief</td>
</tr>
<tr>
<td></td>
<td>• auto-rp—Address of the RP known through the Auto-RP protocol.</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>• bootstrap—Address of the RP known through the bootstrap router protocol (BSR).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• embedded—Address of the RP known through an embedded RP (IPv6).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• static—Address of RP known through static configuration.</td>
<td></td>
</tr>
<tr>
<td>Holdtime</td>
<td>How long to keep the RP active, with time remaining, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Timeout</td>
<td>How long until the local routing device determines the RP to be unreachable,</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>in seconds.</td>
<td></td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups currently using this RP.</td>
<td>All levels</td>
</tr>
<tr>
<td>Group prefixes</td>
<td>Addresses of groups that this RP can span.</td>
<td>brief</td>
</tr>
<tr>
<td>Learned via</td>
<td>Address and method by which the RP was learned.</td>
<td>detailed</td>
</tr>
<tr>
<td>Mode</td>
<td>The PIM mode of the RP: bidirectional or sparse.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>If a sparse and bidirectional RPs are configured with the same RP address, they</td>
<td></td>
</tr>
<tr>
<td></td>
<td>appear as separate entries in both formats.</td>
<td></td>
</tr>
<tr>
<td>Time Active</td>
<td>How long the RP has been active, in the format hh:mm:ss.</td>
<td>detailed</td>
</tr>
</tbody>
</table>
### Table 428: show pim rps Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Index</strong></td>
<td>Index value of the order in which Junos OS finds and initializes the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>For bidirectional RPs, the <strong>Device Index</strong> output field is omitted because</td>
<td></td>
</tr>
<tr>
<td></td>
<td>bidirectional RPs do not require encapsulation and de-encapsulation interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Subunit</strong></td>
<td>Logical unit number of the interface.</td>
<td>detail extensive</td>
</tr>
<tr>
<td></td>
<td>For bidirectional RPs, the <strong>Subunit</strong> output field is omitted because bidirectional</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RPs do not require encapsulation and de-encapsulation interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>Either the encapsulation or the de-encapsulation logical interface, depending on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>whether this routing device is a designated router (DR) facing an RP router, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is the local RP, respectively. For bidirectional RPs, the <strong>Interface</strong> output field</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is omitted because bidirectional RPs do not require encapsulation and de-encapsulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Group Ranges</strong></td>
<td>Addresses of groups that this RP spans.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Active groups using RP</strong></td>
<td>Number of groups currently using this RP.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>total</strong></td>
<td>Total number of active groups for this RP.</td>
<td>detail extensive</td>
</tr>
<tr>
<td><strong>Register State for RP</strong></td>
<td>Current register state for each group:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• <strong>Group</strong>—Multicast group address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Source</strong>—Multicast source address for which the PIM register is sent or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>received, depending on whether this router is a designated router facing an RP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>router, or is the local RP, respectively.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>First Hop</strong>—PIM-designated routing device that sent the Register message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(the source address in the IP header).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>RP Address</strong>—RP to which the Register message was sent (the destination</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address in the IP header).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>State</strong>:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>On the designated router:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Send</strong>—Sending Register messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Probe</strong>—Sent a null register. If a Register-Stop message does not arrive in 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>seconds, the designated router resumes sending Register messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Suppress</strong>—Received a Register-Stop message. The designated router is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>waiting for the timer to resume before changing to <strong>Probe</strong> state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• On the RP:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Receive</strong>—Receiving Register messages.</td>
<td></td>
</tr>
<tr>
<td><strong>Anycast-PIM rpset</strong></td>
<td>If anycast RP is configured, the addresses of the RPs in the set.</td>
<td>extensive</td>
</tr>
<tr>
<td><strong>Anycast-PIM local address used</strong></td>
<td>If anycast RP is configured, the local address used by the RP.</td>
<td>extensive</td>
</tr>
</tbody>
</table>
Table 428: show pim rps Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anycast-PIM Register State</td>
<td>If anycast RP is configured, the current register state for each group:</td>
<td>extensive</td>
</tr>
<tr>
<td></td>
<td>• Group—Multicast group address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Source—Multicast source address for which the PIM register is sent or received, depending on whether this routing device is a designated router facing an RP router, or is the local RP, respectively.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Origin—How the information was obtained:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DIRECT—From a local attachment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MSDP—From the Multicast Source Discovery Protocol (MSDP)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• DR—From the designated router</td>
<td></td>
</tr>
<tr>
<td>RP selected</td>
<td>For sparse mode and bidirectional mode, the identity of the RP for the specified group address.</td>
<td>group-address</td>
</tr>
</tbody>
</table>

Sample Output

show pim rps

```
user@host> show pim rps
Instance: PIM.master
Address family INET
RP address      Type        Mode Holdtime Timeout Groups Group prefixes
10.10.1.3       static      bidir    150 None  2 224.1.3.0/24 225.1.3.0/24
10.10.13.2      static      bidir  150 None  2 224.1.1.0/24 225.1.1.0/24
```

show pim rps brief

The output for the `show pim rps brief` command is identical to that for the `show pim rps` command. For sample output, see `show pim rps on page 3517`.

show pim rps <group-address> (Bidirectional PIM)

```
user@host> show pim rps 224.1.1.1
Instance: PIM.master
224.1.0.0/16
   11.4.12.75 (Bidirectional)

RP selected: 11.4.12.75
```

show pim rps <group-address> (PIM Dense Mode)

```
user@host> show pim rps 224.1.1.1
Instance: PIM.master

Dense Mode active for group 224.1.1.1
```

show pim rps <group-address> (SSM Range Without asm-override-ssm Configured)

```
user@host> show pim rps 224.1.1.1
```
Instance: PIM.master

Source-specific Mode (SSM) active for group 224.1.1.1

show pim rps <group-address> (SSM Range With asm-override-ssm Configured and a Sparse-Mode RP)

Instance: PIM.master

Source-specific Mode (SSM) active with Sparse Mode ASM override for group 224.1.1.1

224.1.0.0/16
11.4.12.75

RP selected: 11.4.12.75

show pim rps <group-address> (SSM Range With asm-override-ssm Configured and a Bidirectional RP)

Instance: PIM.master

Source-specific Mode (SSM) active with Sparse Mode ASM override for group 224.1.1.1

224.1.0.0/16
11.4.12.75 (Bidirectional)

RP selected: (null)

show pim rps instance

Instance: PIM.master

Address family INET

RP address               Type        Holdtime Timeout Groups Group prefixes
10.10.47.100             static             0    None      1 224.0.0.0/4

Address family INET6

show pim rps extensive (PIM Sparse Mode)

Instance: PIM.master

Family: INET
RP: 10.255.245.91
Learned via: static configuration
Time Active: 00:05:48
Holdtime: 45 with 36 remaining
Device Index: 122
Subunit: 32768
Interface: pd-6/0/0.32768
Group Ranges:
   224.0.0.0/4, 36s remaining
Active groups using RP:
   225.1.1.1

   total 1 groups active

Register State for RP:
show pim rps extensive (Bidirectional PIM)

user@host> show pim rps extensive
Instance: PIM.master
Address family INET

RP: 10.10.1.3
Learned via: static configuration
Mode: Bidirectional
Time Active: 01:58:07
Holdtime: 150
Group Ranges:
   224.1.3.0/24
   225.1.3.0/24

RP: 10.10.13.2
Learned via: static configuration
Mode: Bidirectional
Time Active: 01:58:07
Holdtime: 150
Group Ranges:
   224.1.1.0/24
   225.1.1.0/24

show pim rps extensive (PIM Anycast RP in Use)

user@host> show pim rps extensive
Instance: PIM.master

Family: INET
RP: 10.10.2
Learned via: static configuration
Time Active: 00:54:52
Holdtime: 0
Device Index: 130
Subunit: 32769
Interface: pimd.32769
Group Ranges:
   224.0.0.0/4
Active groups using RP:
   224.10.10

   total 1 groups active

Anycast-PIM rpset:
   10.100.111.34
   10.100.111.17
   10.100.111.55

Anycast-PIM local address used: 10.100.111.1
Anycast-PIM Register State:

<table>
<thead>
<tr>
<th>Group</th>
<th>Source</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.1.1</td>
<td>10.10.95.2</td>
<td>DIRECT</td>
</tr>
<tr>
<td>224.1.1.2</td>
<td>10.10.95.2</td>
<td>DIRECT</td>
</tr>
<tr>
<td>224.10.10.10</td>
<td>10.10.70.1</td>
<td>MSDP</td>
</tr>
<tr>
<td>224.10.10.11</td>
<td>10.10.70.1</td>
<td>MSDP</td>
</tr>
<tr>
<td>224.20.20.1</td>
<td>10.10.71.1</td>
<td>DR</td>
</tr>
</tbody>
</table>
Address family INET6

Anycast-PIM rpset:
  ab::1
  ab::2
Anycast-PIM local address used: cd::1

Anycast-PIM Register State:

<table>
<thead>
<tr>
<th>Group</th>
<th>Source</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>::224.1.1.1</td>
<td>::10.10.95.2</td>
<td>DIRECT</td>
</tr>
<tr>
<td>::224.1.1.2</td>
<td>::10.10.95.2</td>
<td>DIRECT</td>
</tr>
<tr>
<td>::224.20.20.1</td>
<td>::10.10.71.1</td>
<td>DR</td>
</tr>
</tbody>
</table>
**show pim source**

**Syntax**

show pim source

- `<brief | detail>`
- `<inet | inet6>`
- `<instance instance-name>`
- `<logical-system (all | logical-system-name)>`
- `<source-prefix>`

**Syntax (EX Series Switch and the QFX Series)**

show pim source

- `<brief | detail>`
- `<inet | inet6>`
- `<instance instance-name>`
- `<source-prefix>`

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
`inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
Command introduced in Junos OS Release 11.3 for the QFX Series.

**Description**

Display information about the Protocol Independent Multicast (PIM) source reverse path forwarding (RPF) state.

**Options**

- **none**—Display standard information about the PIM RPF state for all supported family addresses for all routing instances.

  - `<brief | detail>`—(Optional) Display the specified level of output.

  - `<inet | inet6>`—(Optional) Display information for IPv4 or IPv6 family addresses, respectively.

  - `<instance instance-name>`—(Optional) Display information about the RPF state for a specific PIM-enabled routing instance.

  - `<logical-system (all | logical-system-name)>`—(Optional) Perform this operation on all logical systems or on a particular logical system.

  - `<source-prefix>`—(Optional) Display the state for source RPF states in the given range.

**Required Privilege**

- **view**

**List of Sample Output**

- show pim source on page 3522
- show pim source brief on page 3522
- show pim source detail on page 3522
- show pim source (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 3523

**Output Fields**

Table 429 on page 3522 describes the output fields for the `show pim source` command. Output fields are listed in the approximate order in which they appear.
### Table 429: show pim source Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance.</td>
</tr>
<tr>
<td>Source</td>
<td>Address of the source or reverse path.</td>
</tr>
<tr>
<td>Prefix/length</td>
<td>Prefix and prefix length for the route used to reach the RPF address.</td>
</tr>
<tr>
<td>Upstream Protocol</td>
<td>RPF interface toward the source address.</td>
</tr>
<tr>
<td>Upstream interface</td>
<td>A pseudo multipoint LDP (M-LDP) interface appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
</tr>
<tr>
<td>Upstream Neighbor</td>
<td>Address of the RPF neighbor used to reach the source address.</td>
</tr>
<tr>
<td></td>
<td>The multipoint LDP (M-LDP) root appears on egress nodes in M-LDP point-to-multipoint LSPs with inband signaling.</td>
</tr>
</tbody>
</table>

### Sample Output

**show pim source**

```
user@host> show pim source
Instance: PIM.master Family: INET

Source 10.255.14.144
  Prefix 10.255.14.144/32
  Upstream interface Local
  Upstream neighbor Local

Source 10.255.70.15
  Prefix 10.255.70.15/32
  Upstream interface so-1/0/0.0
  Upstream neighbor 10.111.10.2

Instance: PIM.master Family: INET6
```

**show pim source brief**

The output for the `show pim source brief` command is identical to that for the `show pim source` command. For sample output, see `show pim source on page 3522`.

**show pim source detail**

```
user@host> show pim source detail
Instance: PIM.master Family: INET

Source 10.255.14.144
  Prefix 10.255.14.144/32
  Upstream interface Local
  Upstream neighbor Local
  Active groups: 228.0.0.0
                  239.1.1.1
```

---

3522 Copyright © 2013, Juniper Networks, Inc.
show pim source (Egress Node with Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

user@host> show pim source
Instance: PIM.master Family: INET

Source 1.1.1.1
Prefix 1.1.1.1/32
Upstream interface Local
Upstream neighbor Local

Source 1.2.7.7
Prefix 1.2.7.0/24
Upstream protocol MLDP
Upstream interface Pseudo MLDP
Upstream neighbor MLDP LSP root <1.1.1.2>

Source 192.168.219.11
Prefix 192.168.219.0/28
Upstream protocol MLDP
Upstream interface Pseudo MLDP
Upstream neighbor MLDP LSP root <1.1.1.2>

Instance: PIM.master Family: INET6

Source abcd::1:2:7:7
Prefix abcd::1:2:7:0/120
Upstream protocol MLDP
Upstream interface Pseudo MLDP
Upstream neighbor MLDP LSP root <1.1.1.2>
### show pim statistics

**Syntax**

```
show pim statistics
<inet | inet6>
<instance instance-name>
<interface interface-name>
logical-system (all | logical-system-name)
```

**Syntax (EX Series Switch and the QFX Series)**

```
show pim statistics
<inet | inet6>
<instance instance-name>
<interface interface-name>
```

**Release Information**

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- `inet6` and `instance` options introduced in Junos OS Release 10.0 for EX Series switches.
- Command introduced in Junos OS Release 11.3 for the QFX Series.
- Support for bidirectional PIM added in Junos OS Release 12.1.

**Description**

Display Protocol Independent Multicast (PIM) statistics.

**Options**

- `none`—Display PIM statistics.
- `inet | inet6`—(Optional) Display IPv4 or IPv6 PIM statistics, respectively.
- `instance instance-name`—(Optional) Display statistics for a specific routing instance enabled by Protocol Independent Multicast (PIM).
- `interface interface-name`—(Optional) Display statistics about the specified interface.
- `logical-system (all | logical-system-name)`—(Optional) Perform this operation on all logical systems or on a particular logical system.

**Required Privilege Level**

- `view`

**Related Documentation**

- [clear pim statistics on page 3429](#)

**List of Sample Output**

- `show pim statistics on page 3531`
- `show pim statistics inet interface <interface-name> on page 3533`
- `show pim statistics inet6 interface <interface-name> on page 3533`
- `show pim statistics instance <instance-name> on page 3534`
- `show pim statistics interface <interface-name> on page 3535`

**Output Fields**

Table 430 on page 3525 describes the output fields for the `show pim statistics` command. Output fields are listed in the approximate order in which they appear.
### Table 430: show pim statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>Name of the routing instance. This field only appears if you specify an interface, for example:</td>
</tr>
<tr>
<td></td>
<td>- <code>inet interface interface-name</code></td>
</tr>
<tr>
<td></td>
<td>- <code>inet6 interface interface-name</code></td>
</tr>
<tr>
<td></td>
<td>- <code>interface interface-name</code></td>
</tr>
<tr>
<td>Family</td>
<td>Output is for IPv4 or IPv6 PIM statistics. <code>INET</code> indicates IPv4 statistics, and <code>INET6</code> indicates IPv6 statistics. This field only appears if you specify an interface, for example:</td>
</tr>
<tr>
<td></td>
<td>- <code>inet interface interface-name</code></td>
</tr>
<tr>
<td></td>
<td>- <code>inet6 interface interface-name</code></td>
</tr>
<tr>
<td></td>
<td>- <code>interface interface-name</code></td>
</tr>
<tr>
<td>PIM statistics</td>
<td>PIM statistics for all interfaces or for the specified interface.</td>
</tr>
<tr>
<td>PIM message type</td>
<td>Message type for which statistics are displayed.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of received statistics.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of messages sent of a certain type.</td>
</tr>
<tr>
<td>Rx errors</td>
<td>Number of received packets that contained errors.</td>
</tr>
<tr>
<td>V2 Hello</td>
<td>PIM version 2 hello packets.</td>
</tr>
<tr>
<td>V2 Register</td>
<td>PIM version 2 register packets.</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>PIM version 2 register stop packets.</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>PIM version 2 join and prune packets.</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>PIM version 2 bootstrap packets.</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>PIM version 2 assert packets.</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>PIM version 2 graft packets.</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>PIM version 2 graft acknowledgment packets.</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>PIM version 2 candidate RP packets.</td>
</tr>
</tbody>
</table>
Table 430: show pim statistics Output Fields *(continued)*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 State Refresh</td>
<td>PIM version 2 control messages related to PIM dense mode (PIM-DM) state refresh. State refresh is an extension to PIM-DM. It is not supported in Junos OS.</td>
</tr>
<tr>
<td>V2 DF Election</td>
<td>PIM version 2 send and receive messages associated with bidirectional PIM designated forwarder election.</td>
</tr>
<tr>
<td>V1 Query</td>
<td>PIM version 1 query packets.</td>
</tr>
<tr>
<td>V1 Register</td>
<td>PIM version 1 register packets.</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>PIM version 1 register stop packets.</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>PIM version 1 join and prune packets.</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>PIM version 1 RP reachability packets.</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>PIM version 1 assert packets.</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>PIM version 1 graft packets.</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>PIM version 1 graft acknowledgment packets.</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>Auto-RP announce packets.</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>Auto-RP mapping packets.</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>Auto-RP packets with an unknown type.</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>Auto-RP announce packets.</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>Auto-RP announce packets.</td>
</tr>
<tr>
<td>Global Statistics</td>
<td>Summary of PIM statistics for all interfaces.</td>
</tr>
<tr>
<td>Hello dropped on neighbor policy</td>
<td>Number of hello packets dropped because of a configured neighbor policy.</td>
</tr>
<tr>
<td>Unknown type</td>
<td>Number of PIM control packets received with an unknown type.</td>
</tr>
<tr>
<td>V1 Unknown type</td>
<td>Number of PIM version 1 control packets received with an unknown type.</td>
</tr>
<tr>
<td>Unknown Version</td>
<td>Number of PIM control packets received with an unknown version. The version is not version 1 or version 2.</td>
</tr>
</tbody>
</table>
Table 430: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor unknown</td>
<td>Number of PIM control packets received (excluding PIM hello) without first receiving the hello packet.</td>
</tr>
<tr>
<td>Bad Length</td>
<td>Number of PIM control packets received for which the packet size does not match the PIM length field in the packet.</td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>Number of PIM control packets received for which the calculated checksum does not match the checksum field in the packet.</td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>Number of PIM control packets received on an interface that does not have PIM configured.</td>
</tr>
<tr>
<td>Rx Bad Data</td>
<td>Number of PIM control packets received that contain data for TCP Bad register packets.</td>
</tr>
<tr>
<td>Rx intf disabled</td>
<td>Number of PIM control packets received on an interface that has PIM disabled.</td>
</tr>
<tr>
<td>Rx V1 Require V2</td>
<td>Number of PIM version 1 control packets received on an interface configured for PIM version 2.</td>
</tr>
<tr>
<td>Rx V2 Require V1</td>
<td>Number of PIM version 2 control packets received on an interface configured for PIM version 1.</td>
</tr>
<tr>
<td>Rx Register not RP</td>
<td>Number of PIM register packets received when the routing device is not the RP for the group.</td>
</tr>
<tr>
<td>Rx Register no route</td>
<td>Number of PIM register packets received when the RP does not have a unicast route back to the source.</td>
</tr>
<tr>
<td>Rx Register no decap if</td>
<td>Number of PIM register packets received when the RP does not have a de-encapsulation interface.</td>
</tr>
<tr>
<td>Null Register Timeout</td>
<td>Number of NULL register timeout packets.</td>
</tr>
<tr>
<td>RP Filtered Source</td>
<td>Number of PIM packets received when the routing device has a source address filter configured for the RP.</td>
</tr>
<tr>
<td>Rx Unknown Reg Stop</td>
<td>Number of register stop messages received with an unknown type.</td>
</tr>
<tr>
<td>Rx Join/Prune no state</td>
<td>Number of join and prune messages received for which the routing device has no state.</td>
</tr>
<tr>
<td>Rx Join/Prune on upstream if</td>
<td>Number of join and prune messages received on the interface used to reach the upstream routing device, toward the RP.</td>
</tr>
<tr>
<td>Rx Join/Prune for invalid group</td>
<td>Number of join or prune messages received for invalid multicast group addresses.</td>
</tr>
</tbody>
</table>
### Table 430: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Join/Prune messages dropped</td>
<td>Number of join and prune messages received and dropped.</td>
</tr>
<tr>
<td>Rx sparse join for dense group</td>
<td>Number of PIM sparse mode join messages received for a group that is configured for dense mode.</td>
</tr>
<tr>
<td>Rx Graft/Graft Ack no state</td>
<td>Number of graft and graft acknowledgment messages received for which the router or switch has no state.</td>
</tr>
<tr>
<td>Rx Graft on upstream if</td>
<td>Number of graft messages received on the interface used to reach the upstream routing device, toward the RP.</td>
</tr>
<tr>
<td>Rx CRP not BSR</td>
<td>Number of BSR messages received in which the PIM message type is Candidate-RP-Advertisement, not Bootstrap.</td>
</tr>
<tr>
<td>Rx BSR when BSR</td>
<td>Number of BSR messages received in which the PIM message type is Bootstrap.</td>
</tr>
<tr>
<td>Rx BSR not RPF if</td>
<td>Number of BSR messages received on an interface that is not the RPF interface.</td>
</tr>
<tr>
<td>Rx unknown hello opt</td>
<td>Number of PIM hello packets received with options that Junos OS does not support.</td>
</tr>
<tr>
<td>Rx data no state</td>
<td>Number of PIM control packets received for which the routing device has no state for the data type.</td>
</tr>
<tr>
<td>Rx RP no state</td>
<td>Number of PIM control packets received for which the routing device has no state for the RP.</td>
</tr>
<tr>
<td>Rx aggregate</td>
<td>Number of PIM aggregate MDT packets received.</td>
</tr>
<tr>
<td>Rx malformed packet</td>
<td>Number of PIM control packets received with a malformed IP unicast or multicast address family.</td>
</tr>
<tr>
<td>No RP</td>
<td>Number of PIM control packets received with no RP address.</td>
</tr>
<tr>
<td>No register encap if</td>
<td>Number of PIM register packets received when the first-hop routing device does not have an encapsulation interface.</td>
</tr>
<tr>
<td>No route upstream</td>
<td>Number of PIM control packets received when the routing device does not have a unicast route to the the interface used to reach the upstream routing device, toward the RP.</td>
</tr>
<tr>
<td>Nexthop Unusable</td>
<td>Number of PIM control packets with an unusable nexthop. A path can be unusable if the route is hidden or the link is down.</td>
</tr>
<tr>
<td>RP mismatch</td>
<td>Number of PIM control packets received for which the routing device has an RP mismatch.</td>
</tr>
</tbody>
</table>
### Table 430: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP mode mismatch</td>
<td>RP mode (sparse or bidirectional) mismatches encountered when processing join and prune messages.</td>
</tr>
<tr>
<td>RPF neighbor unknown</td>
<td>Number of PIM control packets received for which the routing device has an unknown RPF neighbor for the source.</td>
</tr>
<tr>
<td>Rx Joins/Prunes filtered</td>
<td>The number of join and prune messages filtered because of configured route filters and source address filters.</td>
</tr>
<tr>
<td>Tx Joins/Prunes filtered</td>
<td>The number of join and prune messages filtered because of configured route filters and source address filters.</td>
</tr>
<tr>
<td>Embedded-RP invalid addr</td>
<td>Number of packets received with an invalid embedded RP address in PIM join messages and other types of messages sent between routing domains.</td>
</tr>
<tr>
<td>Embedded-RP limit exceed</td>
<td>Number of times the limit configured with the maximum-rps statement is exceeded. The maximum-rps statement limits the number of embedded RPs created in a specific routing instance. The range is from 1 through 500. The default is 100.</td>
</tr>
</tbody>
</table>
| Embedded-RP added                 | Number of packets in which the embedded RP for IPv6 is added. The following receive events trigger extraction of an IPv6 embedded RP address on the routing device: 
  - Multicast Listener Discovery (MLD) report for an embedded RP multicast group address 
  - PIM join message with an embedded RP multicast group address 
  - Static embedded RP multicast group address associated with an interface 
  - Packets sent to an embedded RP multicast group address received on the DR 
  An embedded RP node discovered through these receive events is added if it does not already exist on the routing platform. |
| Embedded-RP removed               | Number of packets in which the embedded RP for IPv6 is removed. The embedded RP is removed whenever all PIM join states using this RP are removed or the configuration changes to remove the embedded RP feature. |
| Rx Register msgs filtering drop   | Number of received register messages dropped because of a filter configured for PIM register messages. |
| Tx Register msgs filtering drop   | Number of register messages dropped because of a filter configured for PIM register messages. |
| Rx Bidir Join/Prune on non-Bidir if | Error counter for join and prune messages received on non-bidirectional PIM interfaces. |
Table 430: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Bidir Join/Prune on non-DF if</td>
<td>Error counter for join and prune messages received on non-designated forwarder interfaces.</td>
</tr>
<tr>
<td>V4 (S,G) Maximum</td>
<td>Maximum number of (S,G) IPv4 multicast routes accepted for the VPN routing and forwarding (VRF) routing instance. If this number is met, additional (S,G) entries are not accepted.</td>
</tr>
<tr>
<td>V4 (S,G) Accepted</td>
<td>Number of accepted (S,G) IPv4 multicast routes.</td>
</tr>
<tr>
<td>V4 (S,G) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of (S,G) IPv4 multicast routes accepted by the device).</td>
</tr>
<tr>
<td>V4 (S,G) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V6 (S,G) Maximum</td>
<td>Maximum number of (S,G) IPv6 multicast routes accepted for the VPN routing and forwarding (VRF) routing instance. If this number is met, additional (S,G) entries are not accepted.</td>
</tr>
<tr>
<td>V6 (S,G) Accepted</td>
<td>Number of accepted (S,G) IPv6 multicast routes.</td>
</tr>
<tr>
<td>V6 (S,G) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of (S,G) IPv6 multicast routes accepted by the device).</td>
</tr>
<tr>
<td>V6 (S,G) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Maximum</td>
<td>Maximum number of group-to-rendezvous point (RP) IPv4 multicast mappings accepted for the VRF routing instance. If this number is met, additional mappings are not accepted.</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Accepted</td>
<td>Number of accepted group-to-RP IPv4 multicast mappings.</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of group-to-RP IPv4 multicast mappings accepted by the device).</td>
</tr>
<tr>
<td>V4 (grp-prefix, RP) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V6 (grp-prefix, RP) Maximum</td>
<td>Maximum number of group-to RP IPv6 multicast mappings accepted for the VRF routing instance. If this number is met, additional mappings are not accepted.</td>
</tr>
<tr>
<td>V6 (grp-prefix, RP) Accepted</td>
<td>Number of accepted group-to-RP IPv6 multicast mappings.</td>
</tr>
</tbody>
</table>
Table 430: show pim statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V6 (grp-prefix, RP) Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of group-to-RP IPv6 multicast mappings accepted by the device).</td>
</tr>
<tr>
<td>V6 (grp-prefix, RP) Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V4 Register Maximum</td>
<td>Maximum number of IPv4 PIM registers accepted for the VRF routing instance. If this number is met, additional PIM registers are not accepted. You configure the register limits on the RP.</td>
</tr>
<tr>
<td>V4 Register Accepted</td>
<td>Number of accepted IPv4 PIM registers.</td>
</tr>
<tr>
<td>V4 Register Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of IPv4 PIM registers accepted by the device).</td>
</tr>
<tr>
<td>V4 Register Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
<tr>
<td>V6 Register Maximum</td>
<td>Maximum number of IPv6 PIM registers accepted for the VRF routing instance. If this number is met, additional PIM registers are not accepted. You configure the register limits on the RP.</td>
</tr>
<tr>
<td>V6 Register Accepted</td>
<td>Number of accepted IPv6 PIM registers.</td>
</tr>
<tr>
<td>V6 Register Threshold</td>
<td>Threshold at which a warning message is logged (percentage of the maximum number of IPv6 PIM registers accepted by the device).</td>
</tr>
<tr>
<td>V6 Register Log Interval</td>
<td>Time (in seconds) between consecutive log messages.</td>
</tr>
</tbody>
</table>

Sample Output

```
show pim statistics

user@host> show pim statistics

PIM Message type        Received       Sent  Rx errors
V2 Hello                      15         32          0
V2 Register                    0        362          0
V2 Register Stop             483          0          0
V2 Join Prune                 18        518          0
V2 Bootstrap                   0          0          0
V2 Assert                      0          0          0
V2 Graft                       0          0          0
V2 Graft Ack                   0          0          0
V2 Candidate RP               0          0          0
V2 State Refresh              0          0          0
V2 DF Election                0          0          0
V1 Query                      0          0          0
V1 Register                   0          0          0
```
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
</tr>
<tr>
<td><strong>Global Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Hello dropped on neighbor policy</td>
<td>0</td>
</tr>
<tr>
<td>Unknown type</td>
<td>0</td>
</tr>
<tr>
<td>V1 Unknown type</td>
<td>0</td>
</tr>
<tr>
<td>Unknown Version</td>
<td>0</td>
</tr>
<tr>
<td>ipv4 BSR pkt drop due to excessive rate</td>
<td>0</td>
</tr>
<tr>
<td>ipv6 BSR pkt drop due to excessive rate</td>
<td>0</td>
</tr>
<tr>
<td>Neighbor unknown</td>
<td>0</td>
</tr>
<tr>
<td>Bad Length</td>
<td>0</td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>0</td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bad Data</td>
<td>0</td>
</tr>
<tr>
<td>Rx Intf disabled</td>
<td>0</td>
</tr>
<tr>
<td>Rx V1 Require V2</td>
<td>0</td>
</tr>
<tr>
<td>Rx V2 Require V1</td>
<td>0</td>
</tr>
<tr>
<td>Rx Register not RP</td>
<td>0</td>
</tr>
<tr>
<td>Rx Register no route</td>
<td>0</td>
</tr>
<tr>
<td>Rx Register no decap if</td>
<td>0</td>
</tr>
<tr>
<td>Null Register Timeout</td>
<td>0</td>
</tr>
<tr>
<td>RP Filtered Source</td>
<td>0</td>
</tr>
<tr>
<td>Rx Unknown Reg Stop</td>
<td>0</td>
</tr>
<tr>
<td>Rx Join/Prune no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx Join/Prune on upstream if</td>
<td>0</td>
</tr>
<tr>
<td>Rx Join/Prune for invalid group</td>
<td>0</td>
</tr>
<tr>
<td>Rx Join/Prune messages dropped</td>
<td>0</td>
</tr>
<tr>
<td>Rx sparse join for dense group</td>
<td>0</td>
</tr>
<tr>
<td>Rx Graft/Graft Ack no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx Graft on upstream if</td>
<td>0</td>
</tr>
<tr>
<td>Rx CRP not BSR</td>
<td>0</td>
</tr>
<tr>
<td>Rx BSR when BSR</td>
<td>0</td>
</tr>
<tr>
<td>Rx BSR not RPF if</td>
<td>0</td>
</tr>
<tr>
<td>Rx unknown hello opt</td>
<td>0</td>
</tr>
<tr>
<td>Rx data no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx RP no state</td>
<td>0</td>
</tr>
<tr>
<td>Rx aggregate</td>
<td>0</td>
</tr>
<tr>
<td>Rx malformed packet</td>
<td>0</td>
</tr>
<tr>
<td>Rx illegal TTL</td>
<td>0</td>
</tr>
<tr>
<td>Rx illegal destination address</td>
<td>0</td>
</tr>
<tr>
<td>No RP</td>
<td>0</td>
</tr>
<tr>
<td>No register encap if</td>
<td>0</td>
</tr>
<tr>
<td>No route upstream</td>
<td>0</td>
</tr>
<tr>
<td>Nexthop Unusable</td>
<td>0</td>
</tr>
<tr>
<td>RP mismatch</td>
<td>0</td>
</tr>
<tr>
<td>RP mode mismatch</td>
<td>0</td>
</tr>
<tr>
<td>RPF neighbor unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Joins/Prunes filtered</td>
<td>0</td>
</tr>
<tr>
<td>Tx Joins/Prunes filtered</td>
<td>0</td>
</tr>
<tr>
<td>Embedded-RP invalid addr</td>
<td>0</td>
</tr>
</tbody>
</table>
### Sample Output

**show pim statistics inet interface <interface-name>**

```bash
user@host> show pim statistics inet interface ge-0/3/0.0
Instance: PIM.master Family: INET

PIM Interface statistics for ge-0/3/0.0

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

### Sample Output

**show pim statistics inet6 interface <interface-name>**

```bash
user@host> show pim statistics inet6 interface ge-0/3/0.0
Instance: PIM.master Family: INET6

PIM Interface statistics for ge-0/3/0.0

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show pim statistics instance <instance-name>

```
user@host> show pim statistics instance VPN-A
PIM Message type      Received  Sent  Rx errors
V2 Hello              31        37      0
V2 Register           0         0      0
V2 Register Stop      0         0      0
V2 Join Prune         0         16     0
V2 Bootstrap          0         0      0
V2 Assert             0         0      0
V2 Graft              0         0      0
V2 Graft Ack          0         0      0
V2 Candidate RP       0         0      0
V2 State Refresh      0         0      0
V2 DF Election        0         0      0
V1 Query              0         0      0
V1 Register           0         0      0
V1 Register Stop      0         0      0
V1 Join Prune         0         0      0
V1 RP Reachability    0         0      0
V1 Assert             0         0      0
V1 Graft              0         0      0
V1 Graft Ack          0         0      0
AutoRP Announce       0         0      0
AutoRP Mapping        0         0      0
AutoRP Unknown type   0         0      0
Anycast Register      0         0      0
Anycast Register Stop 0         0      0

Global Statistics

Hello dropped on neighbor policy  0
Unknown type                     0
V1 Unknown type                  0
Unknown Version                  0
Neighbor unknown                 0
Bad Length                       0
Bad Checksum                     0
Bad Receive If                   0
Rx Bad Data                      0
Rx Intf disabled                 0
Rx V1 Require V2                 0
Rx V2 Require V1                 0
Rx Register not RP               0
Rx Register no route             0
Rx Register no decap if          0
Null Register Timeout            0
RP Filtered Source               0
Rx Unknown Reg Stop              0
Rx Join/Prune no state           0
Rx Join/Prune on upstream if     0
Rx Join/Prune for invalid group  0
Rx Join/Prune messages dropped   0
Rx sparse join for dense group   0
Rx Graft/Graft Ack no state      0
Rx Graft on upstream if          0
Rx CRP not BSR                   0
Rx BSR when BSR                  0
```
Sample Output

```
show pim statistics interface <interface-name>
```

```
user@host> show pim statistics interface ge-0/3/0.0
Instance: PIM.master Family: INET

PIM Interface statistics for ge-0/3/0.0

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Query</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 RP Reachability</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V1 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Announce</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Mapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AutoRP Unknown type</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Instance: PIM.master Family: INET6

PIM Interface statistics for ge-0/3/0.0

<table>
<thead>
<tr>
<th>PIM Message type</th>
<th>Received</th>
<th>Sent</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2 Hello</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Join Prune</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Bootstrap</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Assert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Graft Ack</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>V2 Candidate RP</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Anycast Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
PART 22

Network Management and Monitoring

- Overview on page 3539
- Configuration on page 3559
- Administration on page 3783
- Troubleshooting on page 3915
CHAPTER 66

Overview

- Real-Time Performance Monitoring on page 3539
- Analyzers and Port Mirroring on page 3543
- sFlow Monitoring Technology on page 3548
- Ethernet OAM Link Fault Management and Connectivity Fault Management on page 3551
- Uplink Failure Detection on page 3556

Real-Time Performance Monitoring

- Understanding Real-Time Performance Monitoring on EX Series Switches on page 3540
Understanding Real-Time Performance Monitoring on EX Series Switches

Real-time performance monitoring (RPM) enables you to configure active probes to track and monitor traffic across the network and to investigate network problems. You can use RPM with Juniper Networks EX Series Ethernet Switches.

The ways in which you can use RPM include:

- Monitor time delays between devices.
- Monitor time delays at the protocol level.
- Set thresholds to trigger SNMP traps when values are exceeded.

You can configure thresholds for round-trip time, ingress or egress delay, standard deviation, jitter, successive lost probes, and total lost probes per test. (SNMP trap results are stored in `pingResultsTable`, `jnxPingResultsTable`, `jnxPingProbeHistoryTable`, and `pingProbeHistoryTable`.)

- Determine automatically whether a path exists between a host router or switch and its configured BGP neighbors. You can view the results of the discovery using an SNMP client.
- Use the history of the most recent 50 probes to analyze trends in your network and predict future needs.

RPM provides MIB support with extensions for RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.

This topic includes:

- RPM Packet Collection on page 3540
- Tests and Probe Types on page 3540
- Hardware Timestamps on page 3541
- Limitations of RPM on EX Series Switches on page 3543

**RPM Packet Collection**

Probes collect packets per destination and per application, including ping Internet Control Message Protocol (ICMP) packets, User Datagram Protocol and Transmission Control Protocol (UDP/TCP) packets with user-configured ports, user-configured Differentiated Services code point (DSCP) type-of-service (ToS) packets, and Hypertext Transfer Protocol (HTTP) packets.

**Tests and Probe Types**

A test can contain multiple probes. The probe type specifies the packet and protocol contents of the probe.

EX Series switches support the following tests and probe types:

- Ping tests:
  - ICMP echo probe
- ICMP timestamp probe
- HTTP tests:
  - HTTP get probe (not available for BGP RPM services)
  - HTTP get metadata probe
- UDP and TCP tests with user-configured ports:
  - UDP echo probe
  - TCP connection probe
  - UDP timestamp probe

**Hardware Timestamps**

To account for latency or jitter in the communication of probe messages, you can enable timestamping of the probe packets (hardware timestamps). If hardware timestamps are not configured, then timers are generated at the software level and are less accurate than they would have been with hardware timestamps.

---

**NOTE:** EX Series switches support hardware timestamps for UDP and ICMP probes. EX Series switches do not support hardware timestamps for HTTP or TCP probes.

---

You can timestamp the following RPM probes to improve the measurement of latency or jitter:

- ICMP ping
- ICMP ping timestamp
- UDP ping
- UDP ping timestamp

You should configure the requester (the RPM client) with hardware timestamps (see Figure 44 on page 3542) to get more meaningful results than you would get without the timestamps. The responder (the RPM server) does not need to be configured to support hardware timestamps. If the responder supports hardware timestamps, it timestamps the RPM probes. If the responder does not support hardware timestamps, RPM can only report round-trip measurements that include the processing time on the responder.

---

**NOTE:** Hardware timestamps are supported on all EX Series switches.

---

Figure 44 on page 3542 shows the timestamps:
Figure 44: RPM Timestamps

- T1 is the time the packet leaves the requester port.
- T2 is the time the responder receives the packet.
- T3 is the time the responder sends the response.
- T4 is the time the requester receives the response.

The round-trip time is \((T2 - T1) + (T4 - T3)\). If the responder does not support hardware timestamps, then the round-trip time is \((T4 - T1) / 2\), and thus includes the processing time of the responder.

You can use RPM probes to find the following time measurements:

- Minimum round-trip time
- Maximum round-trip time
- Average round-trip time
- Standard deviation of the round-trip time
- Jitter of the round-trip time—Difference between the minimum and maximum round-trip time

**NOTE:** See “Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure)” on page 3611 for information on how to configure hardware timestamps on the requester.

The RPM feature provides a configuration option to set one-way hardware timestamps. Use one-way timestamps when you want information about one-way time, rather than round-trip times, for packets to traverse the network between the requester and the responder. As shown in Figure 44 on page 3542, one-way timestamps represent the time \(T2 - T1\) and the time from \(T4 \rightarrow T3\). Use one-way timestamps when you want to gather information about delay in each direction and to find egress and ingress jitter values.

**NOTE:** For correct one-way measurement, the clocks of the requester and responder must be synchronized. If the clocks are not synchronized, one-way jitter measurements and calculations can include significant variations, in some cases orders of magnitude greater than the round-trip times.
When you enable one-way timestamps in a probe, the following one-way measurements are reported:

- Minimum, maximum, standard deviation, and jitter measurements for egress and ingress times
- Number of probes sent
- Number of probe responses received
- Percentage of lost probes

**Limitations of RPM on EX Series Switches**

- Two-Way Active Measurement Protocol (TWAMP) is not supported on EX Series switches.
- EX Series switches do not support user-configured class-of-service (CoS) classifiers or prioritization of RPM packets over regular data packets received on an input interface.
- Timestamps:
  - If the responder does not support hardware timestamps, RPM can only report the round-trip measurements and cannot calculate round-trip jitter.
  - EX Series switches do not support hardware timestamps for HTTP and TCP probes.
  - Timestamps apply only to IPv4 traffic.

**Related Documentation**

- For further details about RPM, see *Junos OS Services Interfaces Configuration Guide*
- Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure) on page 3611
- Configuring Real-Time Performance Monitoring (J-Web Procedure) on page 3604
- Configuring SNMP (J-Web Procedure) on page 3594
- Monitoring Network Traffic Using Traceroute on page 3785

**Analyzers and Port Mirroring**

- Understanding Port Mirroring and Analyzers on EX4300 Switches on page 3544
Understanding Port Mirroring and Analyzers on EX4300 Switches

NOTE: This concept uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Understanding Port Mirroring on EX Series Switches. For ELS details, see Getting Started with Enhanced Layer 2 Software.

Mirroring might be needed for traffic analysis on a switch because a switch, unlike a hub, does not broadcast packets to every port on the destination device. The switch sends packets only to the port to which the destination device is connected.

Juniper Networks EX4300 Ethernet Switches support the following mirroring methods: port mirroring and analyzers. You can use port mirroring or analyzers to facilitate analyzing traffic on EX4300 switches at the packet level. You might use analyzers as part of monitoring switch traffic for such purposes as enforcing policies concerning network usage and file sharing and for identifying sources of problems on your network by locating abnormal or heavy bandwidth usage by particular stations or applications.

Mirrored packets can be copied either to a local interface for local monitoring or to a VLAN for remote monitoring. The following packets can be copied:

- **Packets entering or exiting a port**—You can mirror the packets in any combination of packets entering or exiting ports on up to 256 ports. For example, you can send copies of the packets entering some ports and the packets exiting other ports to the same local analyzer port or analyzer VLAN.

- **Packets entering a VLAN**—You can mirror the packets entering a VLAN to either a local analyzer port or to an analyzer VLAN. You can configure multiple VLANs (up to 256 VLANs), including a VLAN range and PVLANs, as ingress input to an analyzer.

- **Policy-based sample packets**—You can mirror a policy-based sample of packets that are entering a port or a VLAN. You configure a firewall filter to establish a policy to select the packets to be mirrored. You can send the sample to a port-mirroring instance or to an analyzer VLAN.

This topic describes:

- Port Mirroring Overview on page 3544
- Analyzer Overview on page 3545
- Port Mirroring and Analyzer Terminologies on page 3545
- Configuration Guidelines for Port Mirroring and Analyzers on EX4300 Switches on page 3546

**Port Mirroring Overview**

You configure port mirroring on an EX4300 switch to send copies of unicast traffic to an output destination such as an interface, a routing-instance, or a VLAN. Then, you can analyze the mirrored traffic by using a protocol analyzer application. The protocol analyzer
application can run either on a computer connected to the analyzer output interface or on a remote monitoring station. For the input traffic, you can configure a firewall filter term to specify whether port mirroring must be applied to all packets at the interface to which the firewall filter is applied. You can apply a firewall filter configured with the action `port-mirror` or `port-mirror-instance name` to the input or output logical interfaces (including aggregated Ethernet logical interfaces), to traffic forwarded or flooded to a VLAN, or traffic forwarded or flooded to a VPLS routing instance. EX4300 switches support port mirroring of VPLS (family ethernet-switching or family vpls) traffic and VPN traffic with family ccc in a Layer 2 environment. Within a firewall filter term, you can specify the port-mirroring properties under the `then` statement in either of the following ways:

- Implicitly reference the port-mirroring properties in effect on the port.
- Explicitly reference a particular named instance of port mirroring.

You can configure port mirroring at the `[edit forwarding-options port-mirroring]` hierarchy level.

**Analyzer Overview**

You can configure an analyzer to define both the input traffic and output traffic in the same analyzer configuration. The input traffic to be analyzed can be traffic that enters or exits an interface, or traffic that enters a VLAN. The analyzer configuration enables you to send this traffic to an output interface, instance, or VLAN. You can configure an analyzer at the `[edit forwarding-options analyzer]` hierarchy.

**Port Mirroring and Analyzer Terminologies**

Table 431 on page 3545 lists some port mirroring terms and their descriptions.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer</td>
<td>In a mirroring configuration (analyzer) on an EX4300 switch, the analyzer includes:</td>
</tr>
<tr>
<td></td>
<td>- The name of the analyzer</td>
</tr>
<tr>
<td></td>
<td>- Source (input) ports or VLAN</td>
</tr>
<tr>
<td></td>
<td>- A destination for mirrored packets (either a monitor port or a monitor VLAN)</td>
</tr>
</tbody>
</table>

**Analyzer output interface**

(Also known as monitor port) Interface to which mirrored traffic is sent and to which a protocol analyzer application is connected.

**NOTE:** Interfaces used as output for an analyzer must be configured under the `ethernet-switching` family.

Analyzer output interfaces have the following limitations:

- Cannot also be a source port.
- Do not participate in Layer 2 protocols, such as Spanning Tree Protocol (STP), when part of a port-mirroring configuration.
- If the bandwidth of the analyzer output interface is not sufficient to handle the traffic from the source ports, overflow packets are dropped.
Table 431: Mirroring Terminologies (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer VLAN</td>
<td>VLAN to which mirrored traffic is sent. The mirrored traffic can be used by a protocol analyzer application. The member interfaces in the monitor VLAN are spread across the switches in your network.</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>A port-mirroring configuration that does not specify an input source; it specifies only an output destination. A firewall filter configuration must be defined for the input source. A firewall filter configuration must be defined to mirror packets that match the match conditions defined in the firewall filter term. The action item <strong>port-mirror-instance instance-name</strong> in the firewall filter configuration is used to send packets to the analyzer and these packets form the input source.</td>
</tr>
<tr>
<td>Global port mirror</td>
<td>A port mirroring configuration that does not have an instance name. The firewall filter action <strong>port-mirror</strong> will be the action for the firewall filter configuration.</td>
</tr>
<tr>
<td>Input interface</td>
<td>An interface on the switch that is being mirrored. Traffic that is either entering or exiting this interface is mirrored.</td>
</tr>
<tr>
<td>LAG-based analyzer</td>
<td>An analyzer that has a link aggregation group (LAG) specified as the input (ingress) interface in the analyzer configuration.</td>
</tr>
<tr>
<td>Local mirroring</td>
<td>An analyzer configuration in which packets are mirrored to a local analyzer port.</td>
</tr>
<tr>
<td>Monitoring station</td>
<td>A computer running a protocol analyzer application.</td>
</tr>
<tr>
<td>Native analyzer session</td>
<td>An analyzer session that has both input and output definitions in its analyzer configuration.</td>
</tr>
<tr>
<td>Policy-based mirroring</td>
<td>Mirroring of packets that match the match items in the defined firewall filter term. The action item <strong>port-mirror-instance instance-name</strong> is used in the firewall filter to send the packets to the monitor port.</td>
</tr>
<tr>
<td>Port-based analyzer</td>
<td>An analyzer session whose configuration defines interfaces for both input and output.</td>
</tr>
<tr>
<td>Protocol analyzer application</td>
<td>An application used to examine packets transmitted across a network segment. Also commonly called network analyzer, packet sniffer, or probe.</td>
</tr>
<tr>
<td>Remote port mirroring</td>
<td>Functions the same way as local port mirroring, except that the mirrored traffic is not copied to a local analyzer port but is flooded to an analyzer VLAN that you create specifically for the purpose of receiving mirrored traffic.</td>
</tr>
<tr>
<td>VLAN-based analyzer</td>
<td>An analyzer session whose configuration uses VLANs for both input and output or for either input or output.</td>
</tr>
</tbody>
</table>

Configuration Guidelines for Port Mirroring and Analyzers on EX4300 Switches

When you configure port mirroring or analyzers on EX4300 switches, we recommend that you follow certain guidelines to ensure that you obtain optimum benefit from mirroring. Additionally, we recommend that you disable mirroring when you are not using it and that you select specific interfaces for which packets must be mirrored (that is,
select specific interfaces as input to the analyzer) in preference to using the all keyword option, which will enable mirroring on all interfaces. Mirroring only the necessary packets reduces any potential performance impact.

With local mirroring, traffic from multiple ports is replicated to the analyzer output interface. If the output interface for an analyzer reaches capacity, packets are dropped. Thus, while configuring an analyzer, you must consider whether the traffic being mirrored exceeds the capacity of the analyzer output interface.

Table 432 on page 3547 summarizes further configuration guidelines for mirroring on EX4300 switches.

Table 432: Configuration Guidelines for Port Mirroring and Analyzers on EX4300 Switches

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Value or Support Information</th>
<th>Comment</th>
</tr>
</thead>
</table>
| Number of VLANs that you can use as ingress input to an analyzer. | 256                           | • You can configure more than the specified number of analyzers on the switch, but you can enable only the specified number for a session. Use disable forwarding-options analyzer name to disable an analyzer.  
• You can configure three port-mirroring sessions and one global port-mirroring session. See Table 431 on page 3545 for a description of global port mirror. A single port-mirroring session is reserved for a global port-mirroring session.  
• Multiple analyzer and port-mirroring sessions can co-exist, but their total must be three.  |
| Number of port-mirroring sessions and analyzers that you can enable concurrently. | 4                             | • Virtual Chassis ports (VCPs)  
• Management Ethernet ports (me0 or vme0)  
• Integrated routing and bridging (IRB) interfaces; also known as routed VLAN interfaces (RVIs).  
• VLAN-tagged Layer 3 interfaces  |
| Types of ports on which you cannot mirror traffic.          |                               | • Protocol families that you can include in a port-mirroring configuration for remote traffic.  
• Traffic directions that you can configure for mirroring on ports in firewall-filter–based configurations.  
• Mirrored packets exiting an interface reflect rewritten class-of-service (CoS) DSCP or 802.1p bits. |
| Protocol families that you can include in a port-mirroring configuration for remote traffic. | any                           | Applicable  |
| Traffic directions that you can configure for mirroring on ports in firewall-filter–based configurations. | Ingress only                  |               |
| Mirrored packets exiting an interface reflect rewritten class-of-service (CoS) DSCP or 802.1p bits. | Applicable                    |               |
Table 432: Configuration Guidelines for Port Mirroring and Analyzers on EX4300 Switches (continued)

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Value or Support Information</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets with physical layer errors are not sent to the local or remote analyzer.</td>
<td>Applicable</td>
<td>Packets with these errors are filtered out and thus are not sent to the analyzer.</td>
</tr>
<tr>
<td>Port mirroring does not support line-rate traffic.</td>
<td>Applicable</td>
<td>Port mirroring for line-rate traffic is done on a best-effort basis.</td>
</tr>
<tr>
<td>Mirroring of packets egressing a VLAN.</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>Port-mirroring or analyzer output on a LAG interface.</td>
<td>Supported</td>
<td></td>
</tr>
<tr>
<td>Maximum number of child members on a port-mirroring or analyzer output LAG interface.</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Maximum number of interfaces in a remote port-mirroring or analyzer VLAN.</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Egress mirroring of host-generated control packets.</td>
<td>Not Supported</td>
<td></td>
</tr>
<tr>
<td>Configuring Layer 3 logical interfaces in the input stanza of an analyzer.</td>
<td>Not supported</td>
<td>This functionality can be achieved by configuring port mirroring.</td>
</tr>
<tr>
<td>The analyzer input and output stanzas containing members of the same VLAN or the VLAN itself must be avoided.</td>
<td>Applicable</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**

- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 3601
- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) on page 3597
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096

**sFlow Monitoring Technology**

- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 3549
Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch

The sFlow technology is a monitoring technology for high-speed switched or routed networks. sFlow monitoring technology randomly samples network packets and sends the samples to a monitoring station. You can configure sFlow technology on a Juniper Networks EX Series Ethernet Switch to continuously monitor traffic at wire speed on all interfaces simultaneously.

This topic describes:

- Sampling Mechanism and Architecture of sFlow Technology on EX Series Switches on page 3549
- Adaptive Sampling on page 3550
- sFlow Agent Address Assignment on page 3551

Sampling Mechanism and Architecture of sFlow Technology on EX Series Switches

sFlow technology uses the following two sampling mechanisms:

- Packet-based sampling: Samples one packet out of a specified number of packets from an interface enabled for sFlow technology.
- Time-based sampling: Samples interface statistics at a specified interval from an interface enabled for sFlow technology.

The sampling information is used to create a network traffic visibility picture. The Juniper Networks Junos operating system (Junos OS) fully supports the sFlow standard described in RFC 3176, *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks* (see [http://faqs.org/rfcs/rfc3176.html](http://faqs.org/rfcs/rfc3176.html)).

**NOTE:** sFlow technology on the switches samples only raw packet headers. A raw Ethernet packet is the complete Layer 2 network frame.

An sFlow monitoring system consists of an sFlow agent embedded in the switch and a centralized collector. The sFlow agent’s two main activities are random sampling and statistics gathering. It combines interface counters and flow samples and sends them across the network to the sFlow collector in UDP datagrams, directing those datagrams to the IP address and UDP destination port of the collector. Each datagram contains the following information:

- The IP address of the sFlow agent
- The number of samples
- The interface through which the packets entered the agent
- The interface through which the packets exited the agent
- The source and destination interface for the packets
- The source and destination VLAN for the packets
EX Series switches adopt the distributed sFlow architecture. The sFlow agent has two separate sampling entities that are associated with each Packet Forwarding Engine. These sampling entities are known as subagents. Each subagent has a unique ID that is used by the collector to identify the data source. A subagent has its own independent state and forwards its own sample messages to the sFlow agent. The sFlow agent is responsible for packaging the samples into datagrams and sending them to the sFlow collector. Because sampling is distributed across subagents, the protocol overhead associated with sFlow technology is significantly reduced at the collector.

**NOTE:** If the mastership assignment changes in a Virtual Chassis setup, sFlow technology continues to function.

### Adaptive Sampling

The switches use adaptive sampling to ensure both sampling accuracy and efficiency. Adaptive sampling is a process of monitoring the overall incoming traffic rate on the network device and providing intelligent feedback to interfaces to dynamically adapt their sampling rate to the traffic conditions. Interfaces on which incoming traffic exceeds the system threshold are checked so that all violations can be regulated without affecting the traffic on other interfaces. Every 12 seconds the agent checks interfaces to get the number of samples, and interfaces are grouped based on the slot that they belong to. The top five interfaces that produce the highest number of samples are selected. Using the binary backoff algorithm, the sampling load on these interfaces is reduced by half and allotted to interfaces that have a lower sampling rate. Therefore, when the processor’s sampling limit is reached, the sampling rate is adapted such that it does not load the processor any further. If the switch is rebooted, the adaptive sampling rate is reset to the user-configured sampling rate. Also, if you modify the sampling rate, the adaptive sampling rate changes.

The advantage of adaptive sampling is that the switch continues to operate at its optimum level even when there is a change in the traffic patterns in the interfaces. You do not need to make any changes. Because the sampling rate adapts dynamically to changing network conditions, the resources are utilized optimally resulting in a high performance network.

Infrequent sampling flows are not reported in the sFlow information, but over time the majority of flows are reported. Based on a defined sampling rate, 1 out of \( N \) packets is captured and sent to the collector. This type of sampling does not provide a 100 percent accurate result in the analysis, but it does provide a result with quantifiable accuracy. A user-configured polling interval defines how often the sFlow data for a specific interface are sent to the collector, but an sFlow agent can also schedule polling.

**NOTE:** sFlow technology on EX Series switches does not support graceful restart. When a graceful restart occurs, the adaptive sampling rate is set to the user-configured sampling rate.
sFlow Agent Address Assignment

The sFlow collector uses the sFlow agent's IP address to determine the source of the sFlow data. You can configure the IP address of the sFlow agent to ensure that the agent ID of the sFlow agent remains constant. If you do not specify the IP address to be assigned to the agent, an IP address is automatically assigned to the agent based on the following order of priority of interfaces configured on the switch:

1. Virtual management Ethernet (VME) interface
2. Management Ethernet interface

If neither of the preceding interfaces has been configured, the IP address of any Layer 3 interface or the routed VLAN interface (RVI) is assigned to the agent. At least one interface must be configured on the switch for an IP address to be automatically assigned to the agent. When the agent's IP address is assigned automatically, the IP address is dynamic and changes when the switch reboots.

sFlow data can be used to provide network traffic visibility information. You can explicitly configure the IP address to be assigned to source data (sFlow datagrams). If you do not explicitly configure that address, the IP address of the configured Gigabit Ethernet interface, 10-Gigabit Ethernet interface, or the routed VLAN interface (RVI) is used as the source IP address.

Related Documentation

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
- Monitoring Interface Status and Traffic on page 2463

Ethernet OAM Link Fault Management and Connectivity Fault Management

- Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 3551
- Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 3553
- Understanding Ethernet Frame Delay Measurements on Switches on page 3554

Understanding Ethernet OAM Link Fault Management for an EX Series Switch

Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches allows the Ethernet interfaces on these switches to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities even as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward-compatible with existing Ethernet technology.
Ethernet OAM provides the tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. Ethernet OAM should:

- Rely only on the media access control (MAC) address or virtual LAN identifier for troubleshooting.
- Work independently of the actual Ethernet transport and function over physical Ethernet ports or a virtual service such as pseudowire.
- Isolate faults over a flat (or single operator) network architecture or nested or hierarchical (or multiprovider) networks.

The following OAM LFM features are supported on EX Series switches:

- **Discovery and Link Monitoring**
  The discovery process is triggered automatically when OAM is enabled on the interface. The discovery process permits Ethernet interfaces to discover and monitor the peer on the link if it also supports the IEEE 802.3ah standard. You can specify the discovery mode used for IEEE 802.3ah OAM support. In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality. In passive mode, the peer initiates the discovery process. After the discovery process has been initiated, both sides participate in discovery. The switch performs link monitoring by sending periodic OAM protocol data units (PDUs) to advertise OAM mode, configuration, and capabilities.
  
  You can specify the number of OAM PDUs that an interface can miss before the link between peers is considered down.

- **Remote Fault Detection**
  Remote fault detection uses flags and events. Flags are used to convey the following: Link Fault means a loss of signal, Dying Gasp means an unrecoverable condition such as a power failure, and Critical Event means an unspecified vendor-specific critical event. You can specify the periodic OAM PDU sending interval for fault detection. The EX Series switch uses the Event Notification OAM PDU to notify the remote OAM device when a problem is detected. You can specify the action to be taken by the system when the configured link-fault event occurs.

- **Remote Loopback Mode**
  Remote loopback mode ensures link quality between the switch and a remote peer during installation or troubleshooting. In this mode, when the interface receives a frame that is not an OAM PDU or a pause frame, it sends it back on the same interface on which it was received. The link appears to be in the active state. You can use the returned loopback acknowledgement to test delay, jitter, and throughput.
  
  Junos OS can place a remote DTE into loopback mode (if remote loopback mode is supported by the remote DTE). When you place a remote DTE into loopback mode, the interface receives the remote loopback request and puts the interface into remote loopback mode. When the interface is in remote loopback mode, all frames except OAM PDUs are looped back without any changes made to the frames. OAM PDUs continue to be sent and processed.
Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch

Ethernet interfaces on Juniper Networks EX Series Ethernet Switches and Juniper Networks Junos operating system (Junos OS) for EX Series switches support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM). CFM monitors Ethernet networks that might comprise one or more service instances for network-compromising connectivity faults.

The major features of CFM are:

- Fault monitoring using the continuity check protocol. This is a neighbor discovery and health check protocol that discovers and maintains adjacencies at the VLAN or link level.
- Path discovery and fault verification using the linktrace protocol.
- Fault isolation using the loopback protocol.

CFM partitions the service network into various administrative domains. For example, operators, providers, and customers might be part of different administrative domains. Each administrative domain is mapped into one maintenance domain providing enough information to perform its own management, thus avoiding security breaches and making end-to-end monitoring possible.

In a CFM maintenance domain, each service instance is called a maintenance association. A maintenance association can be thought of as a full mesh of maintenance association endpoints (MEPs) having similar characteristics. MEPs are active CFM entities generating and responding to CFM protocol messages. There is also a maintenance intermediate point (MIP), which is a CFM entity similar to the MEP, but more passive (MIPs only respond to CFM messages).

Each maintenance domain is associated with a maintenance domain level from 0 through 7. Level allocation is based on the network hierarchy, where outer domains are assigned a higher level than the inner domains. Configure customer end points to have the highest maintenance domain level. The maintenance domain level is a mandatory parameter that indicates the nesting relationships between various maintenance domains. The level is embedded in each CFM frame. CFM messages within a given level are processed by MEPs at that same level.

To enable CFM on an Ethernet interface, you must configure maintenance domains, maintenance associations, and maintenance association end points (MEPs). Figure 45 on page 3554 shows the relationships among maintenance domains, maintenance association end points (MEPs), and maintenance intermediate points (MIPs) configured on a switch.
Performance management depends on the accurate measurement of service-level agreement (SLA) objective parameters, which can include bandwidth and reliability. In many cases, a service provider could be subject to penalties imposed by regulation, statute, or contract if network performance is not within the bounds established for the service. One key performance objective is delay, along with its close relative, delay variation (often called jitter). Some applications (such as bulk file transfer) will function just as well with high delays across the network and high delay variations, while other applications (such as voice) can function only with low and stable delays. Many networks invoke protocols or features available at Layer 3 (the packet layer) or higher to measure network delays and jitter link by link. However, when the network consists of many Ethernet links, there are few protocols and features available at Layer 2 (the frame layer) that allow routers and switches to measure frame delay and jitter. This is where the ability to configure and monitor Ethernet frame delay is helpful.

This topic includes:

- **Ethernet Frame Delay Measurements on page 3554**
- **Types of Ethernet Frame Delay Measurements on page 3555**
- **Limitations on page 3556**

**Ethernet Frame Delay Measurements**

You can perform Ethernet frame delay measurements (referred to as ETH-DM in Ethernet specifications) on Juniper Networks EX Series Ethernet Switches. This feature allows you to configure on-demand Operation, Administration, and Maintenance (OAM) statements for the measurement of frame delay and frame delay variation (jitter). You
can configure Ethernet frame delay measurement in either one-way or two-way (round-trip) mode to gather frame delay statistics simultaneously from multiple sessions. Ethernet frame delay measurement provides fine control to operators for triggering delay measurement on a given service and can be used to monitor SLAs.

Ethernet frame delay measurement also collects other useful information, such as worst and best case delays, average delay, and average delay variation. It supports software-assisted timestamping in the receive direction for delay measurements. It also provides runtime display of delay statistics when two-way delay measurement is triggered. Ethernet frame delay measurement records the last 100 samples collected per remote maintenance association end point (MEP) or per connectivity fault management (CFM) session. You can retrieve the history at any time using simple commands. You can clear all Ethernet frame delay measurement statistics and PDU counters. Ethernet frame delay measurement is fully compliant with the ITU-T Y.1731 (OAM Functions and Mechanisms for Ethernet-based Networks) specification.

Ethernet frame delay measurement uses the IEEE 802.1ag CFM infrastructure.

Generally, Ethernet frame delay measurements are made in a peer fashion from one MEP or CFM session to another. However, these measurements are not made to maintenance association intermediate points (MIPs).

For a complete description of Ethernet frame delay measurement, see the ITU-T Y.1731 Ethernet Service OAM topics in the Junos OS Network Interfaces Library for Routing Devices.

Types of Ethernet Frame Delay Measurements

There are two types of Ethernet frame delay measurements:

- One-way
- Two-way (round-trip)

For one-way Ethernet frame delay measurement, either MEP can send a request to begin a one-way delay measurement to its peer MEP. However, the statistics are collected only at the receiver MEP. This feature requires the clocks at the transmitting and receiving MEPs to be synchronized. If these clocks fall out of synchronization, only one-way delay variation and average delay variation values are computed correctly (and will, therefore, be valid). Use the show commands at the receiver MEP to display one-way delay statistics.

For two-way (round-trip) Ethernet frame delay measurement, either MEP can send a request to begin a two-way delay measurement to its peer MEP, which responds with timestamp information. Run-time statistics are collected and displayed at the initiator MEP. The clocks do not need to be synchronized at the transmitting and receiving MEPs. Junos OS supports timestamps in delay measurement reply (DMR) frames to increase the accuracy of delay calculations.

Use the show commands at the initiator MEP to display two-way delay statistics, and at the receiver MEP to display one-way delay statistics.

You can create an iterator profile to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for delay measurement or loss measurement.
**Limitations**

The following are some limitations with regard to using Ethernet frame delay measurement:

- Ethernet frame delay measurements are available only when distributed periodic packet management (PPM) is enabled.
- The statistics collected are lost after a graceful Routing Engine switchover (GRES).
- You can monitor only one session to the same remote MEP or MAC address.
- Accuracy is compromised when the system configuration changes (such as from reconfiguration). We recommend performing Ethernet frame delay measurements on a stable system.

**Related Documentation**

- Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) on page 3619
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620
- Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3623
- Triggering an Ethernet Frame Delay Measurement Session on a Switch on page 3622

**Uplink Failure Detection**

- Understanding Uplink Failure Detection on page 3556

**Understanding Uplink Failure Detection**

Uplink failure detection allows Juniper Networks EX Series Ethernet Switches to detect link failure on uplink interfaces and to propagate the failure to the downlink interfaces so that servers connected to those downlink interfaces can switch over to secondary interfaces.

Uplink failure detection supports network adapter teaming and provides network redundancy. In network adapter teaming, all the network interface cards (NICs) on a server are configured in a primary or secondary relationship and share the same IP address. When the primary link goes down, the server transparently shifts the connection to the secondary link. With uplink failure detection, the switch monitors uplink interfaces for link failures. When it detects a failure, it disables the downlink interfaces. When the server detects disabled downlink interfaces, it switches over to the secondary link to help ensure balanced traffic flow on switches.

This topic describes:

- Uplink Failure Detection Overview on page 3557
- Failure Detection Pair on page 3558
Uplink Failure Detection Overview

Uplink failure detection allows switches to monitor uplink interfaces to spot link failures. When a switch detects a link failure, it automatically disables the downlink interfaces in that group. The server that is connected to the disabled downlink interfaces triggers a network-adapter failover to a secondary link to avoid any information drop.

Figure 46 on page 3557 illustrates a typical setup for uplink failure detection.

Figure 46: Uplink Failure Detection Configuration on Switches

For uplink failure detection, you specify a group of uplink interfaces to be monitored and downlink interfaces to be brought down when an uplink fails. The downlink interfaces are bound to the uplink interfaces within the group. If all uplink interfaces in a group go down, then the switch brings down all downlink interfaces within that group. If any uplink interface returns to service, then the switch brings all downlink interfaces in that group back to service.

**NOTE:** Routed VLAN interfaces (RVIs) cannot be configured as uplink interfaces to be monitored.

The switch can monitor both physical-interface links and logical-interface links for uplink failures, but you must put the two types of interfaces in separate groups.

**NOTE:** To detect failure of logical interfaces, the server must run some high level protocol such as keepalives between the switch and the server.
failureDetectionPair

Uplink failure detection requires that you create groups that contain uplink interfaces and downlink interfaces. Each group includes one of each of the following:

- A link-to-monitor interface—The link-to-monitor interfaces specify the uplink interfaces the switch monitors. You can configure a maximum of 48 uplink interfaces as link-to-monitor in a group.

- A link-to-disable interface—The link-to-disable interfaces specify the downlink interfaces the switch disables when the switch detects an uplink failure. You can configure a maximum of 48 downlink interfaces as link-to-disable in a group.

The link-to-disable interfaces are bound to the link-to-monitor interfaces within the group. When a link-to-monitor interface returns to service, the switch automatically enables all link-to-disable interfaces in the group.

Related Documentation

- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618
CHAPTER 67

Configuration

- Configuration Examples on page 3559
- Configuration Tasks on page 3593
- Configuration Statements: SNMP on page 3623
- Configuration Statements: Analyzers and Port Mirroring on page 3700
- Configuration Statements: sFlow Technology on page 3707
- Configuration Statements: Ethernet OAM Connectivity Fault Management on page 3717
- Configuration Statements: Ethernet OAM Link Fault Management on page 3739
- Configuration Statements: RPM on page 3758
- Configuration Statements: Uplink Failure Detection on page 3778

Configuration Examples

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches on page 3580
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 3587
- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591

Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches

You can configure sFlow technology, designed for monitoring high-speed switched or routed networks, to continuously monitor traffic at wire speed on all interfaces simultaneously. You can specify sample rates for ingress and egress packets. sFlow data can be used to provide network traffic visibility information.
This example describes how to configure and use sFlow technology to monitor network traffic. Junos OS fully supports the sFlow standard described in RFC 3176, InMon Corporation’s sFlow: A Method for Monitoring Traffic in Switched and Routed Networks (see http://faqs.org/rfcs/rfc3176.html).

- Requirements on page 3560
- Overview and Topology on page 3560
- Configuration on page 3561
- Verification on page 3563

**Requirements**

This example uses the following hardware and software components:

- One EX Series switch
- Junos OS Release 9.3 or later for EX Series switches

**Overview and Topology**

sFlow technology is a statistical-sampling–based network monitoring technology for high-speed switched or routed networks. sFlow technology samples network packets and sends the samples to a monitoring station. You can specify sample rates for ingress and egress packets. The information gathered is used to create a network traffic visibility picture.

An sFlow monitoring system consists of an sFlow agent embedded in the switch and a centralized collector. The sFlow agent runs on the switch. It combines interface counters and flow samples and sends them across the network to the sFlow collector. Figure 47 on page 3561 depicts the basic elements of the sFlow system.
To configure sFlow technology, perform the following tasks:

**CLI Quick Configuration**

To quickly configure sFlow technology, copy the following commands and paste them into the switch terminal window:

```
[edit protocols]
set sflow collector 10.204.32.46 udp-port 5600
set sflow interfaces ge-0/0/0
set sflow polling-interval 20
set sflow sample-rate egress 1000
```

**Step-by-Step Procedure**

To configure sFlow technology:

1. Configure the IP address and UDP port of the collector:

   ```
   [edit protocols]
   user@switch# set sflow collector 10.204.32.46 udp-port 5600
   ```

   **NOTE:** You can configure a maximum of 4 collectors.

2. Enable sFlow technology on a specific interface:
[edit protocols sflow]
user@switch# set Interfaces (sFlow Monitoring Technology) ge-0/0/0

**NOTE:** You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.

You cannot enable sFlow technology on a link aggregation group (LAG) interface—that is, an aggregated Ethernet interface with a name such as ae0. You can enable sFlow technology on the member interfaces that make up the LAG.

3. Specify how often the sFlow agent polls the interface:

[edit protocols sflow]
user@switch# set polling-interval 20

**NOTE:** The polling interval can be specified as a global parameter also. Specify 0 if you do not want to poll the interface.

4. Specify the rate at which egress packets must be sampled:

[edit protocols sflow]
user@switch# set sample-rate egress 1000

**NOTE:** If you set only the egress sample rate, the ingress sample rate will be disabled.

**Results**

Check the results of the configuration:

[edit protocols sflow]
user@switch# show
polling-interval 20;
sample-rate egress 1000;
collector 10.204.32.46 {
  udp-port 5600;
}
interfaces ge-0/0/0.0;
Verification

To confirm that the configuration is correct, perform these tasks:

- Verifying That sFlow Technology Has Been Configured Properly on page 3563
- Verifying That sFlow Technology Is Enabled on the Intended Interface on page 3563
- Verifying the sFlow Collector Configuration on page 3564

**Verifying That sFlow Technology Has Been Configured Properly**

**Purpose** Verify that sFlow technology has been configured properly.

**Action** Use the `show sflow` command:

```
user@switch> show sflow
sFlow: Enabled
Sample limit: 300 packets/second
Polling interval: 20 seconds
Sample rate egress: 1:1000: Enabled
Sample rate ingress: 1:2048: Disabled
Agent ID: 10.204.96.222
```

**NOTE:** The sample limit cannot be configured and is set to 300 packets/second.

**Meaning** The output shows that sFlow technology is enabled and specifies the values for the sample limit, polling interval, and sample rate.

**Verifying That sFlow Technology Is Enabled on the Intended Interface**

**Purpose** Verify that sFlow technology is enabled on interfaces and display the sampling parameters.

**Action** Use the `show sflow interface` command:

```
user@switch> show sflow interface
Interface    Status     Sample rate   Adapted sample rate   Polling-interval
ge-0/0/0.0   Enabled    1000         2048                 20
```

**NOTE:** The sample limit cannot be configured and is set to 300 packets/second.

**Meaning** The output indicates that sFlow technology is enabled on the `ge-0/0/0.0` interface with an egress sample rate of 1000, a disabled ingress sample rate, a sampling limit of 300 packets per second and a polling interval of 20 seconds.
Verifying the sFlow Collector Configuration

Purpose
Verify the sFlow collector's configuration.

Action
Use the `show sflow collector` command:

```
user@switch> show sflow collector
```

<table>
<thead>
<tr>
<th>Collector address</th>
<th>Udp-port</th>
<th>No. of samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.204.32.46</td>
<td>5600</td>
<td>1000</td>
</tr>
<tr>
<td>10.204.32.76</td>
<td>3400</td>
<td>1000</td>
</tr>
</tbody>
</table>

Meaning
The output displays the IP address of the collectors and the UDP ports. It also displays the number of samples.

Related Documentation
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 3549

Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches

**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches. For ELS details, see Getting Started with Enhanced Layer 2 Software.

EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN

You can analyze the mirrored traffic by using a protocol analyzer application installed on a system connected to the local destination interface (or running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN).

This example describes how to configure local mirroring on an EX4300 switch. This example describes how to configure the switch to mirror traffic entering interfaces connected to employee computers to an analyzer output interface on the same switch.

- Requirements on page 3565
- Overview and Topology on page 3565
- Mirroring All Employee Traffic for Local Analysis on page 3566
• Mirroring Employee-to-Web Traffic for Local Analysis on page 3567
• Verification on page 3569

Requirements

This example uses the following hardware and software components:

• One EX4300 switch
• Junos OS Release 13.2X50-D10. or later for EX Series switches

Before you configure mirroring, be sure you have an understanding of mirroring concepts. For information about mirroring, see “Understanding Port Mirroring and Analyzers on EX4300 Switches” on page 3544.

Overview and Topology

This topic includes two examples that describe how to mirror traffic entering ports on the switch to a destination interface on the same switch (local mirroring). The first example shows how to mirror all traffic entering the ports connected to employee computers. The second example shows the same scenario, but includes a filter to mirror only the employee traffic going to the Web.

The interfaces ge-0/0/0 and ge-0/0/1 serve as connections for employee computers. The interface ge0/0/10 is reserved for analysis of mirrored traffic. Connect a PC running a protocol analyzer application to the analyzer output interface to analyze the mirrored traffic.

NOTE: Multiple ports mirrored to one interface can cause buffer overflow and dropped packets.

Both examples use the network topology shown in Figure 48 on page 3566.
To configure mirroring for all employee traffic for local analysis, perform these tasks:

**CLI Quick Configuration**

To quickly configure local mirroring for ingress traffic to the two ports connected to employee computers, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set interfaces ge-0/0/0 unit 0 family ethernet-switching
set interfaces ge-0/0/1 unit 0 family inet 192.1.1.1/24
set interfaces ge-0/0/10 unit 0 family ethernet-switching
set forwarding-options analyzer employee–monitor input ingress interface ge-0/0/0.0
set forwarding-options analyzer employee–monitor input ingress interface ge-0/0/1.0
set forwarding-options analyzer employee–monitor output interface ge-0/0/10.0
```

**Step-by-Step Procedure**

To configure an analyzer called `employee-monitor` and specify the input (source) interfaces and the analyzer output interface:

1. Configure each interface connected to employee computers as an input interface for the analyzer `employee-monitor`:
   ```plaintext
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
   ```

2. Configure the output analyzer interface for the analyzer `employee-monitor`. This will be the destination interface for the mirrored packets:
   ```plaintext
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

**Results**

Check the results of the configuration:

```plaintext
[edit]
user@switch> show
```
forwarding-options {
    analyzer employee-monitor {
        input {
            ingress {
                interface ge-0/0/0.0;
                interface ge-0/0/1.0;
            }
        }
        output {
            interface {
                ge-0/0/10.0;
            }
        }
    }
}

Mirroring Employee-to-Web Traffic for Local Analysis

To configure mirroring for employee to Web traffic, perform these tasks:

**CLI Quick Configuration**

To quickly configure local mirroring of traffic from the two ports connected to employee computers, filtering so that only traffic to the external Web is mirrored, copy the following commands and paste them into the switch terminal window:

```
[edit]
set forwarding-options port-mirroring instance employee--web--monitor output interface ge-0/0/10.0
set firewall family ethernet-switching filter watch-employee term employee-to-corp from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web then port-mirroring instance employee-web-monitor
set firewall family ethernet-switching filter watch-employee term employee-to-web then port-mirroring instance employee-web-monitor
set interfaces ge-0/0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces ge-0/0/1/0 unit 0 family ethernet-switching filter input watch-employee
```

**Step-by-Step Procedure**

To configure local mirroring of employee to Web traffic from the two ports connected to employee computers:

1. Configure the local analyzer interface:
   ```
   [edit interfaces]
   user@switch# set ge-0/0/10 unit 0 family ethernet-switching
   ```
2. Configure the **employee-web-monitor** output instance (the input to the instance comes from the action of the filter):
   ```
   [edit forwarding-options port-mirroring]
   user@switch# set instance employee-web-monitor output interface ge-0/0/10.0
   ```
3. Configure a firewall filter called **watch-employee** to send mirrored copies of employee requests to the Web to the **employee-web-monitor** instance. Accept all traffic to and from the corporate subnet (destination or source address of 192.0.2.16/28). Send mirrored copies of all packets destined for the Internet (**destination port 80**) to the **employee-web-monitor** instance.
   ```
   [edit firewall family ethernet-switching]
   ```
4. Apply the **watch-employee** filter to the appropriate ports:

```junos
[edit interfaces]
user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```

**Results**

Check the results of the configuration:

```junos
[edit]
user@switch> show
forwarding-options {
    port-mirroring {
        instance {
            employee-web-monitor {
                family ethernet-switching {
                    output {
                        interface ge-0/0/10.0;
                    }
                }
            }
        }
    }
}

firewall {
    family ethernet-switching {
        filter watch-employee {
            term employee-to-corp {
                from {
                    destination-address 192.0.2.16/28;
                    source-address 192.0.2.16/28;
                }
                then accept {
                }
            }
            term employee-to-web {
                from {
                    destination-port 80;
                }
                then port-mirroring-instance employee-web-monitor;
            }
        }
    }
}

interfaces {
    ge-0/0/0 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan members [employee-vlan, voice-vlan];
            }
        }
    }
```
input watch-employee;
}
}
}
}
ge-0/0/1 {
    family ethernet-switching {
        filter {
            input watch-employee;
        }
    }
}
}

Verification
To confirm that the configuration is correct, perform these tasks:

- Verifying That the Analyzer Has Been Correctly Created on page 3569
- Verifying That The Port-Mirroring Instance Is Configured Properly on page 3569

Verifying That the Analyzer Has Been Correctly Created

Purpose
Verify that the analyzer employee-monitor or employee-web-monitor has been created on the switch with the appropriate input interfaces, and appropriate output interface.

Action
You can use the `show analyzer` command to verify that the analyzer is configured properly.

```
user@switch> show forwarding-options analyzer
Analyzer name : employee-monitor
Mirror rate : 1
Maximum packet length : 0
State : up
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
Output interface : ge-0/0/10.0
```

Meaning
This output shows that the analyzer employee-monitor has a ratio of 1 (mirroring every packet, the default setting), the maximum size of the original packet that was mirrored (0 indicates the entire packet), the state of the configuration (is up indicates that the analyzer is mirroring the traffic entering the ge-0/0/0, and ge-0/0/1 interfaces, and sending the mirrored traffic to the ge-0/0/10 interface). If the state of the output interface is down or if the output interface is not configured, the value of state will be down and the analyzer will not be programmed for mirroring.

Verifying That The Port-Mirroring Instance Is Configured Properly

Purpose
Verify that the port-mirroring instance employee-web-monitor has been configured properly on the switch with the appropriate input interfaces.
Action

You can verify that the port-mirroring instance is configured properly by using the `show forwarding-options port-mirroring` command.

```
user@switch> show forwarding-options port-mirroring
Instance Name: employee-web-monitor
    Instance Id: 3
    Input parameters:
        Rate              : 1
        Run-length        : 0
        Maximum-packet-length : 0
    Output parameters:
        Family    State     Destination          Next-hop
        ethernet-switching  up        ge-0/0/10.0
```

Meaning

This output shows that the `employee-web-monitor` instance has a ratio of 1 (mirroring every packet, the default), the maximum size of the original packet that was mirrored (0 indicates an entire packet), the state of the configuration is up and port mirroring is programmed, and that mirrored traffic from the firewall filter action is sent out on interface `ge-0/0/10.0`. If the state of the output interface is down or if the interface is not configured, the value for state will be down and port mirroring will not be programmed for mirroring.

Related Documentation

- [Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches](#)
- [Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure)](#)
- [Configuring Port Mirroring to Analyze Traffic (J-Web Procedure)](#)
- [Understanding Port Mirroring and Analyzers on EX4300 Switches](#)

Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see “Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches” on page 3570. For ELS details see: Getting Started with Enhanced Layer 2 Software.

EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX4300 switches

You can analyze the mirrored traffic by using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.
This topic includes two related examples that describe how to mirror traffic entering ports on the switch to the remote-analyzer VLAN so that you can perform analysis from a remote monitoring station. The first example shows how to mirror all traffic entering the ports connected to employee computers. The second example shows the same scenario but includes a filter to mirror only the employee traffic going to the Web.

**BEST PRACTICE:** Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring sessions when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by using firewall filters.

This example describes how to configure remote mirroring:

- Requirements on page 3571
- Overview and Topology on page 3571
- Mirroring All Employee Traffic for Remote Analysis on page 3572
- Mirroring Employee-to-Web Traffic for Remote Analysis on page 3575
- Verification on page 3579

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 13.2X50-D10 or later for EX Series switches
- An EX4300 switch connected to another EX4300 switch

The diagram shows an EX4300 Virtual Chassis connected to an EX4300 destination switch.

Before you configure remote mirroring, be sure that:

- You have an understanding of mirroring concepts.
- The interfaces that the analyzer will use as input interfaces have been configured on the switch.

**Overview and Topology**

This topic includes two related examples that describe how to configure mirroring to the remote-analyzer VLAN so that analysis can be performed from a remote monitoring station. The first example shows how to configure a switch to mirror all traffic from employee computers. The second example shows the same scenario, but the setup includes a filter to mirror only the employee traffic going to the Web.

Figure 49 on page 3572 shows the network topology for both these example scenarios.
In this example:

a. Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 3 interface (both interfaces on the source switch) that serve as connections for employee computers.

b. Interface ge-0/0/10 is a Layer 2 interface that connects the source switch to the destination switch.

c. Interface ge-0/0/5 is a Layer 2 interface that connects the destination switch to the remote monitoring station.

d. VLAN remote-analyzer is configured on all switches in the topology to carry the mirrored traffic.

**Mirroring All Employee Traffic for Remote Analysis**

To configure an analyzer for remote traffic analysis for all incoming and outgoing employee traffic, perform these tasks:

- **CLI Quick Configuration**

  To quickly configure an analyzer for remote traffic analysis for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

  - Copy and paste the following commands in the source switch terminal window:

    ```
    [edit]
    set vlans remote-analyzer vlan-id 999
    set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
    set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
    set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0/0.0
    set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
    set forwarding-options analyzer employee-monitor input egress interface ge-0/0/0/0.0
    set forwarding-options analyzer employee-monitor input egress interface ge-0/0/1.0
    set forwarding-options analyzer employee-monitor output vlan remote-analyzer
    ```

  - Copy and paste the following commands in the destination switch terminal window:
Step-by-Step Procedure

1. On the source switch:
   - Configure the VLAN ID for the remote-analyzer VLAN:
     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```
   - Configure the interface on the network port connected to the destination switch for trunk mode and associate it with the remote-analyzer VLAN:
     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```
   - Configure the employee-monitor analyzer:
     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@switch# set instance employee-monitor input egress interface ge-0/0/0.0
     user@switch# set instance employee-monitor input egress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor output vlan remote-analyzer
     ```
2. On the destination switch:
   - Configure the VLAN ID for the remote-analyzer VLAN:
     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```
   - Configure the interface on the destination switch for trunk mode and associate it with the remote-analyzer VLAN:
     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```
   - Configure the interface connected to the destination switch for trunk mode:
     ```
     [edit interfaces]
     user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
     ```
   - Configure the employee-monitor analyzer:
     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
     user@switch# set analyzer employee-monitor output interface ge-0/0/5.0
     ```

Results

Check the results of the configuration on the source switch:

```
[edit]
user@switch> show
forwarding-options {
 analyzer employee-monitor {
```
input {
    ingress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
    }
    egress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
    }
}
output {
    vlan {
        remote-analyzer;
    }
}
}

interfaces {
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members 999;
                }
            }
        }
    }
}

vlans {
    remote-analyzer {
        vlan-id 999;
        interface {
            ge-0/0/10.0
        }
    }
}
}

Check the results of the configuration on the destination switch:

[edit]
user@switch> show
interfaces {
    ge0/0/5 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
            }
        }
    }
    ge-0/0/10 {
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
            }
        }
    }
}
Mirroring Employee-to-Web Traffic for Remote Analysis

To configure port mirroring for remote traffic analysis of employee-to-Web traffic, perform these tasks:

**CLI Quick Configuration**

To quickly configure port mirroring to mirror employee traffic to the external Web, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch terminal window:

```plaintext
[edit]
set forwarding-options port-mirroring instance employee-web-monitor output vlan 999
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
set firewall family ethernet-switching filter watch-employee term employee-to-corp from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp from source-address 192.0.2.16/28
set firewall family ethernet-switching filter watch-employee term employee-to-corp then accept
set firewall family ethernet-switching filter watch-employee term employee-to-web from destination-port 80
set firewall family ethernet-switching filter watch-employee term employee-to-web then port-mirror-instance employee-web-monitor
set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
set interfaces ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
```
• Copy and paste the following commands in the destination switch terminal window:

```plaintext
[edit]
set vlans remote-analyzer vlan-id 999
set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
set interfaces ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk
set forwarding-options analyzer employee-web-monitor input ingress vlan remote-analyzer
set forwarding-options analyzer employee-web-monitor output interface ge-0/0/5.0
```

**Step-by-Step Procedure**

To configure port mirroring of all traffic from the two ports connected to employee computers to the remote-analyzer VLAN for use from a remote monitoring station:

1. On the source switch:
   - Configure the **employee-web-monitor** port mirroring instance:
     ```plaintext
     [edit ]
     user@switch# set interfaces ge-0/0/10 unit 0 family ethernet-switching port mode trunk
     user@switch# set forwarding-options port-mirroring instance employee-web-monitor output vlan 999
     ```
   - Configure the VLAN ID for the remote-analyzer VLAN:
     ```plaintext
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```
   - Configure the interface to associate it with the remote-analyzer VLAN:
     ```plaintext
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```
   - Configure the firewall filter called **watch-employee**:
     ```plaintext
     [edit firewall family ethernet-switching]
     user@switch# set filter (Firewall Filters) watch-employee term employee-to-corp from destination-address 192.0.2.16/28
     user@switch# set filter watch-employee term employee-to-corp from source-address 192.0.2.16/28
     user@switch# set filter watch-employee term employee-to-corp then accept
     user@switch# set filter watch-employee term employee-to-web from destination-port 80
     user@switch# set filter watch-employee term employee-to-web then port-mirror-instance employee-web-monitor
     ```
   - Apply the firewall filter to the employee interfaces:
     ```plaintext
     [edit interfaces]
     user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input watch-employee
     user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input watch-employee
     ```
2. On the destination switch:
   - Configure the VLAN ID for the remote-analyzer VLAN:
     ```plaintext
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```
   - Configure the interface on the destination switch for trunk mode and associate it with the remote-analyzer VLAN:
     ```plaintext
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/5 unit 0 family ethernet-switchingvlan members 999
     ```
   - Configure the interface connected to the destination switch for trunk mode:
[edit interfaces]
user@switch# set ge-0/0/5 unit 0 family ethernet-switching interface-mode trunk

- Configure the employee-monitor analyzer:

[edit forwarding-options port-mirroring]
user@switch# set instance employee-web-monitor input ingress vlan remote-analyzer
user@switch# set instance employee-web-monitor output interface ge-0/0/5.0

Results Check the results of the configuration on the source switch:

[edit]
user@switch> show
interfaces {
  ge-0/0/10 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members remote-analyzer;
        }
      }
    }
  }
  ge-0/0/0 {
    unit 0 {
      family ethernet-switching {
        filter {
          input watch-employee;
        }
      }
    }
  }
  ge-0/0/1 {
    unit 0 {
      family ethernet-switching {
        filter {
          input watch-employee;
        }
      }
    }
  }
}
firewall {
  family ethernet-switching {
    filter watch-employee {
      term employee-to-corp {
        from {
          source-address {
            192.0.2.16/28;
          }
          destination-address {
            192.0.2.16/28;
          }
        }
        then accept;
      }
    }
  }
}
term employee-to-web {
  from {
    destination-port 80;
  }
  then port-mirror-instance employee-web-monitor;
}
}
}
forwarding-options {
  analyzer employee-web-monitor {
    output {
      vlan {
        999;
      }
    }
  }
  vlans {
    remote-analyzer {
      vlan-id 999;
    }
  }
}
vlans {
  remote-analyzer {
    vlan-id 999;
  }
}
}
Check the results of the configuration on the destination switch:

[edit]
user@switch> show
vlans {
  remote-analyzer {
    vlan-id 999;
  }
}
interfaces {
  ge-0/0/10 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
        vlan {
          members remote-analyzer;
        }
      }
    }
  }
  ge-0/0/5 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
      }
    }
  }
}
forwarding-options {
  port-mirroring {
    instance employee-web-monitor {
      input {
      }
      ingress [
Verify that the analyzer named `employee-monitor` or `employee-web-monitor` has been created on the switch with the appropriate input interfaces and appropriate output interface.

You can verify the analyzer is configured as expected by using the `show forwarding-options analyzer` command. To view previously created analyzers that are disabled, go to the J-Web interface.

To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switch, run the `show analyzer` command on the source switch. The following output is displayed for this configuration example:

```
user@switch> show forwarding-options analyzer
Analyzer name            : employee-monitor
Mirror rate              : 1
Maximum packet length    : 0
State                    : up
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
Egress monitored interfaces : ge-0/0/0.0
Egress monitored interfaces : ge-0/0/1.0
Output VLAN              : default-switch/remote-analyzer
```

This output shows that the `employee-monitor` instance has a ratio of 1 (mirroring every packet, the default), the maximum size of the original packet that was mirrored (0 indicates the entire packet), the state of the configuration is up (which indicates the proper state and that the analyzer is programmed, and is mirroring the traffic entering `ge-0/0/0/0` and `ge-0/0/1.0` and is sending the mirrored traffic to the VLAN called `remote-analyzer`). If the state of the output interface is down or if the output interface is not configured, the value of state will be down and the analyzer will not be programmed for mirroring.

- **Related Documentation**
  - Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX4300 switches

You can analyze the mirrored traffic by using a protocol analyzer application running on a remote monitoring station if you are sending mirrored traffic to an analyzer VLAN.

This topic includes an example that describes how to mirror traffic entering ports on the switch to the remote-analyzer VLAN through a transit switch, so that you can perform analysis from a remote monitoring station.

**BEST PRACTICE:** Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring sessions when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by using firewall filters.

This example describes how to configure remote mirroring through a transit switch:
Requirements

This example uses the following hardware and software components:

• An EX4300 switch connected to another EX4300 switch through a third EX4300 switch
• Junos OS Release 13.2X50-D10 or later for EX Series switches

Before you configure remote mirroring, be sure that:

• You have an understanding of mirroring concepts.
• The interfaces that the analyzer will use as input interfaces have been configured on the switch.

Overview and Topology

This example describes how to mirror traffic entering ports on the switch to the remote-analyzer VLAN through a transit switch so that you can perform analysis from a remote monitoring station. The example shows how to configure a switch to mirror all traffic from employee computers to a remote analyzer.

In this configuration, an analyzer session is required on the destination switch to mirror incoming traffic from the analyzer VLAN to the egress interface to which the remote monitoring station is connected. You must disable MAC learning on the transit switch for the remote-analyzer VLAN so that MAC learning is disabled for all member interfaces of the remote-analyzer VLAN on the transit switch.

Figure 50 on page 3581 shows the network topology for this example.

Figure 50: Remote Mirroring Through a Transit Switch Network—Sample Topology
In this example:

- Interface ge-0/0/0 is a Layer 2 interface, and interface ge-0/0/1 is a Layer 3 interface (both interfaces on the source switch) that serve as connections for employee computers.
- Interface ge-0/0/10 is a Layer 2 interface that connects to the transit switch.
- Interface ge-0/0/11 is a Layer 2 interface on the transit switch.
- Interface ge-0/0/12 is a Layer 2 interface on the transit switch and connects to the destination switch.
- Interface ge-0/0/13 is a Layer 2 interface on the destination switch.
- Interface ge-0/0/14 is a Layer 2 interface on the destination switch and connects to the remote monitoring station.
- VLAN remote-analyzer is configured on all switches in the topology to carry the mirrored traffic.

**Mirroring All Employee Traffic for Remote Analysis Through a Transit Switch**

To configure mirroring for remote traffic analysis through a transit switch, for all incoming and outgoing employee traffic, perform these tasks:

**CLI Quick Configuration**

To quickly configure mirroring for remote traffic analysis through a transit switch, for incoming and outgoing employee traffic, copy the following commands and paste them into the switch terminal window:

- Copy and paste the following commands in the source switch (monitored switch) terminal window:
  ```
  [edit]
  set vlans remote-analyzer vlan-id 999
  set interfaces ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
  set interfaces ge-0/0/10 unit 0 family ethernet-switching vlan members 999
  set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/0.0
  set forwarding-options analyzer employee-monitor input ingress interface ge-0/0/1.0
  set forwarding-options analyzer employee-monitor output vlan remote-analyzer
  ```
- Copy and paste the following commands in the transit switch window:
  ```
  [edit]
  set vlans remote-analyzer vlan-id 999
  set interfaces ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
  set vlans remote-analyzer interface ge-0/0/11
  set interfaces ge-0/0/12 unit 0 family ethernet-switching interface-mode trunk
  set vlans remote-analyzer interface ge-0/0/12
  set vlans remote-analyzer no-mac-learning
  ```
- Copy and paste the following commands in the destination switch window:
  ```
  [edit]
  set vlans remote-analyzer vlan-id 999
  set interfaces ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
  set vlans remote-analyzer interface ge-0/0/13 ingress
  set interfaces ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
  ```
To configure remote mirroring through a transit switch:

1. **On the source switch:**
   - Configure the VLAN ID for the `remote-analyzer` VLAN:
     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```
   - Configure the interfaces on the network port connected to transit switch for trunk mode and associate it with the `remote-analyzer` VLAN:
     ```
     [edit interfaces]
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set ge-0/0/10 unit 0 family ethernet-switching vlan members 999
     ```
   - Configure the `employee-monitor` analyzer:
     ```
     [edit forwarding-options]
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/0.0
     user@switch# set analyzer employee-monitor input egress interface ge-0/0/1.0
     user@switch# set analyzer employee-monitor output vlan remote-analyzer
     ```

2. **On the transit switch:**
   - Configure the VLAN ID for the `remote-analyzer` VLAN:
     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```
   - Configure the `ge-0/0/11` interface for trunk mode, associate it with the `remote-analyzer` VLAN:
     ```
     [edit interfaces]
     user@switch# set ge-0/0/11 unit 0 family ethernet-switching interface-mode trunk
     ```
   - Configure the `ge-0/0/12` interface for trunk mode, associate it with the `remote-analyzer` VLAN, and set the interface for egress traffic only:
     ```
     [edit interfaces]
     user@switch# set ge-0/0/12 unit 0 family ethernet-switching interface-mode trunk
     user@switch# set vlans remote-analyzer interface ge-0/0/12
     ```
   - Configure the `no-mac-learning` option for the `remote-analyzer` VLAN to disable MAC learning on all interfaces that are members of the `remote-analyzer` VLAN:
     ```
     [edit interfaces]
     user@switch# set vlans remote-analyzer no-mac-learning
     ```

3. **On the destination switch:**
   - Configure the VLAN ID for the `remote-analyzer` VLAN:
     ```
     [edit vlans]
     user@switch# set remote-analyzer vlan-id 999
     ```
   - Configure the `ge-0/0/13` interface for trunk mode, associate it with the `remote-analyzer` VLAN, and set the interface for ingress traffic only:
     ```
     [edit interfaces]
     user@switch# set ge-0/0/13 unit 0 family ethernet-switching interface-mode trunk
     ```
user@switch# set vlans remote-analyzer interface ge-0/0/13 ingress
• Configure the interface connected to the remote monitoring station for trunk mode:
  [edit interfaces]
user@switch# set ge-0/0/14 unit 0 family ethernet-switching interface-mode trunk
• Configure the employee-monitor analyzer:
  [edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress vlan remote-analyzer
user@switch# set analyzer employee-monitor output interface ge-0/0/14.0

Results
Check the results of the configuration on the source switch:

[edit]
user@switch> show forwarding-options {
  analyzer employee-monitor {
    input {
      ingress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
      }
      egress {
        interface ge-0/0/0.0;
        interface ge-0/0/1.0;
      }
    }
    output {
      vlan {
        remote-analyzer;
      }
    }
  }
  vlans {
    remote-analyzer {
      vlan-id 999;
    }
  }
  interfaces {
    ge-0/0/10 {
      unit 0 {
        family ethernet-switching {
          interface-mode trunk;
          vlan {
            member 999;
          }
        }
      }
    }
  }
}
Check the results of the configuration on the transit switch:

[edit]
user@switch> show vlans {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/11.0 {
      }
      ge-0/0/12.0 {
      }
    }
    no-mac-learning;
  }
}

interfaces {
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
      }
    }
  }
  ge-0/0/12 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
      }
    }
  }
}

Check the results of the configuration on the destination switch:

[edit]
user@switch> show vlans {
  remote-analyzer {
    vlan-id 999;
    interface {
      ge-0/0/13.0 {
        ingress;
      }
    }
  }
}

interfaces {
  ge-0/0/13 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
      }
    }
  }
  ge-0/0/14 {
    unit 0 {
      family ethernet-switching {
        interface-mode trunk;
      }
    }
  }
}
forwarding-options {
  analyzer employee-monitor {
    input {
      ingress {
        vlan remote-analyzer;
      }
    }
    output {
      interface {
        ge-0/0/14.0;
      }
    }
  }
}

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Analyzer Has Been Correctly Created on page 3586

**Verifying That the Analyzer Has Been Correctly Created**

**Purpose**

Verify that the analyzer named `employee-monitor` has been created on the switch with the appropriate input interfaces and the appropriate output interface.

**Action**

You can verify whether the analyzer is configured as expected by using the `show analyzer` command. To view previously created analyzers that are disabled, go to the J-Web interface.

To verify that the analyzer is configured as expected while monitoring all employee traffic on the source switch, run the `show analyzer` command on the source switch. The following output is displayed for this example configuration:

```
user@switch> show forwarding-options analyzer
Analyzer name : employee-monitor
  Mirror rate : 1
  Maximum packet length : 0
  State : up
  Ingress monitored interfaces : ge-0/0/0.0
  Ingress monitored interfaces : ge-0/0/1.0
  Egress monitored interfaces : ge-0/0/0.0
  Egress monitored interfaces : ge-0/0/1.0
  Output vlan : default-switch/remote-analyzer
```

**Meaning**

This output shows that the `employee-monitor` analyzer has a ratio of 1 (mirroring every packet, the default), is mirroring the traffic entering ge-0/0/0 and ge-0/0/1, and sending the mirrored traffic to the analyzer `remote-analyzer`.
Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches

Ethernet interfaces on EX Series switches and Junos OS for EX Series switches support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM).

This example describes how to enable and configure OAM CFM on a Gigabit Ethernet interface:

- Requirements on page 3587
- Overview and Topology on page 3587
- Configuring Ethernet OAM Connectivity Fault Management on Switch 1 on page 3587
- Configuring Ethernet OAM Connectivity Fault Management on Switch 2 on page 3588
- Verification on page 3590

Requirements

This example uses the following hardware and software components:

- Junos OS Release 10.2 or later for EX Series switches
- Two EX Series switches connected by a point-to-point Gigabit Ethernet link

Overview and Topology

CFM can be used to monitor the physical link between two switches. In the following example, two switches are connected by a point-to-point Gigabit Ethernet link. The link between these two switches is monitored using CFM.

Configuring Ethernet OAM Connectivity Fault Management on Switch 1

To quickly configure Ethernet OAM CFM, copy the following commands and paste them into the switch terminal window:

```cli
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]
set name-format character-string
set maintenance-domain private level 0
set maintenance-association private-ma
set continuity-check hold-interval 1s
```
**Step-by-Step Procedure**

To enable and configure OAM CFM on switch 1:

1. Specify the maintenance domain name format:
   
   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain]
   user@switch1# set name-format character-string
   ```

2. Specify the maintenance domain name and the maintenance domain level:
   
   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@switch1# set maintenance-domain private level 0
   ```

3. Create a maintenance association:
   
   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain private]
   user@switch1# set maintenance-association private-ma
   ```

4. Enable the continuity check protocol and specify the continuity check hold interval:
   
   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain private maintenance-association private-ma]
   user@switch1# set continuity-check hold-interval 1s
   ```

5. Configure the maintenance association end point (MEP):
   
   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain private maintenance-association private-ma]
   user@switch1# set mep 100 interface ge-1/0/1 auto-discovery direction down
   ```

**Results**

Check the results of the configuration.

```
[edit]
user@switch1 > show
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        maintenance-domain private {
          level 0;
          maintenance-association private-ma {
            continuity-check {
              interval 1s;
            }
            mep 100 {
              interface ge-1/0/1;
              auto-discovery;
              direction down;
            }
          }
        }
      }
    }
  }
}
```

---

**CLI Quick Configuration**

To quickly configure Ethernet OAM CFM, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain]
set name-format character-string
```
Step-by-Step Procedure

The configuration on switch 2 mirrors that on switch 2.

1. Specify the maintenance domain name format:
   
   \[
   \text{set name-format character-string} \\
   \text{[edit protocols oam ethernet connectivity-fault-management]} \\
   \text{user@switch2# set name-format character-string} \\
   \]

2. Specify the maintenance domain name and the maintenance domain level:
   
   \[
   \text{set maintenance-domain private level 0} \\
   \text{[edit protocols oam ethernet connectivity-fault-management]} \\
   \text{user@switch2# set maintenance-domain private level 0} \\
   \]

3. Create a maintenance association:
   
   \[
   \text{set maintenance-association private-ma} \\
   \text{[edit protocols oam ethernet connectivity-fault-management maintenance-domain private]} \\
   \text{user@switch2# set maintenance-association private-ma} \\
   \]

4. Enable the continuity check protocol and specify the continuity check hold interval:
   
   \[
   \text{set continuity-check hold-interval 1s} \\
   \text{[edit protocols oam ethernet connectivity-fault-management maintenance-domain private maintenance-association private-ma]} \\
   \text{user@switch2# set continuity-check hold-interval 1s} \\
   \]

5. Configure the maintenance association end point (MEP)
   
   \[
   \text{set mep 200 interface ge-0/2/5 auto-discovery direction down} \\
   \text{[edit protocols oam ethernet connectivity-fault-management maintenance-domain private maintenance-association private-ma]} \\
   \text{user@switch2# set mep 200 interface ge-0/2/5 auto-discovery direction down} \\
   \]

Results

Check the results of the configuration.

\[
\text{[edit]} \\
\text{user@switch2 > show} \\
\text{protocols { 
  oam { 
    ethernet { 
      connectivity-fault-management { 
        maintenance-domain private { 
          level 0; 
        maintenance-association private-ma { 
          continuity-check { 
            interval 1s; 
          } 
          mep 200 { 
            interface ge-0/2/5; 
            auto-discovery; 
            direction down; 
          } 
        } 
      } 
    } 
  } 
} 
\]
Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That OAM CFM Has Been Configured Properly on page 3590

**Verifying That OAM CFM Has Been Configured Properly**

**Purpose**
 Verify that OAM CFM has been configured properly.

**Action**
 Use the `show oam ethernet connectivity-fault-management interfaces detail` command:

```
user@switch1# show oam ethernet connectivity-fault-management interfaces detail
```

**Sample Output**

```
Interface name: ge-1/0/1.0, Interface status: Active, Link status: Up
Maintenance domain name: private, Format: string, Level: 0
Maintenance association name: private-ma, Format: string
Continuity-check status: enabled, Interval: 1ms, Loss-threshold: 3 frames
MEP identifier: 100, Direction: down, MAC address: 00:90:69:0b:4b:94
MEP status: running
Defects:
  Remote MEP not receiving CCM : no
  Erroneous CCM received : yes
  Cross-connect CCM received : no
  RDI sent by some MEP : yes
Statistics:
  CCMs sent : 76
  CCMs received out of sequence : 0
  LBMs sent : 0
  Valid in-order LBRs received : 0
  Valid out-of-order LBRs received : 0
  L BRs received with corrupted data : 0
  L BRs sent : 0
  L TMs sent : 0
  L TMs received : 0
  L TRs sent : 0
  L TRs received : 0
Sequence number of next LTM request : 0
Remote MEP count: 2
Identifier MAC address State Interface
2001 00:90:69:0b:7f:71 ok ge-0/2/5.0
```

**Meaning**
 When the output displays that continuity-check status is **enabled** and displays details of the remote MEP, it means that connectivity fault management (CFM) has been configured properly.

**Related Documentation**
- Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 3553
- Junos OS Network Interfaces Configuration Guide
Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches

Junos OS for EX Series switches allows the Ethernet interfaces on these switches to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters.

This example describes how to enable and configure OAM LFM on a Gigabit Ethernet interface:

- Requirements on page 3591
- Overview and Topology on page 3591
- Configuring Ethernet OAM Link Fault Management on Switch 1 on page 3591
- Configuring Ethernet OAM Link Fault Management on Switch 2 on page 3592
- Verification on page 3593

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.4 or later for EX Series switches
- Two EX3200 or EX4200 switches connected directly

Overview and Topology

Junos OS for EX Series switches allows the Ethernet interfaces on these switches to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters.

This example uses two EX4200 switches connected directly. Before you begin configuring Ethernet OAM LFM on two switches, connect the two switches directly through a trunk interface.

Configuring Ethernet OAM Link Fault Management on Switch 1

CLI Quick Configuration

To quickly configure Ethernet OAM LFM, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet link-fault-management]
set interface ge-0/0/0
set interface ge-0/0/0 link-discovery active
set interface ge-0/0/0 pdu-interval 800
set interface ge-0/0/0 remote-loopback
```

Step-by-Step Procedure

To configure Ethernet OAM LFM on switch 1:

1. Enable IEEE 802.3ah OAM support on an interface:

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface (OAM LFM) ge-0/0/0
```
2. Specify that the interface initiates the discovery process by configuring the link discovery mode to **active**:

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface ge-0/0/0 link-discovery active
```

3. Set the periodic OAM PDU-sending interval (in milliseconds) to 800 on switch 1:

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface pdu-interval 800
```

4. Set a remote interface into loopback mode so that all frames except OAM PDUs are looped back without any changes made to the frames. Ensure that the remote DTE supports remote loopback mode. To set the remote DTE in loopback mode:

```
[edit protocols oam ethernet link-fault-management]
user@switch1# set interface ge-0/0/0.0 remote-loopback
```

### Results

Check the results of the configuration:

```
[edit]
user@switch1# show
protocols {
oam {
ethernet {
link-fault-management {
interface ge-0/0/0 {
pdu-interval 800;
link-discovery active;
remote-loopback;
}
}
}
```

---

**Configuring Ethernet OAM Link Fault Management on Switch 2**

**CLI Quick Configuration**

To quickly configure Ethernet OAM LFM on switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit protocols oam ethernet link-fault-management ]
set interface ge-0/0/1
set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

**Step-by-Step Procedure**

To configure Ethernet OAM LFM on switch 2:

1. Enable OAM on the peer interface on switch 2:

```
[edit protocols oam ethernet link-fault-management]
user@switch2# set interface ge-0/0/1
```

2. Enable remote loopback support for the local interface:

```
[edit protocols oam ethernet link-fault-management]
user@switch2# set interface ge-0/0/1 negotiation-options allow-remote-loopback
```

### Results

Check the results of the configuration:

```
[edit]
```
Verification

Verifying That OAM LFM Has Been Configured Properly

Purpose

Verify that OAM LFM has been configured properly.

Action

Use the `show oam ethernet link-fault-management` command:

```
user@switch1# show oam ethernet link-fault-management
```

Sample Output

```
Interface: ge-0/0/0.0
Status: Running, Discovery state: Send Any
Peer address: 00:19:e2:50:3b:e1
Flags: Remote-Stable Remote-State-Valid Local-Stable 0x50
Remote entity information:
  Remote MUX action: forwarding, Remote parser action: forwarding
  Discovery mode: active, Unidirectional mode: unsupported
  Remote loopback mode: supported, Link events: supported
  Variable requests: unsupported
```

Meaning

When the output displays the MAC address and the discover state is **Send Any**, it means that OAM LFM has been configured properly.

Related Documentation

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
- Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 3551

Configuration Tasks

- Configuring SNMP (J-Web Procedure) on page 3594
- Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure) on page 3597
- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 3601
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
- Configuring Real-Time Performance Monitoring (J-Web Procedure) on page 3604
Configuring the Interface for RPM Timestamping for Client/Server on an EX Series Switch (CLI Procedure) on page 3611

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612

Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618

Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) on page 3619

Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620

Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621

Triggering an Ethernet Frame Delay Measurement Session on a Switch on page 3622

Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3623

Configuring SNMP (J-Web Procedure)

You can use the J-Web interface to define system identification information, create SNMP communities, create SNMP trap groups, and configure health monitor options for EX Series switches.

To configure SNMP features:

1. Select Configure > Services > SNMP.
2. Enter information into the configuration page for SNMP as described in Table 433 on page 3594.
3. To apply the configuration click Apply.

NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

Table 433: SNMP Configuration Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact Information</td>
<td>Free-form text string that specifies an administrative contact for the system.</td>
<td>Type contact information for the administrator of the system (such as name and phone number).</td>
</tr>
<tr>
<td>System Description</td>
<td>Free-form text string that specifies a description for the system.</td>
<td>Type information that describes the system</td>
</tr>
</tbody>
</table>
Table 433: SNMP Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Engine ID</td>
<td>Provides an administratively unique identifier of an SNMPv3 engine for system identification. The local engine ID contains a prefix and a suffix. The prefix is formatted according to specifications defined in RFC 3411. The suffix is defined by the local engine ID. Generally, the local engine ID suffix is the MAC address of Ethernet management port 0.</td>
<td>Type the MAC address of Ethernet management port 0.</td>
</tr>
<tr>
<td>System Location</td>
<td>Free-form text string that specifies the location of the system.</td>
<td>Type location information for the system (lab name or rack name, for example).</td>
</tr>
<tr>
<td>System Override Name</td>
<td>Free-form text string that overrides the system hostname.</td>
<td>Type the hostname of the system.</td>
</tr>
</tbody>
</table>

**Communities**

To add a community, click **Add**

<table>
<thead>
<tr>
<th>Community Name</th>
<th>Specifies the name of the SNMP community.</th>
<th>Type the name of the community being added.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>Specifies the type of authorization (either read-only or read-write) for the SNMP community being configured.</td>
<td>Select the authorization (either read-only or read-write) from the list.</td>
</tr>
</tbody>
</table>

**Traps**

To add a trap group, click **Add**.

| Trap Group Name | Specifies the name of the SNMP trap group being configured. | Type the name of the group being added.                                      |
### Table 433: SNMP Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories</td>
<td>Specifies which trap categories are added to the trap group being configured.</td>
<td>• To generate traps for authentication failures, select <strong>Authentication</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps for chassis and environment notifications, select <strong>Chassis</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps for configuration changes, select <strong>Configuration</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps for link-related notifications (up-down transitions), select <strong>Link</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps for remote operation notifications, select <strong>Remote operations</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps for remote network monitoring (RMON), select <strong>RMON alarm</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps for routing protocol notifications, select <strong>Routing</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps on system warm and cold starts, select <strong>Startup</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To generate traps on Virtual Router Redundancy Protocol (VRRP) events (such as new-master or authentication failures), select <strong>VRRP events</strong>.</td>
</tr>
<tr>
<td>Targets</td>
<td>Specifies one or more hostnames or IP addresses for the systems to receive SNMP traps generated by the trap group being configured.</td>
<td>1. Enter the hostname or IP address, in dotted decimal notation, of the target system to receive the SNMP traps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

**Health Monitoring**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Health Monitoring</td>
<td>Enables the SNMP health monitor on the switch. The health monitor periodically (over the time you specify in the interval field) checks the following key indicators of switch health:</td>
<td>Select the check box to enable the health monitor and configure options. Clear the check box to disable the health monitor.</td>
</tr>
<tr>
<td></td>
<td>• Percentage of file storage used</td>
<td><strong>NOTE:</strong> If you select the Enable Health Monitoring check box and do not specify options, then SNMP health monitoring is enabled with default values.</td>
</tr>
<tr>
<td></td>
<td>• Percentage of Routing Engine CPU used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Percentage of Routing Engine memory used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Percentage of memory used for each system process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Percentage of CPU used by the forwarding process</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Percentage of memory used for temporary storage by the forwarding process</td>
<td></td>
</tr>
<tr>
<td>Interval</td>
<td>Specifies the sampling frequency, in seconds, over which the key health indicators are sampled and compared with the rising and falling thresholds.</td>
<td>Enter an interval time, in seconds, from 1 through 2147483647. The default value is 300 seconds (5 minutes).</td>
</tr>
<tr>
<td></td>
<td>For example, if you configure the interval as 100 seconds, the values are checked every 100 seconds.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 433: SNMP Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rising Threshold</strong></td>
<td>Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is increasing.</td>
<td>Enter a value from 0 through 100. The default value is 90.</td>
</tr>
<tr>
<td></td>
<td>For example, if the rising threshold is 90 (the default), SNMP generates an event when the value of any key indicator reaches or exceeds 90 percent.</td>
<td></td>
</tr>
<tr>
<td><strong>Falling Threshold</strong></td>
<td>Specifies the value at which SNMP generates an event (trap and system log message) when the value of a sampled indicator is decreasing.</td>
<td>Enter a value from 0 through 100. The default value is 80.</td>
</tr>
<tr>
<td></td>
<td>For example, if the falling threshold is 80 (the default), SNMP generates an event when the value of any key indicator falls back to 80 percent or less.</td>
<td>NOTE: The falling threshold value must be less than the rising threshold value.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Monitoring System Process Information on page 718
- Monitoring System Properties on page 714

### Configuring Mirroring on EX4300 Switches to Analyze Traffic (CLI Procedure)

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Port Mirroring to Analyze Traffic (CLI Procedure). For ELS details, see Getting Started with Enhanced Layer 2 Software.

EX4300 switches enable you to configure mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN

**BEST PRACTICE:** Mirror only necessary packets to reduce potential performance impact. We recommend that you:

- Disable your configured mirroring configurations when you are not using them.
- Specify individual interfaces as input to analyzers rather than specifying all interfaces as input.
- Limit the amount of mirrored traffic by using firewall filters.
NOTE: If you want to create additional analyzers without deleting the existing analyzers, then disable the existing analyzers by using the disable analyzer analyzer-name statement from the command-line interface or the J-Web configuration page for mirroring.

NOTE: Interfaces used as output for an analyzer must be configured under the ethernet-switching family.

- Configuring an Analyzer for Local Traffic Analysis on page 3598
- Configuring an Analyzer for Remote Traffic Analysis on page 3598
- Configuring Port Mirroring on page 3599

Configuring an Analyzer for Local Traffic Analysis

To mirror interface traffic or VLAN traffic on the switch to an interface on the switch (by using analyzers):

1. Choose a name for the analyzer and specify the input:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name input ingress interface interface-name
   ```
   
   For example, create an analyzer called employee-monitor for which the input traffic is packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
   ```

2. Configure the destination interface for the mirrored packets:

   ```
   [edit forwarding-options]
   user@switch# set analyzer analyzer-name output interface interface-name
   ```
   
   For example, configure ge-0/0/10.0 as the destination interface for the employee-monitor analyzer:

   ```
   [edit forwarding-options]
   user@switch# set analyzer employee-monitor output interface ge-0/0/10.0
   ```

Configuring an Analyzer for Remote Traffic Analysis

To mirror traffic that is traversing interfaces or a VLAN on the switch to a VLAN for analysis from a remote location (by using analyzers):

1. Configure a VLAN to carry the mirrored traffic:

   ```
   [edit]
   user@switch# set vlans analyzer-name vlan-id vlan-ID
   ```
   
   For example, define an analyzer VLAN called remote-analyzer and assign it a VLAN ID of 999:

   ```
   [edit]
   user@switch# set vlans remote-analyzer vlan-id 999
   ```
2. Set the uplink module interface that is connected to the distribution switch to trunk mode and associate it with the analyzer VLAN:

```plaintext
[edit]
user@switch# set interfaces interface-name unit 0 family ethernet-switching interface-mode trunk vlan members vlan-ID
```

For example, set the interface ge-0/1/1 to trunk mode and associate it with the analyzer VLAN ID 999:

```plaintext
[edit]
user@switch# set interfaces ge-0/1/1 unit 0 family ethernet-switching interface-mode trunk vlan members 999
```

3. Configure the analyzer:

a. Define an analyzer and specify the traffic to be mirrored:

```plaintext
[edit forwarding-options]
user@switch# set analyzer analyzer-name input ingress interface interface-name
```

For example, define the `employee-monitor` analyzer for which traffic to be mirrored is packets entering interfaces ge-0/0/0.0 and ge-0/0/1.0:

```plaintext
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/0.0
[edit forwarding-options]
user@switch# set analyzer employee-monitor input ingress interface ge-0/0/1.0
```

b. Specify the analyzer VLAN as the output for the analyzer:

```plaintext
[edit forwarding-options]
user@switch# set analyzer analyzer-name output vlan vlan-ID
```

For example, specify the `remote-analyzer` VLAN as the output analyzer for the `employee-monitor` analyzer:

```plaintext
[edit forwarding-options]
user@switch# set analyzer employee-monitor output vlan 999
```

### Configuring Port Mirroring

To filter packets to be mirrored to a port-mirroring instance, create the instance and then use it as the action in the firewall filter. You can use firewall filters in both local and remote mirroring configurations.

If the same port-mirroring instance is used in multiple filters or terms, the packets are copied to the analyzer output port or analyzer VLAN only once.

To filter mirrored traffic, create a port-mirroring instance under the [edit forwarding-options] hierarchy level, and then create a firewall filter. The filter can use any of the available match conditions and must have `port-mirror-instance instance-name` as an action. This action in the firewall filter configuration provides the input to the port-mirroring instance.

To configure a port-mirroring instance with firewall filters:

1. Configure the port-mirroring instance name (here, `employee-monitor`) and the output:

   a. For local analysis, set the output to the local interface to which you will connect the computer running the protocol analyzer application:

      ```plaintext
      [edit forwarding-options]
      ```
user@switch# set port-mirroring instance employee-monitor output interface ge-0/0/10.0

b. For remote analysis, set the output to the remote-analyzer VLAN:
   [edit forwarding-options]
   user@switch# set port-mirroring instance employee-monitor output vlan 999

2. Create a firewall filter by using any of the available match conditions and assign employee-monitor to the port-mirror-instance action:

   This step shows a firewall filter example-filter, with two terms (no-analyzer and to-analyzer):

   a. Create the first term to define the traffic that should not pass through to the port-mirroring instance employee-monitor:
      [edit firewall family ethernet-switching]
      user@switch# set filter (Firewall Filters) example-filter term no-analyzer from source-address ip-address
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term no-analyzer from destination-address ip-address
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term no-analyzer then accept

   b. Create the second term to define the traffic that should pass through to the port-mirroring instance employee-monitor:
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term to-analyzer from destination-port 80
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term to-analyzer then port-mirror-instance employee-monitor
      [edit firewall family ethernet-switching]
      user@switch# set filter example-filter term to-analyzer then accept

3. Apply the firewall filter to the interfaces or VLAN that provide input to the port-mirroring instance:
   [edit]
   user@switch# set interfaces ge-0/0/0 unit 0 family ethernet-switching filter input example-filter
   [edit]
   user@switch# set vlan (802.1Q Tagging) remote-analyzer filter input example-filter

Related Documentation

- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Understanding Port Mirroring on EX Series Switches
- Firewall Filters for EX Series Switches Overview on page 4088
Configuring Port Mirroring to Analyze Traffic (J-Web Procedure)

EX Series switches allow you to configure port mirroring to send copies of packets to either a local interface for local monitoring or to a VLAN for remote monitoring. You can use port mirroring to copy these packets:

- Packets entering or exiting a port
- Packets entering a VLAN on EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, EX6200 switches
- Packets exiting a VLAN on EX8200 switches

To configure port mirroring on an EX Series switch using the J-Web interface:

1. Select Configure > Security > Port Mirroring.

   The top of the screen displays analyzer details such as the name, status, analyzer port, ratio, and loss priority.

   The bottom of the screen lists ingress and egress ports of the selected analyzer.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - Add—Add an analyzer. Enter information as specified in Table 434 on page 3602.
   - Edit—Modify details of the selected analyzer. Enter information as specified in Table 434 on page 3602.
   - Delete—Delete the selected analyzer.
   - Enable/Disable—Enable or disable the selected analyzer (toggle).

   NOTE: On EX2200, EX3200, EX4200, and EX4500 switches, only one analyzer can be enabled at a time. On EX8200 switches, a maximum of seven analyzers can be enabled. On EX4300 switches a maximum of four Analyzers/Port Mirror instances can be enabled.

   NOTE: When an analyzer is deleted or disabled, any filter association is removed.
### Table 434: Port Mirroring Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer Name</td>
<td>Specifies the name of the analyzer.</td>
<td>Type a name for the analyzer.</td>
</tr>
<tr>
<td>Ratio</td>
<td>Specifies the ratio of packets to be mirrored.</td>
<td>Enter a number from 0 through 2047.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Loss Priority</td>
<td>Specifies the loss priority of the mirrored packets.</td>
<td>Keep the default of low, unless the output is to a VLAN.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Analyzer Port</td>
<td>Specifies a local interface or VLAN to which mirrored packets are sent.</td>
<td>Click <strong>Select</strong>. In the Select Analyzer Port/VLAN window, select either port or VLAN as the <strong>Analyzer Type</strong>. Next, select the required port or VLAN. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the port (interface) from the list.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>A VLAN must have only one associated interface to be specified as an analyzer interface.</td>
<td></td>
</tr>
<tr>
<td>Analyzer Type</td>
<td>Specifies the analyzer type.</td>
<td>Select the <strong>Analyzer Type</strong> from the list.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This option is supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>No Filter check</td>
<td>Enable this option to skip checking for filters on port-mirroring instance.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This option is supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Ingress</td>
<td>Specifies interfaces or VLANs for which entering traffic is mirrored.</td>
<td>Click <strong>Add</strong>. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. Click <strong>Remove</strong> to delete an ingress interface or VLAN.</td>
</tr>
<tr>
<td>Egress</td>
<td>Specifies interfaces for which exiting traffic is mirrored.</td>
<td>Click <strong>Add</strong> and select <strong>Port</strong> or <strong>VLAN</strong>. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. Click <strong>Remove</strong> to remove egress interfaces.</td>
</tr>
</tbody>
</table>
Configuring sFlow Technology for Network Monitoring (CLI Procedure)

You can configure sFlow technology, designed for monitoring high-speed switched or routed networks, to continuously monitor traffic at wire speed on all interfaces simultaneously. Junos OS fully supports the sFlow standard described in RFC 3176, InMon Corporation’s sFlow: A Method for Monitoring Traffic in Switched and Routed Networks (see http://faqs.org/rfcs/rfc3176.html).

To configure sFlow features:

1. Configure the IP address and the UDP port of the collector:

   ```
   [edit protocols]
   user@switch# set sflow collector ip-address udp-port port-number
   ```

2. Enable sFlow technology on a specific interface:

   ```
   [edit protocols sflow]
   user@switch# set interfaces interface-name
   ```

   \[NOTE: You cannot enable sFlow technology on a Layer 3 VLAN-tagged interface.\]

   You cannot enable sFlow technology on a link aggregation group (LAG), but you can enable it on the member interfaces of a LAG.

3. Specify how often the sFlow agent polls the interface:

   ```
   [edit protocols sflow]
   user@switch# set polling-interval seconds
   ```

   \[NOTE: Specify 0 if you do not want to poll the interface.\]

4. Specify the rate at which packets must be sampled. You can specify either an egress or an ingress qualifier, or both.

   ```
   [edit protocols sflow]
   user@switch# set sample-rate number
   ```

   \[NOTE: The sample-rate number (the global sampling rate) statement has been deprecated and might be removed from future product releases. We strongly recommend that you phase out its use.\]
NOTE: We recommend that you configure the same sample rates for both ingress and egress. If the sample rates are different, the lower value is used.

To specify an egress sampling rate:

```
[edit protocols sflow]
user@switch# set sample-rate egress number
```

To specify an ingress sampling rate:

```
[edit protocols sflow]
user@switch# set sample-rate ingress number
```

5. To configure the polling interval and the egress and ingress sampling rates at the interface level:

```
[edit protocols sflow interfaces interface-name]
user@switch# set polling-interval seconds
[edit protocols sflow interfaces]
user@switch# set sample-rate egress number
[edit protocols sflow interfaces]
user@switch# set sample-rate ingress number
```

NOTE: The interface-level configuration overrides the global configuration.

6. To specify an IP address to be used as the agent ID for the sFlow agent:

```
[edit protocols sflow]
user@switch# set agent-id ip-address
```

7. To specify the source IP address to be used for sFlow datagrams:

```
[edit protocols sflow]
user@switch# set source-ip ip-address
```

Related Documentation

- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Understanding How to Use sFlow Technology for Network Monitoring on an EX Series Switch on page 3549

Configuring Real-Time Performance Monitoring (J-Web Procedure)

Real-time performance monitoring (RPM) in EX Series switches enables you to configure and send probes to a specified target and monitor the analyzed results to determine packet loss, round-trip time, and jitter. Jitter is the difference in relative transit time between two consecutive probes. You can set up probe owners and configure one or more performance probe tests under each probe owner.

The ways in which you can use RPM include:

- Monitor time delays between devices.
- Monitor time delays at the protocol level.
• Set thresholds to trigger SNMP traps when threshold values are exceeded. You can configure thresholds for round-trip time, ingress or egress delay, standard deviation, jitter, successive lost probes, and total lost probes per test.
• Determine automatically whether a path exists between a host switch and its configured Border Gateway Protocol (BGP) neighbors. You can view the results of the discovery using an SNMP client.
• Use the history of the most recent 50 probes to analyze trends in your network and predict future needs.

Probes collect packets per destination and per application, including PING Internet Control Message Protocol (ICMP) packets, User Datagram Protocol and Transmission Control Protocol (UDP/TCP) packets with user-configured ports, user-configured Differentiated Services code point (DSCP) type-of-service (ToS) packets, and Hypertext Transfer Protocol (HTTP) packets.

EX Series switches support the following tests and probe types:

• Ping tests:
  • ICMP echo
  • ICMP timestamp

• HTTP tests:
  • HTTP get (not available for BGP RPM services)

• UDP and TCP tests with user-configured ports:
  • UDP echo
  • TCP connection
  • UDP timestamp

To account for latency in the communication of probe messages, you can enable timestamping of the probe packets. You should configure both the requester and the responder to timestamp the RPM packets. The RPM features provides an additional configuration option to set one-way hardware timestamps. Use one-way timestamps when you want information about one-way, rather than round-trip, times for packets to traverse the network between the requester and the responder.

**NOTE:**

• EX Series switches support hardware timestamps for UDP and ICMP probes. EX Series switches do not support hardware timestamps for HTTP or TCP probes.
• If the responder does not support hardware timestamps, RPM can only report the round-trip measurements, it cannot calculate round-trip jitter.
• In EX Series switches timestamps apply only to IPv4 traffic.
To configure RPM using the J-Web interface:

1. Select **Troubleshoot > RPM > Configure RPM**.

2. In the **Configure RPM** page, enter information as specified in Table 435 on page 3606.
   a. Click **Add** to set up the **Owner Name** and **Performance Probe Tests**.
   b. Select a probe owner from **Probe Owners** list and click **Delete** to remove the selected
      probe owner.
   c. Double-click one of the probe owners in **Probe Owners** list to display the list of
      performance probe tests.
   d. Double-click one of the performance probe tests to edit the test parameters.

3. Enter the **Maximum Number of Concurrent Probes** and specify the **Probe Servers**.

4. Click **Apply** to apply the RPM probe settings.

### Table 435: RPM Probe Owner, Concurrent Probes, and Probe Servers Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| Probe Owners            | Identifies a owner for whom one or more RPM tests are configured. In most implementations, the owner name identifies a network on which a set of tests is being run. | 1. Click **Add** and type an owner name.  
2. In **Performance Probe Tests**, click **Add** to define the RPM test parameters. See Table 436 on page 3607 for information on configuring RPM test parameters.  
3. Click **OK** to save the settings or **Cancel** to exit from the window without saving the changes. |
| Maximum Number of Concurrent Probes | Specifies the maximum number of concurrent probes allowed. | Type a number from 1 through 500. |
| Probe Servers           | Specifies the servers that act as receivers and transmitters for the probes. | Set up the following servers:  
  - TCP Probe Server—Specifies the port on which the device is to receive and transmit TCP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535.  
  - UDP Probe Server—Specifies the port on which the device is to receive and transmit UDP probes. Type the number 7 (a standard TCP port number) or a port number from 49160 through 65535. |
Table 436: Performance Probe Tests Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identification</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Name</td>
<td>Identifies the RPM test.</td>
<td>Type a test name.</td>
</tr>
<tr>
<td>Target (Address or URL)</td>
<td>Specifies the IP address or the URL of the probe target.</td>
<td>Type the IP address in dotted decimal notation or the URL of the probe target. If the target is a URL, type a fully formed URL that includes http://.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Specifies the IP address to be used as the probe source address.</td>
<td>Type the source address to be used for the probe. If you do not supply this value, the packet uses the outgoing interface’s address as the probe source address.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Specifies the routing instance over which the probe is sent.</td>
<td>Type the routing instance name. The routing instance applies only to icmp-ping and icmp-ping-timestamp probe types. The default routing instance is inet.0.</td>
</tr>
<tr>
<td>History Size</td>
<td>Specifies the number of probe results to be saved in the probe history.</td>
<td>Type a number from 0 through 255. The default history size is 50.</td>
</tr>
<tr>
<td><strong>Request Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probe Type</td>
<td>Specifies the type of probe to send as part of the test.</td>
<td>Select a probe type from the list:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• http-get</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• http-get-metadata</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• icmp-ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• icmp-ping-timestamp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• tcp-ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• udp-ping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• udp-ping-timestamp</td>
</tr>
<tr>
<td>Interval</td>
<td>Sets the wait time (in seconds) between probe transmissions.</td>
<td>Type a number from 1 through 255.</td>
</tr>
<tr>
<td>Test Interval</td>
<td>Sets the wait time (in seconds) between tests.</td>
<td>Type a number from 0 through 86400.</td>
</tr>
<tr>
<td>Probe Count</td>
<td>Sets the total number of probes to be sent for each test.</td>
<td>Type a number from 1 through 15.</td>
</tr>
<tr>
<td>Moving Average Size</td>
<td>Specifies the number of samples to be used in the statistical calculation operations to be performed across a number of the most recent samples.</td>
<td>Type a number from 0 through 255.</td>
</tr>
</tbody>
</table>
Table 436: Performance Probe Tests Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Port</td>
<td>Specifies the TCP or UDP port to which probes are sent.</td>
<td>Type the number 7 (a standard TCP or UDP port number) or a port number from 49160 through 65535.</td>
</tr>
<tr>
<td>DSCP Bits</td>
<td>Specifies the Differentiated Services code point (DSCP) bits. This value must be a valid 6-bit pattern.</td>
<td>Type a valid 6-bit pattern.</td>
</tr>
<tr>
<td>Data Size</td>
<td>Specifies the size (in bytes) of the data portion of the ICMP probes.</td>
<td>Type a number from 0 through 65507.</td>
</tr>
<tr>
<td>Data Fill</td>
<td>Specifies the hexadecimal value of the data portion of the ICMP probes.</td>
<td>Type a hexadecimal value from 1h through 800h.</td>
</tr>
<tr>
<td>Hardware Timestamp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>One Way Hardware Timestamp</td>
<td>Enables one-way hardware timestamp.</td>
<td>To enable timestamping, select the check box.</td>
</tr>
<tr>
<td>Destination Interface</td>
<td>Enables hardware timestamp on the specified interface.</td>
<td>Select an interface from the list.</td>
</tr>
<tr>
<td>Maximum Probe Thresholds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Successive Lost Probes</td>
<td>Sets the number of probes that can be lost successively, if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 15.</td>
</tr>
<tr>
<td>Lost Probes</td>
<td>Sets the number of probes that can be lost, if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 15.</td>
</tr>
<tr>
<td>Round Trip Time</td>
<td>Sets the round-trip time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000.</td>
</tr>
<tr>
<td>Jitter</td>
<td>Sets the jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000.</td>
</tr>
</tbody>
</table>
### Table 436: Performance Probe Tests Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Deviation</strong></td>
<td>Sets the maximum allowable standard deviation (in microseconds), if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000.</td>
</tr>
<tr>
<td><strong>Egress Time</strong></td>
<td>Sets the one-way time (in microseconds), from the switch to the remote server, if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000.</td>
</tr>
<tr>
<td><strong>Ingress Time</strong></td>
<td>Sets the one-way time (in microseconds), from the remote server to the switch, if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000 (microseconds).</td>
</tr>
<tr>
<td><strong>Jitter Egress Time</strong></td>
<td>Sets the outbound-time jitter (in microseconds), if exceeded triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000.</td>
</tr>
<tr>
<td><strong>Jitter Ingress Time</strong></td>
<td>Sets the inbound-time jitter (in microseconds), if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 and 60000000.</td>
</tr>
<tr>
<td><strong>Egress Standard Deviation</strong></td>
<td>Sets the maximum allowable standard deviation of outbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000.</td>
</tr>
<tr>
<td><strong>Ingress Standard Deviation</strong></td>
<td>Sets the maximum allowable standard deviation of inbound times (in microseconds), if exceeded, triggers a probe failure and generates a system log message.</td>
<td>Type a number from 0 through 60000000.</td>
</tr>
</tbody>
</table>

### Traps

<table>
<thead>
<tr>
<th>Trap</th>
<th>Description</th>
<th>Actions</th>
</tr>
</thead>
</table>
| **Egress Jitter Exceeded** | Generates SNMP traps when the threshold for jitter in outbound time is exceeded. | • To enable SNMP traps for this condition, select the check box.  
• To disable SNMP traps, clear the check box. |
| **Egress Standard Deviation Exceeded** | Generates SNMP traps when the threshold for standard deviation in outbound times is exceeded. | • To enable SNMP traps for this condition, select the check box.  
• To disable SNMP traps, clear the check box. |
#### Table 436: Performance Probe Tests Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Time Exceeded</td>
<td>Generates SNMP traps when the threshold for maximum outbound time is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Ingress Jitter Exceeded</td>
<td>Generates SNMP traps when the threshold for jitter in inbound time is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Ingress Standard Deviation Exceeded</td>
<td>Generates SNMP traps when the threshold for standard deviation in inbound times is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Ingress Time Exceeded</td>
<td>Generates SNMP traps when the threshold for maximum inbound time is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Jitter Exceeded</td>
<td>Generates SNMP traps when the threshold for jitter in round-trip time is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Probe Failure</td>
<td>Generates SNMP traps when the threshold for the number of successive lost probes is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>RTT Exceeded</td>
<td>Generates SNMP traps when the threshold for maximum round-trip time is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Standard Deviation Exceeded</td>
<td>Generates SNMP traps when the threshold for standard deviation in round-trip times is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Test Completion</td>
<td>Generates SNMP traps when a test is completed.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
<tr>
<td>Test Failure</td>
<td>Generates SNMP traps when the threshold for the total number of lost probes is exceeded.</td>
<td>• To enable SNMP traps for this condition, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To disable SNMP traps, clear the check box.</td>
</tr>
</tbody>
</table>
Use real-time performance monitoring (RPM) to configure active probes to track and monitor traffic across the network and to investigate network problems. To configure basic RPM probes on the EX Series switch, you must configure the probe owner, the test, and the specific parameters of the RPM probe.

You can also set a timestamp to improve the measurement of latency or jitter. The probe is timestamped by the device originating the probe (the RPM client). If you do not enable hardware timestamps, the timer values are set. You should configure both the RPM client (the requester) and the RPM server (the responder) to timestamp the RPM packets. However, if the RPM server does not support hardware timestamps, RPM can only report the round-trip measurements.

Timestamps apply only to IPv4 traffic.

You can enable hardware timestamps for the following RPM probe types:

- icmp-ping
- icmp-ping-timestamp
- udp-ping
- udp-ping-timestamp

To configure RPM probes and enable hardware timestamping:

1. Specify the probe owner:
   
   ```
   [edit services rpm]
   user@switch# set probe owner
   ```

2. Specify a test name. A test represents the range of probes over which the standard deviation, average, and jitter are calculated.
   
   ```
   [edit services rpm probe owner]
   user@switch# set test test-name
   ```

3. Specify the packet and protocol contents of the probe:
   
   ```
   [edit services rpm probe owner test test-name]
   user@switch# set probe-type type
   ```

4. Specify the destination IPv4 address to be used for the probes:
   
   ```
   [edit services rpm probe owner test test-name]
   user@switch# set target address
   ```

5. Specify the number of probes within a test:
   
   ```
   [edit services rpm probe owner test test-name]
   user@switch# set probe-count count
   ```

6. Specify the time, in seconds, to wait between sending packets:
   
   ```
   [edit services rpm probe owner test test-name]
   ```
user@switch# set probe-interval interval

7. Specify the time, in seconds, to wait between tests:

[edit services rpm probe owner test test-name]
user@switch# set test-interval interval

8. Specify the source IP address to be used for probes. If the source IP address is not one of the switch’s assigned addresses, the packet uses the outgoing interface’s address as its source.

[edit services rpm probe owner test test-name]
user@switch# set source-address address

9. Specify the value of the Differentiated Services (DiffServ) field within the IP header. The DiffServ code point (DSCP) bits value must be set to a valid 6-bit pattern.

[edit services rpm probe owner test test-name]
user@switch# set dscp-code-point dscp-bits

10. If you are using ICMP probes, specify the size of the data portion of ICMP probes:

[edit services rpm probe owner test test-name]
user@switch# set data-size size

11. Enable hardware timestamping of RPM probe messages:

[edit services rpm probe owner test test-name]
user@switch# set hardware-timestamp

Related Documentation
• Configuring Real-Time Performance Monitoring (J-Web Procedure) on page 3604
• Understanding Real-Time Performance Monitoring on EX Series Switches on page 3540

Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure)

Ethernet interfaces on Juniper Networks EX Series Ethernet Switches and Juniper Networks Junos OS for EX Series switches support the IEEE 802.1ag standard for Operation, Administration, and Management (OAM). The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM).

This topic describes these tasks:

1. Creating the Maintenance Domain on page 3612
2. Configuring the Maintenance Domain MIP Half Function on page 3613
3. Creating a Maintenance Association on page 3613
4. Configuring the Continuity Check Protocol on page 3614
5. Configuring a Maintenance Association End Point on page 3614
6. Configuring a Connectivity Fault Management Action Profile on page 3615
7. Configuring the Linktrace Protocol on page 3615

Creating the Maintenance Domain

A maintenance domain comprises network entities such as operators, providers, and customers. To enable connectivity fault management (CFM) on an Ethernet interface, you must create a maintenance domains, maintenance associations, and MEPs.
To create a maintenance domain:

1. Specify a name for the maintenance domain:

   ```
   [edit protocols oam ethernet connectivity-fault-management]
   user@switch# set maintenance-domain domain-name
   ```

2. Specify a format for the maintenance domain name. If you specify none, no name is configured:

   - A plain ASCII character string
   - A domain name service (DNS) format
   - A media access control (MAC) address plus a two-octet identifier in the range 0 through 65,535
   - none

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
   user@switch# set name-format format
   ```

   For example, to specify the name format as MAC address plus a two-octet identifier:

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
   user@switch# set name-format mac+2oct
   ```

3. Configure the maintenance domain level, which is used to indicate the nesting relationship between this domain and other domains. Use a value from 0 through 7:

   ```
   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
   user@switch# set level level
   ```

**Configuring the Maintenance Domain MIP Half Function**

MIP Half Function (MHF) divides the maintenance association intermediate point (MIP) functionality into two unidirectional segments, improves visibility with minimal configuration, and improves network coverage by increasing the number of points that can be monitored. MHF extends monitoring capability by responding to loop-back and link-trace messages to help isolate faults. Whenever a MIP is configured, the MIP half function value for all maintenance domains and maintenance associations must be the same.

To configure the MIP half function:

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]
user@switch# set mip-half-function (none | default | explicit)
```
Configuring the Continuity Check Protocol

The continuity check protocol is used for fault detection by a maintenance association end point (MEP) within a maintenance association. The MEP periodically sends continuity check multicast messages. The receiving MEPs use the continuity check messages (CCMs) to build a MEP database of all MEPs in the maintenance association.

To configure the continuity check protocol:

1. Enable the continuity check protocol:

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name]
   user@switch# set continuity-check

2. Specify the continuity check hold interval. The hold interval is the number of minutes to wait before flushing the MEP database if no updates occur. The default value is 10 minutes.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]
   user@switch# set hold-interval number

3. Specify the CCM interval. The interval is the time between the transmission of CCMs. You can specify 10 minutes (10m), 1 minute (1m), 10 seconds (10s), 1 second (1s), 100 milliseconds (100ms), or 10 milliseconds (10ms).

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]
   user@switch# set interval number

4. Specify the number of CCMs (that is, protocol data units) that can be lost before the MEP is marked as down. The default number of protocol data units (PDUs) is 3.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name continuity-check]
   user@switch# set loss-threshold number

Configuring a Maintenance Association End Point

To configure a maintenance association end point:

1. Specify an ID for the MEP. The value can be from 1 through 8191.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name]
   user@switch# set mep mep-id

2. Enable maintenance endpoint automatic discovery if you want to have the MEP accept continuity check messages (CCMs) from all remote MEPS of the same maintenance association:

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]
   user@switch# set auto-discovery

3. You can specify that CFM packets (CCMs) be transmitted only in one direction for the MEP, that is, the direction be set as down so that CCMs are transmitted only out of (not into) the interface configured on this MEP.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]
   user@switch# set direction down
4. Specify the logical interface to which the MEP is attached. It can be either an access interface or a trunk interface. If you specify a trunk interface, the VLAN associated with that interface must have a VLAN ID.

   NOTE: You cannot associate an access interface that belongs to multiple VLANs with the MEP.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]  
   user@switch# set interface interface-name

5. You can configure a remote MEP from which CCMs are expected. If autodiscovery is not enabled, the remote MEP must be configured under the mep statement. If the remote MEP is not configured under the mep statement, the CCMs from the remote MEP are treated as errors.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]  
   user@switch# set remote-mep mep-id

**Configuring a Connectivity Fault Management Action Profile**

You can configure an action profile and specify the action to be taken when any of the configured events occur. Alternatively, you can configure an action profile and specify default actions when connectivity to a remote MEP fails.

To configure an action profile:

1. Specify a name for an action profile:

   [edit protocols oam ethernet connectivity-fault-management]  
   user@switch# set action-profile profile-name

2. Configure the action of the action profile:

   [edit protocols oam ethernet connectivity-fault-management action-profile profile-name]  
   user@switch# set action interface-down

3. Configure one or more events under the action profile, the occurrence of which will trigger the corresponding action to be taken:

   [edit protocols oam ethernet connectivity-fault-management action-profile profile-name]  
   user@switch# set event event
   See Junos OS Network Interfaces Configuration Guide

**Configuring the Linktrace Protocol**

The linktrace protocol is used for path discovery between a pair of maintenance points. Linktrace messages are triggered by an administrator using the traceroute command to verify the path between a pair of MEPs under the same maintenance association. Linktrace messages can also be used to verify the path between a MEP and a MIP under the same maintenance domain.

To configure the linktrace protocol:
1. Configure the linktrace path age timer. If no response to a linktrace request is received, the request and response entries are deleted after the age timer expires:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set linktrace age time
```

2. Configure the number of linktrace reply entries to be stored per linktrace request:

```
[edit protocols oam ethernet connectivity-fault-management]
user@switch# set linktrace path-database-size path-database-size
```

## Related Documentation
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 3587
- Understanding Ethernet OAM Connectivity Fault Management for an EX Series Switch on page 3553
- Junos OS Network Interfaces Configuration Guide

### Configuring Ethernet OAM Link Fault Management (CLI Procedure)

Ethernet OAM link fault management (LFM) can be used for physical link-level fault detection and management. The IEEE 802.3ah LFM works across point-to-point Ethernet links either directly or through repeaters.

To configure Ethernet OAM LFM using the CLI:

1. Enable IEEE 802.3ah OAM support on an interface:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name
```

**NOTE:** You can configure Ethernet OAM LFM on aggregated interfaces.

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name link-discovery active
```

**NOTE:** The remaining steps are optional. You can choose which of these features to configure for Ethernet OAM LFM on your switch.

2. Specify whether the interface or the peer initiates the discovery process by configuring the link discovery mode to **active** or **passive** (**active** = interface initiates; **passive** = peer initiates):

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name link-discovery active
```

3. Configure a periodic OAM PDU-sending interval (in milliseconds) for fault detection:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface pdu-interval interval
```

4. Specify the number of OAM PDUs that an interface can miss before the link between peers is considered down:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name pdu-threshold threshold-value
```

5. Configure event threshold values on an interface for the local errors that trigger the sending of link event TLVs:
Set the threshold value (in seconds) for sending frame-error events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-error count
```

Set the threshold value (in seconds) for sending frame-period events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-period count
```

Set the threshold value (in seconds) for sending frame-period-summary events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds frame-period-summary count
```

Set the threshold value (in seconds) for sending symbol-period events or taking the action specified in the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name event-thresholds symbol-period count
```

**NOTE:** You can disable the sending of link event TLVs.

To disable the sending of link event TLVs:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name negotiation-options no-allow-link-events
```

6. Create an action profile to define event fault flags and thresholds to be taken when the link fault event occurs. Then apply the action profile to one or more interfaces. (You can also apply multiple action profiles to a single interface.)

a. Name the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set action-profile profile-name
```

b. Specify actions to be taken by the system when the link fault event occurs:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set action-profile profile-name action syslog
user@switch# set action-profile profile-name action link-down
```

c. Specify events for the action profile:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set action-profile profile-name event link-adjacency-loss
```

**NOTE:** For each action profile, you must specify at least one link event and one action. The actions are taken only when all of the events in the action profile are true. If more than one action is specified, all actions are executed. You can set a low threshold for a specific action such as logging the error and set a high threshold for another action such as system logging.

7. Set a remote interface into loopback mode so that all frames except OAM PDUs are looped back without any changes made to the frames. Set the remote DTE in loopback mode as follows:

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name negotiation-options no-allow-link-events
```
mode (the remote DTE must support remote-loopback mode) and then enable remote loopback support for the local interface.

```
[edit protocols oam ethernet link-fault-management]
user@switch# set interface interface-name remote-loopback
user@switch# set interface interface-name negotiation-options allow-remote-loopback
```

Related Documentation

- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Understanding Ethernet OAM Link Fault Management for an EX Series Switch on page 3551

Configuring Interfaces for Uplink Failure Detection (CLI Procedure)

You can configure uplink failure detection on EX Series switches to help ensure balanced traffic flow. Using this feature, switches can monitor and detect link failure on uplink interfaces and can propagate the failure to downlink interfaces so that servers connected to those downlink interfaces can switch over to secondary interfaces.

Follow these configuration guidelines:

- You can configure a maximum of 48 groups for each switch.
- You can configure a maximum of 48 uplink interfaces and 48 downlink interfaces in each group.
- You can configure physical links and logical links in separate groups.
- Ensure that all the interfaces in the group are up. If the interfaces are down, uplink failure detection does not work.

NOTE: Routed VLAN interfaces (RVIs) cannot be configured as uplink interfaces to be monitored.

To configure uplink failure detection on a switch:

1. Specify a name for the group:

```
[edit protocols]
user@switch# set uplink-failure-detection group group-name
```

2. Add an uplink interface to the group:

```
[edit protocols]
user@switch# set uplink-failure-detection group group-name link-to-monitor interface-name
```

3. Repeat Step 2 for adding each uplink interface to the group.

NOTE: An interface can be configured as link-to-monitor in multiple groups.

4. Add a downlink interface to the group:

```
[edit protocols]
```
5. Repeat Step 4 for adding each downlink interface to the group.

NOTE: After you have configured a group, use the show uplink-failure-detection group group-name command to verify that all interfaces in the group are up.

Related Documentation

- Verifying That Uplink Failure Detection Is Working Correctly on page 3788
- Understanding Uplink Failure Detection on page 3556

Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure)

Ethernet frame delay measurement is a useful tool for providing performance statistics or supporting or challenging service-level agreements (SLAs). By default, Ethernet frame delay measurement uses software for timestamping and delay calculations. You can configure an EX Series switch to perform and display Ethernet frame delay measurements on Ethernet interfaces. The switches support software-assisted timestamping.

Before you can begin configuring MEP interfaces to support Ethernet frame delay measurements on switches, ensure that you have:

- Configured Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) correctly
- Enabled distributed periodic packet management (PPM) (distributed PPM is enabled by default)
To configure MEP interfaces on switches to support Ethernet frame delay measurements:

1. Enable the Ethernet frame delay measurement by issuing the `monitor ethernet delay-measurement` operational mode command. In this command, you must specify one measurement type (either one-way or two-way measurement), and you must specify either the unicast MAC address of the peer MEP or its numeric identifier.

Optionally, you can also specify the following parameters:

- Number of frames to send to the peer MEP (`count count`)
- Number of seconds to wait between sending frames (`wait time`)
- Priority value of the delay measurement request frame (`priority value`)
- Size of the data in the data TLV of the request packet (`size value`)
- Suppression of the insertion of the session ID TLV in the request packet (`no-session-id-tlv`)

```
user@switch> monitor ethernet delay-measurement maintenance-domain md-name maintenance-association ma-name one-way mep remote-mep-id count count wait time priority value size value no-session-id-tlv
```

**Related Documentation**

- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620
- Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3623
- Triggering an Ethernet Frame Delay Measurement Session on a Switch on page 3622
- Understanding Ethernet Frame Delay Measurements on Switches on page 3554

## Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)

Ethernet frame delay measurement is a useful tool for providing performance statistics or supporting or challenging service-level agreements (SLAs). You can configure the frame delay measurements in either a one-way mode or a two-way (round-trip) mode to gather frame delay statistics. For one-way Ethernet frame delay measurement, clocks at the local and remote MEPs need to be synchronized. However, clock synchronization is not required for two-way Ethernet frame delay measurement.

Before you begin configuring one-way Ethernet frame delay measurements on two EX Series switches, ensure that you have:

- Configured Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) correctly on both the switches
- Synchronized the system clocks of both the switches

To configure one-way Ethernet frame delay measurements:

1. Configure the maintenance domain, maintenance association, and MEP ID on both the switches.
2. From either switch, start a one-way Ethernet frame delay measurement:
Configuring an Iterator Profile on a Switch (CLI Procedure)

Ethernet frame delay measurement provides fine control to operators for triggering delay measurement on a given service and can be used to monitor service-level agreements (SLAs). You can create an iterator profile with its parameters to periodically transmit SLA measurement packets in the form of ITU-Y.1731-compliant frames for two-way delay measurement.

To create an iterator profile:

1. Specify a name for an SLA iterator profile—for example, il:

   [edit protocols oam ethernet connectivity-fault-management performance-monitoring]
   user@switch# edit sla-iterator-profiles il

2. (Optional) Configure the cycle time, which is the time (in milliseconds) between back-to-back transmissions of SLA frames.

   [edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles il]
   user@switch# set cycle-time cycle-time-value

3. (Optional) Configure the iteration period, which indicates the maximum number of cycles per iteration (the number of connections registered to an iterator cannot exceed this value).

   [edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles il]
   user@switch# set iteration-period iteration-period-value

4. Configure the measurement type as two-way delay measurement.

   [edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles il]
   user@switch# set measurement-type two-way-delay

5. (Optional) Configure the calculation weight for delay.
6. (Optional) Configure the calculation weight for delay variation.

   [edit protocols oam ethernet connectivity-fault-management performance-monitoring
   sla-iterator-profiles i1]
   user@switch# set calculation-weight delay delay-value

7. Configure a remote MEP with the iterator profile.

   [edit protocols oam ethernet connectivity-fault-management maintenance-domain
   md-name maintenance-association ma-name mep mep-id remote-mep remote-mep-id]
   user@switch# set sla-iterator-profiles i1

---

**Related Documentation**

- Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) on page 3619
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620
- Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3623
- Triggering an Ethernet Frame Delay Measurement Session on a Switch on page 3622
- Understanding Ethernet Frame Delay Measurements on Switches on page 3554

---

**Triggering an Ethernet Frame Delay Measurement Session on a Switch**

To trigger Ethernet frame delay measurement, use the `monitor ethernet delay-measurement` operational command and specify the following values:

- Either one-way (**one-way**) or two-way (**two-way**) measurement
- Either the MAC address (**remote-mac-address**) or the MEP ID (**mep**) of the remote host
- The maintenance domain (**maintenance-domain**)
- The maintenance association (**maintenance-association**)
- (Optional) Any or all of these options: `count`, `size`, `wait`, `no-session-id-tlv`, `priority`

For example:

```
user@switch> monitor ethernet delay-measurement one-way 00:05:85:73:39:4a
maintenance-domain md6 maintenance-association ma6 count 10 size 50 wait 5
no-session-id-tlv priority 1
```

---

**Related Documentation**

- Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) on page 3619
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620
Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure)

Ethernet frame delay measurement is a useful tool for providing performance statistics or supporting or challenging service-level agreements (SLAs). You can configure the frame delay measurements in either a one-way mode or a two-way (round-trip) mode to gather frame delay statistics. For one-way Ethernet frame delay measurement, clocks at the local and remote MEPs need to be synchronized. However, clock synchronization is not required for two-way Ethernet frame delay measurement.

Before you begin configuring two-way Ethernet frame delay measurements on two EX Series switches, ensure that you have:

- Configured Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) correctly on both the switches

To configure two-way Ethernet frame delay measurements:

1. Configure the maintenance domain, maintenance association, and MEP ID on both the switches.
2. From either switch, start a two-way Ethernet frame delay measurement:

   user@switch> monitor ethernet delay-measurement maintenance-domain md-name maintenance-association ma-name two-way mep remote-mep-id count count wait time

   You can view the result on the other switch:

   user@switch> show oam ethernet connectivity-fault-management delay-statistics maintenance-domain md-name maintenance-association ma-name local-mep mep-id remote-mep mep-id

Related Documentation

- Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) on page 3619
- Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620
- Triggering an Ethernet Frame Delay Measurement Session on a Switch on page 3622
- Understanding Ethernet Frame Delay Measurements on Switches on page 3554

Configuration Statements: SNMP

- [edit snmp] Configuration Statement Hierarchy on EX Series Switches on page 3623
• **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.

• **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27

This topic lists:

• Supported Statements in the [edit snmp] Hierarchy Level on page 3624

• Unsupported Statements in the [edit snmp] Hierarchy Level on page 3628

**Supported Statements in the [edit snmp] Hierarchy Level**

The following hierarchy shows the **[edit snmp]** configuration statements supported on EX Series switches:

```
snmp {
  client-list list-name {
    address {
      restrict;
    }
  }
  community community-name {
    authorization (read-only | read-write);
    client-list-name list-name;
    clients {
      address <restrict>;
    }
    routing-instance instance-name;
    routing-instance instance-name {
      client-list-name list-name;
      clients {
        address <restrict>;
      }
    }
  }
  view view-name;
}
contact contact-information;
description description;
engine-id {
  (local engine-id | use-default-ip-address | use-mac-address);
}
filter-duplicates;
filter-interfaces {
  interfaces
  all-internal-interfaces;
  interface 1;
  interface 2;
}
health-monitor {
  falling-threshold percentage;
```
idp {
    falling-threshold;
    interval seconds;
    rising-threshold;
}
    interval seconds;
    rising-threshold percentage;
}
interface [ interface-names ];
location location;
name system-name;
nonvolatile {
    commit-delay seconds;
}
rmont {
    alarm index {
        description description;
        falling-event-index index;
        falling-threshold integer;
        falling-threshold-interval seconds;
        interval seconds;
        request-type (get-next-request | get-request | walk-request);
        rising-event-index index;
        rising-threshold integer;
        sample-type (absolute-value | delta-value);
        startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
        syslog-subtag text-string;
        variable oid-variable;
    }
    event index {
        community community-name;
        description description;
        type (log | log-and-trap | none | snmptrap);
    }
    history index {
        bucket-size number;
        interface interface-name;
        interval seconds;
        owner owner-name;
    }
}
    routing-instance-access { access-list {
        routing-instance-name <restrict>;
    }
}
traceoptions {
    file <files number> <match regular-expression> <size maximum-file-size>
    <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
trap-group group-name {
    categories {
        authentication;
        chassis;
configuration;
link;
otn-alarms {
    alarm-name;
}
remote-operations;
rmon-alarm;
routing;
services;
sonet-alarms {
    alarm-name;
}
startup;
vrp-events;
}
destination-port port-number;
routing-instance instance-name;
routing-instance instance-name {
targets {
    address;
}
version (all | v1 | v2);
}
trap-options {
    agent-address outgoing-interface;
    enterprise-oid;
routing-instance instance-name;
routing-instance instance-name {
    source-address (address | lo0);
}
    source-address address;
}
v3 {
    ... the v3 subhierarchy appears after the main [edit snmp] hierarchy level ...
}
view view-name {
    oid object-identifier <exclude | include>;
}
}

snmp {
    v3 {
        notify name {
            tag tag-name;
            type (inform | trap);
        }
        notify-filter profile-name {
            oid oid <exclude | include>;
        }
        snmp-community community-index {
            community-name community-name;
            context context-name;
            security-name security-name;
            tag tag-name;
        }
        target-address target-address-name {


address address;
address-mask address-mask;
routing-instance routing-instance-name;
port port-number;
retry-count number;
routing-instance routing-instance-name;
tag-list tag-list;
target-parameters parameter-name;
timeout seconds;
}
target-parameters parameter-name {
  notify-filter profile-name;
  parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
usm {
  local-engine {
    user username {
      authentication-md5 {
        authentication-key password;
        authentication-password password;
      }
      authentication-none;
      authentication-sha {
        authentication-key password;
        authentication-password password;
      }
      privacy-3des {
        privacy-password password;
      }
      privacy-aes128 {
        privacy-password password;
      }
      privacy-des {
        privacy-password password;
      }
      privacy-none;
    }
  }
}
remote-engine engine-id {
  user username {
    authentication-md5 {
      authentication-key password;
      authentication-password password;
    }
    authentication-none;
    authentication-sha {
      authentication-key
      authentication-password password;
    }
    privacy-3des {
      privacy-password password;
    }
  }
}
Unsupported Statements in the [edit snmp] Hierarchy Level

All statements in the [edit snmp] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:
Table 437: Unsupported [edit snmp] Configuration Statements on EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
</table>

**NOTE:** Variables, such as *community-name*, are not shown in the statements or hierarchies.
Table 437: Unsupported [edit snmp] Configuration Statements on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>logical-system</td>
<td>[edit snmp community]</td>
</tr>
<tr>
<td></td>
<td>[edit snmp trap-group]</td>
</tr>
</tbody>
</table>
Table 437: Unsupported [edit snmp] Configuration Statements on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy</th>
</tr>
</thead>
<tbody>
<tr>
<td>[edit snmp trap-options]</td>
<td>[edit snmp v3 target-address]</td>
</tr>
<tr>
<td>logical-systems-trap-filter</td>
<td>[edit snmp]</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring SNMP (J-Web Procedure) on page 3594
- Network Management Administration Guide for Routing Devices

**address (SNMP)**

**Syntax**

address address;

**Hierarchy Level**

[edit snmp v3 target-address target-address-name]

**Release Information**


**Description**

Specify the SNMP target address.

**Options**

address—IPv4 address of the system to receive traps or informs. You must specify an address, not a hostname.

**Required Privilege Level**

- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**

- Configuring the Address
### address-mask

**Syntax**

```snmp
address-mask address-mask;
```

**Hierarchy Level**

```
[edit snmp v3 target-address target-address-name]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 on the QFX Series.

**Description**

Define and verify the source addresses for a group of target addresses for SNMP traps and informs.

**Options**

- `address-mask`—Define a range of addresses.

**Required Privilege**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Address Mask](#)

### agent-address

**Syntax**

```snmp
agent-address outgoing-interface;
```

**Hierarchy Level**

```
[edit snmp trap-options]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Set the agent address of all SNMPv1 traps generated by this router or switch. Currently, the only option is `outgoing-interface`, which sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

**Options**

- `outgoing-interface`—Value of the agent address of all SNMPv1 traps generated by this router or switch. The `outgoing-interface` option sets the agent address of each SNMPv1 trap to the address of the outgoing interface of that trap.

**Default:** disabled (the agent address is not specified in SNMPv1 traps).

**Required Privilege**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring the Agent Address for SNMP Traps](#)
alarm (SNMP RMON)

Syntax

```plaintext
alarm index {
  description description;
  falling-event-index index;
  falling-threshold integer;
  falling-threshold-interval seconds;
  interval seconds;
  request-type (get-next-request | get-request | walk-request);
  rising-event-index index;
  rising-threshold integer;
  sample-type (absolute-value | delta-value);
  startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
  syslog-subtag syslog-subtag;
  variable oid-variable;
}
```

Hierarchy Level

[edit snmp rmon]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure RMON alarm entries.

Options

- `index`—Identifies this alarm entry as an integer.

The remaining statements are explained separately.

Required Privilege

- snmp—to view this statement in the configuration.
- snmp-control—to add this statement to the configuration.

Related Documentation

- Configuring an Alarm Entry and Its Attributes
- event (SNMP) on page 3644
- Configuring RMON Alarms and Events
- RMON MIB Event, Alarm, Log, and History Control Tables
- Monitoring RMON MIB Tables
- Understanding RMON
- Junos OS Network Management Configuration Guide
### authorization

**Syntax**
```
authorization authorization;
```

**Hierarchy Level**
```
[edit snmp community community-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Set the access authorization for SNMP Get, GetBulk, GetNext, and Set requests.

**Options**
```
authorization—Access authorization level:
```
- `read-only`—Enable Get, GetNext, and GetBulk requests.
- `read-write`—Enable all requests, including Set requests. You must configure a view to enable Set requests.

**Default**: `read-only`

**Required Privilege**
```
level
```

**Related Documentation**
- Configuring the SNMP Community String

### bucket-size

**Syntax**
```
bucket-size number;
```

**Hierarchy Level**
```
[edit snmp rmon history]
```

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the sampling of Ethernet statistics for network fault diagnosis, planning, and performance tuning.

**Default**
50

**Options**
```
number—Number of discrete samples of Ethernet statistics requested.
```

**Required Privilege**
```
level
```

**Related Documentation**
- Configuring SNMP (J-Web Procedure) on page 3594
- Junos OS Network Management Configuration Guide
### categories

| Syntax     | categories {  
|            |   
|            |     category;  
|            | }  
| Hierarchy Level | [edit snmp trap-group group-name]  
| Release Information | Statement introduced before Junos OS Release 7.4.  
| Description | Statement introduced in Junos OS Release 9.0 for EX Series switches.  
| Default | Define the types of traps that are sent to the targets of the named trap group.  
| Options | If you omit the `categories` statement, all trap types are included in trap notifications.  
| Options | `category`—Name of a trap type: authentication, chassis, configuration, link, remote-operations, rmon-alarm, routing, sonet-alarms, startup, or vrrp-events.  
| Required Privilege | snmp—To view this statement in the configuration.  
| Required Privilege | snmp-control—To add this statement to the configuration.  
| Related Documentation | • Configuring SNMP Trap Groups  

### client-list

| Syntax     | client-list client-list-name {  
|            |   
|            |   ip-addresses;  
|            | }  
| Hierarchy Level | [edit snmp]  
| Release Information | Statement introduced in Junos OS Release 8.5.  
| Options | Define a list of SNMP clients.  
| Options | `client-list-name`—Name of the client list.  
| Options | `ip-addresses`—IP addresses of the SNMP clients to be added to the client list,  
| Required Privilege | snmp—To view this statement in the configuration.  
| Required Privilege | snmp-control—To add this statement to the configuration.  
| Related Documentation | • Adding a Group of Clients to an SNMP Community  

Copyright © 2013, Juniper Networks, Inc.
### client-list-name

**Syntax**

```plaintext
client-list-name client-list-name;
```

**Hierarchy Level**

```plaintext
[edit snmp community community-name]
```

**Release Information**


**Description**

Add a client list or prefix list to an SNMP community.

**Options**

- `client-list-name`—Name of the client list or prefix list.

**Required Privilege**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- *Adding a Group of Clients to an SNMP Community*

### clients

**Syntax**

```plaintext
clients {
  address <restrict>;
}
```

**Hierarchy Level**

```plaintext
[edit snmp community community-name]
```

**Release Information**


**Description**

Specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community.

**Default**

If you omit the `clients` statement, all SNMP clients using this community string are authorized to access the router.

**Options**

- `address`—Address of an SNMP client that is authorized to access this router. You must specify an address, not a hostname. To specify more than one client, include multiple `address` options.
- `restrict`—(Optional) Do not allow the specified SNMP client to access the router.

**Required Privilege**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- *Configuring the SNMP Community String*
### commit-delay

**Syntax**
```
commit-delay seconds;
```

**Hierarchy Level**
```
[edit snmp nonvolatile]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure the timer for the SNMP Set reply and start of the commit.

**Options**
- `seconds`—Delay between an affirmative SNMP Set reply and start of the commit.
- **Default:** 5 seconds

**Required Privilege**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- [Configuring the Commit Delay Timer](#)
community (SNMP)

Syntax  

```
community community-name {
    authorization authorization;
    client-list-name client-list-name;
    clients {
        address restrict;
    }
    view view-name;
}
```

Hierarchy Level  [edit snmp]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Define an SNMP community. An SNMP community authorizes SNMP clients based on the source IP address of incoming SNMP request packets. A community also defines which MIB objects are available and the operations (read-only or read-write) allowed on those objects.

The SNMP client application specifies an SNMP community name in `Get`, `GetBulk`, `GetNext`, and `Set` SNMP requests.

Default  If you omit the `community` statement, all SNMP requests are denied.

Options  community-name—Community string. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately.

Required Privilege  

Level  snmp—To view this statement in the configuration.

Related Documentation  

- Configuring the SNMP Community String
community (SNMP RMON)

Syntax  
community community-name;

Hierarchy Level  
[edit snmp rmon event index]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
The trap group that is used when generating a trap (if eventType is configured to send traps). If that trap group has the rmon-alarm trap category configured, a trap is sent to all the targets configured for that trap group. The community string in the trap matches the name of the trap group (and hence, the value of eventCommunity). If nothing is configured, traps are sent to each group with the rmon-alarm category set.

Options  
community-name—Identifies the trap group that is used when generating a trap if the event is configured to send traps.

Required Privilege  
Level  
snmp—To view this statement in the configuration.  
snmp-control—To add this statement to the configuration.

Related Documentation  
• Configuring an Event Entry and Its Attributes
community-name (SNMP)

Syntax  

community-name community-name;

Hierarchy Level  

[edit snmp v3 snmp-community community-index]

Release Information  

Statement introduced before Junos OS Release 7.4. 
Statement introduced in Junos OS Release 9.0 for EX Series switches. 
Statement introduced in Junos OS Release 11. for the QFX Series.

Description  

Define an SNMP community to authorize SNMPv1 or SNMPv2c clients in an SNMPv3 system. When you configure a community in SNMPv3, you can also specify a security name. The access privileges associated with the security name determine which MIB objects are available and which operations (read, write, or notify) are allowed on those objects.

Options  

community-name—Community string for an SNMPv1 or SNMPv2c community. If unconfigured, it is the same as the community index. If the name includes spaces, enclose the name in quotation marks (" ").

NOTE: Community names must be unique. You cannot configure the same community name at the [edit snmp community] and [edit snmp v3 snmp-community community-index] hierarchy levels.

The community name at the [edit snmp v3 snmp-community community-index] hierarchy level is encrypted and not displayed in the command-line interface (CLI).

Required Privilege Level  

snmp—To view this statement in the configuration. 
snmp-control—To add this statement to the configuration.

Related Documentation  

• Configuring the SNMPv3 Community
contact (SNMP)

**Syntax**  
```
contact contact;
```

**Hierarchy Level**  
```
[edit snmp]
```

**Release Information**  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Define the value of the MIB II `sysContact` object, which is the contact person for the managed system.

**Options**  
- `contact`—Name of the contact person. If the name includes spaces, enclose it in quotation marks (" ").

**Required Privilege**  
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**  
- Configuring the System Contact on a Device Running Junos OS

---

description (SNMP)

**Syntax**  
```
description description;
```

**Hierarchy Level**  
```
[edit snmp]
```

**Release Information**  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**  
Define the value of the MIB II `sysDescription` object, which is the description of the system being managed.

**Options**  
- `description`—System description. If the name includes spaces, enclose it in quotation marks (" ").

**Required Privilege**  
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**  
- Configuring the System Description on a Device Running Junos OS
### description (SNMP RMON)

**Syntax**
```
description description;
```

**Hierarchy Level**
- [edit snmp rmon alarm index]
- [edit snmp rmon event index]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Text description of alarm or event.

**Options**
- `description`—Text description of an alarm or event entry. If the description includes spaces, enclose it in quotation marks (" ").

**Required Privilege**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring the Description
- Configuring an Event Entry and Its Attributes

### destination-port

**Syntax**
```
destination-port port-number;
```

**Hierarchy Level**
- [edit snmp trap-group]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Assign a trap port number other than the default.

**Default**
If you omit this statement, the default port is 162.

**Options**
- `port-number`—SNMP trap port number.

**Required Privilege**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring SNMP Trap Groups
engine-id (SNMP)

Syntax

```
engine-id {
  (local engine-id-suffix | use-default-ip-address | use-mac-address);
}
```

Hierarchy Level
[edit snmp]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
The local engine ID is defined as the administratively unique identifier of an SNMPv3 engine, and is used for identification, not for addressing. There are two parts of an engine ID: prefix and suffix. The prefix is formatted according to the specifications defined in RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*. You can configure the suffix here.

NOTE: SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID. If you configure or change the engine ID, you must commit the new engine ID before you configure SNMPv3 users. Otherwise the keys generated from the configured passwords are based on the previous engine ID.

For the engine ID, we recommend using the MAC address of the management port.

Options
- **local engine-id-suffix**—Explicit setting for the engine ID suffix.
- **use-default-ip-address**—The engine ID suffix is generated from the default IP address.
- **use-mac-address**—The SNMP engine identifier is generated from the MAC address of the management interface on the router.

Default: **use-default-ip-address**

Required Privilege Level
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

Related Documentation
- Configuring the Local Engine ID
### event (SNMP)

**Syntax**

```plaintext
event index {
    community community-name;
    description description;
    type type;
}
```

**Hierarchy Level**

```plaintext
[edit snmp rmon]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure RMON event entries.

**Options**

- `index`—Identifier for a specific event entry.

  The remaining statements are explained separately.

**Required Privilege**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring an Event Entry and Its Attributes
- alarm on page 3633

### falling-event-index

**Syntax**

```plaintext
falling-event-index index;
```

**Hierarchy Level**

```plaintext
[edit snmp rmon alarm index]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

The index of the event entry that is used when a falling threshold is crossed. If this value is zero, no event is triggered.

**Options**

- `index`—Index of the event entry that is used when a falling threshold is crossed.

  **Range:** 0 through 65,535
  **Default:** 0

**Required Privilege**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring the Falling Event Index or Rising Event Index
- rising-event-index on page 3665
## falling-threshold

**Syntax**  
falling-threshold *percentage*;

**Hierarchy Level**  
[edit snmp ]

**Release Information**  
Statement introduced in Junos OS Release 8.0.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
The lower threshold is expressed as a percentage of the maximum possible value for the sampled variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the **rising-threshold**.

**Options**  

- **percentage**—The lower threshold for the alarm entry.  
  - **Range:** 1 through 100  
  - **Default:** 70 percent of the maximum possible value

**Required Privilege Level**  
- snmp—To view this statement in the configuration.  
- snmp-control—To add this statement to the configuration.

**Related Documentation**  
- [Configuring the Falling Threshold or Rising Threshold](#)  
- rising-threshold (SNMP Health Monitor) on page 3666
falling-threshold

Syntax  falling-threshold integer;

Hierarchy Level  [edit snmp rmon alarm index]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  The lower threshold for the sampled variable. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval is greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is less than or equal to this threshold, and the associated startup-alarm value is equal to falling-alarm value or rising-or-falling-alarm value. After a falling event is generated, another falling event cannot be generated until the sampled value rises above this threshold and reaches the rising-threshold.

Options  integer—The lower threshold for the alarm entry.
Range:  -2,147,483,648 through 2,147,483,647
Default:  20 percent less than rising-threshold

Required Privilege  snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring the Falling Threshold or Rising Threshold
• rising-threshold (SNMP RMON) on page 3667
falling-threshold-interval

Syntax  
falling-threshold-interval seconds;

Hierarchy Level  
[edit snmp rmon alarm index]

Release Information  
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Interval between samples when the rising threshold is crossed. Once the alarm crosses
the falling threshold, the regular sampling interval is used.

Options  
seconds—Time between samples, in seconds.

Range: 1 through 2,147,483,647 seconds
Default: 60 seconds

Required Privilege Level  
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  
- Configuring the Falling Threshold Interval
- interval (SNMP RMON) on page 3654

filter-duplicates

Syntax  
filter-duplicates;

Hierarchy Level  
[edit snmp]

Release Information  
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Filter duplicate Get, GetNext, or GetBulk SNMP requests.

Required Privilege Level  
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  
- Filtering Duplicate SNMP Requests
filter-interfaces

Syntax

```
filter-interfaces {
    interfaces {
        all-internal-interfaces;
        interface 1;
        interface 2;
    }
}
```

Hierarchy Level
[edits snmp]

Release Information
Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 9.4 for EX Series Switches.

Description
Filter out information related to specific interfaces from the output of SNMP Get and GetNext requests performed on interface-related MIBs.

Options
- **all-internal-interfaces**—Filters out information from SNMP Get and GetNext requests for the specified interfaces.
- **interfaces**—Specifies the interfaces to filter out from the output of SNMP Get and GetNext requests.

NOTE: Starting with Release 12.1, Junos OS provides an except option (! operator) that enables you to filter out all interfaces except those interfaces that match the regular expressions prefixed with the ! mark.

Required Privilege
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

Related Documentation
- Filtering Interface Information Out of SNMP Get and GetNext Output
**group (Configuring Access Privileges)**

**Syntax**
```
group.group-name {
    (default-context-prefix | context-prefix context-prefix)
    security-model (any | usm | v1 | v2c) {
        security-level (authentication | none | privacy) {
            notify-view view-name;
            read-view view-name;
            write-view view-name;
        }
    }
}
```

**Hierarchy Level**
[edit snmp v3 vacm access]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Assign the security name to a group, and specify the SNMPv3 context applicable to the group. The `default-context-prefix` statement, when included, adds all the contexts configured on the device to the group, whereas the `context-prefix context-prefix` statement enables you to specify a context and to add that particular context to the group.

(Not applicable to the QFX Series.) When the context prefix is specified as default (for example, `context-prefix default`), the context associated with the master routing instance is added to the group. To specify a routing instance that is part of a logical system, specify it as `logical system/routing instance`. For example, to specify routing instance ri1 in logical system ls1, include `context-prefix ls1/ri1`.

The remaining statements under this hierarchy are explained separately.

**Options**
- `group-name`—SNMPv3 group name created for the SNMPv3 group.

**Required Privilege Level**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring the Group
**group (Associating a Security Name)**

**Syntax**

```
group group-name;
```

**Hierarchy Level**

```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)
    security-name security-name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Associate a security name with a group composed of users with the same access privileges. The security name is used during authentication of SNMP messages, and is mapped to a username.

**Options**

- `group-name`—Collection of SNMP security names that share the same SNMPv3 access privileges.

**Required Privilege**

- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**

- Configuring the Group

---

**health-monitor**

**Syntax**

```
health-monitor {
    falling-threshold percentage;
    interval seconds;
    rising-threshold percentage;
}
```

**Hierarchy Level**

```
[edit snmp]
```

**Release Information**

Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure health monitoring.

The remaining statements are explained separately.

**Required Privilege**

- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Health Monitoring on Devices Running Junos OS
**history**

**Syntax**

```plaintext
history history-index {
    bucket-size number;
    interface (SNMP RMON History) interface-name;
    interval seconds;
    owner owner-name;
}
```

**Hierarchy Level**

[edit snmp rmon]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure RMON history group entries. This RMON feature can be used with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments. It collects statistics in accordance with user-configurable parameters.

The history group controls the periodic statistical sampling of data from various types of networks. This group contains configuration entries that specify an interface, polling period, and other parameters. The `interface (SNMP RMON History) interface-name` statement is mandatory. Other statements in the history group are optional.

**Default**

Not configured.

**Options**

- `history-index`—identifies this history entry as an integer.
  
  **Range:** 1 through 655535

**Required Privilege Level**

- snmp—To view this statement in the configuration.
- snmp—control—To add this statement to the configuration.

**Related Documentation**

- Configuring SNMP (J-Web Procedure) on page 3594
- Junos OS Network Management Configuration Guide
interface (SNMP RMON History)

Syntax  
interface interface-name;

Hierarchy Level  
[edit snmp rmon history history-index]

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Specify the interface to be monitored in the specified RMON history entry. Only one interface can be specified for a particular RMON history index. There is a one-to-one relationship between the interface and the history index. The interface must be specified in order for the RMON history to be created.

Options  
interface-name—Specify the interface to be monitored within the specified entry of the RMON history of Ethernet statistics.

Required Privilege
Level  
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  
• Configuring SNMP (J-Web Procedure) on page 3594
• Junos OS Network Management Configuration Guide

interface (SNMP)

Syntax  
interface [ interface-names ];

Hierarchy Level  
[edit snmp]

Release Information  

Description  
Configure the interfaces on which SNMP requests can be accepted.

Default  
If you omit this statement, SNMP requests entering the router or switch through any interface are accepted.

Options  
interface-names—Names of one or more logical interfaces.

Required Privilege
Level  
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  
• Configuring the Interfaces on Which SNMP Requests Can Be Accepted
interval

Syntax    interval seconds;

Hierarchy Level    [edit snmp rmon history]

Release Information    Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description    Configure the interval over which data is to be sampled for the specified interface.

Default    1800 sec

Options    seconds—Interval at which data is to be sampled for the specified interface.

Required Privilege Level    

snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

interval (SNMP Health Monitor)

Syntax    interval seconds;

Hierarchy Level    [edit snmp health-monitor]

Release Information    Statement introduced in Junos OS Release 8.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description    Interval between samples.

Options    seconds—Time between samples, in seconds.
Range: 1 through 2147483647 seconds
Default: 300 seconds

Required Privilege Level    

snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation    • Configuring the Interval
interval (SNMP RMON)

Syntax  interval seconds;

Hierarchy Level  [edit snmp rmon alarm index]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Interval between samples.

Options  seconds—Time between samples, in seconds.
Range: 1 through 2,147,483,647 seconds
Default: 60 seconds

Required Privilege Level  snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring the Interval

location (SNMP)

Syntax  location location;

Hierarchy Level  [edit snmp]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Define the value of the MIB II sysLocation object, which is the physical location of the managed system.

Options  location—Location of the local system. You must enclose the name within quotation marks (" ").

Required Privilege Level  snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring the System Location for a Device Running Junos OS
logical-system (SNMP)

Syntax
logical-system logical-system-name {
    routing-instance routing-instance-name;
}

Hierarchy Level
[edit snmp community community-name],
[edit snmp trap-options],
[edit snmp v3target-address target-address-name]

Release Information
Statement introduced in Junos OS Release 9.3
Statement introduced in Junos OS Release 9.0 for EX Series switches.

NOTE: The logical-system statement replaces the logical-router statement, and is backward-compatible with Junos OS Release 8.3 and later.

Description
Specify a logical system name for SNMP v1 and v2c clients.

Include at the [edit snmp trap-options] hierarchy level to specify a logical-system address as the source address of an SNMP trap.

Include at the [edit snmp v3 target-address] hierarchy level to specify a logical-system name as the destination address for an SNMPv3 trap or inform.

Options
logical-system-name—Name of the logical system.

routing-instance routing-instance-name—Statement to specify a routing instance associated with the logical system.

Required Privilege Level
snmp—to view this statement in the configuration.

snmp-control—to add this statement to the configuration.

Related Documentation
• Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community
• Configuring the Trap Target Address
message-processing-model

Syntax  
message-processing-model (v1 | v2c | v3);

Hierarchy Level  
[edit snmp v3 target-parameters target-parameter-name parameters]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Configure the message processing model to be used when generating SNMP notifications.

Options  
v1—SNMPv1 message process model.

v2c—SNMPv2c message process model.

v3—SNMPv3 message process model.

Required Privilege Level  
snmp—to view this statement in the configuration.
snmp-control—to add this statement to the configuration.

Related Documentation  
• Configuring the Message Processing Model

name

Syntax  
name name;

Hierarchy Level  
[edit snmp]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Set the system name from the command-line interface.

Options  
name—System name override.

Required Privilege Level  
snmp—to view this statement in the configuration.
snmp-control—to add this statement to the configuration.

Related Documentation  
• Configuring the System Name
nonvolatile

Syntax:  
```
nonvolatile {
  commit-delay seconds;
}
```

Hierarchy Level: [edit snmp]

Release Information:  
Statement introduced before Junos OS Release 7.4. The `commit-delay` statement introduced in Junos OS Release 9.0 for EX Series switches.

Description:  
Conﬁgure options for SNMP Set requests.

The statement is explained separately.

Required Privilege Level:  
- snmp—To view this statement in the conﬁguration.
- snmp-control—To add this statement to the conﬁguration.

Related Documentation:  
- Configuring the Commit Delay Timer
- `commit-delay` on page 3637
**notify**

**Syntax**
```
notify name {
    tag tag-name;
    type (trap | inform);
}
```

**Hierarchy Level**
[edit snmp v3]

**Release Information**
Statement introduced before Junos OS Release 7.4.
*type inform* option added in Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Select management targets for SNMPv3 notifications as well as the type of notifications. Notifications can be either traps or informs.

**Options**
- `name`—Name assigned to the notification.
- `tag-name`—Notifications are sent to all targets configured with this tag.
- `type`—Notification type is `trap` or `inform`. Traps are unconfirmed notifications. Informs are confirmed notifications.

**Required Privilege Level**
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**
- *Configuring the Inform Notification Type and Target Address*
- *Configuring the SNMPv3 Trap Notification*
notify-filter (Applying to the Management Target)

Syntax

```
notify-filter profile-name;
```

Hierarchy Level

```
[edit snmpv3 target-parameters target-parameters-name]
```

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the notify filter applied to a specific set of SNMPv3 target parameters. Target parameters are the message processing and security parameters for notifications sent to a target SNMP manager.

Options

- **profile-name**—Name of the notify filter to apply to notifications.

Required Privilege Level

- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

Related Documentation

- [Applying the Trap Notification Filter](#)

notify-filter (Configuring the Profile Name)

Syntax

```
notify-filter profile-name {
  oid oid (include | exclude);
}
```

Hierarchy Level

```
[edit snmp v3]
```

Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Specify a group of MIB objects for which you define access. The notify filter limits the type of traps or informs sent to the network management system.

Options

- **profile-name**—Name assigned to the notify filter.

The remaining statement is explained separately.

Required Privilege Level

- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

Related Documentation

- [Configuring the Trap Notification Filter](#)
- [oid (SNMP) on page 3660](#)
**notify-view**

**Syntax**
```
notify-view view-name;
```

**Hierarchy Level**
```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Associate the notify view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

**Options**
- `view-name`—Name of the view to which the SNMP user group has access.

**Required Privilege**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring MIB Views
- Configuring the Notify View

**oid (SNMP)**

**Syntax**
```
oid oid (include | exclude):
```

**Hierarchy Level**
```
[edit snmp v3 notify-filter profile-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Specify an object identifier (OID) used to represent a subtree of MIB objects. This OID is a prefix that the represented MIB objects have in common.

**Options**
- `exclude`—Exclude the subtree of MIB objects represented by the specified OID.
- `include`—Include the subtree of MIB objects represented by the specified OID.
- `oid`—Object identifier used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

**Required Privilege**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring the Trap Notification Filter
oid

Syntax  oid object-identifier (exclude | include);

Hierarchy Level  [edit snmp view view-name]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify an object identifier (OID) used to represent a subtree of MIB objects.

Options  exclude—Exclude the subtree of MIB objects represented by the specified OID.
include—Include the subtree of MIB objects represented by the specified OID.

object-identifier—OID used to represent a subtree of MIB objects. All MIB objects represented by this statement have the specified OID as a prefix. You can specify the OID using either a sequence of dotted integers or a subtree name.

Required Privilege  Level
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring MIB Views

owner

Syntax  owner owner-name;

Hierarchy Level  [edit snmp rmon history]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify the user or group responsible for this configuration.

Options  owner-name—The user or group responsible for this configuration.

Range: 0 through 32 alphanumeric characters

Required Privilege  Level
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring SNMP (J-Web Procedure) on page 3594
• Junos OS Network Management Configuration Guide
parameters

Syntax

```
parameters {
  message-processing-model (v1 | v2c | v3);
  security-level (none | authentication | privacy);
  security-model (usm | v1 | v2c);
  security-name security-name;
}
```

Hierarchy Level

[edit snmp v3 target-parameters target-parameters-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure a set of target parameters for message processing and security.
The remaining statements are explained separately.

Required Privilege

Level

snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation

• Defining and Configuring the Trap Target Parameters

port (SNMP)

Syntax

```
port port-number;
```

Hierarchy Level

[edit snmp v3 target-address target-address-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure a UDP port number for an SNMP target.

Default

If you omit this statement, the default port is 162.

Options

```
port-number—Port number for the SNMP target.
```

Required Privilege

Level

snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation

• Configuring the Port

Copyright © 2013, Juniper Networks, Inc.
### read-view

**Syntax**  
read-view view-name;

**Hierarchy Level**  
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]

**Release Information**  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**  
Associate the read-only view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

**Options**  
`view-name`—The name of the view to which the SNMP user group has access.

**Required Privilege**  
- `snmp`—To view this statement in the configuration.  
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**  
- Configuring the Read View  
- Configuring MIB Views
**request-type**

**Syntax**

```
request-type (get-next-request | get-request | walk-request);
```

**Hierarchy Level**

```
[edit snmp rmon alarm index]
```

**Release Information**

Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Extend monitoring to a specific SNMP object instance (**get-request**), or extend monitoring to all object instances belonging to a MIB branch (**walk-request**), or extend monitoring to the next object instance after the instance specified in the configuration (**get-next-request**).

**Options**

- **get-next-request**—Performs an SNMP get next request.
- **get-request**—Performs an SNMP get request.
- **walk-request**—Performs an SNMP walk request.

**Default**: walk-request

**Required Privilege**

- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring the Request Type
- variable on page 3697
rising-event-index

Syntax  rising-event-index index;

Hierarchy Level  [edit snmp rmon alarm index]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Index of the event entry that is used when a rising threshold is crossed. If this value is zero, no event is triggered.

Options  index—Index of the event entry that is used when a rising threshold is crossed.
Range:  0 through 65,535
Default:  0

Required Privilege Level  snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring the Falling Event Index or Rising Event Index
• falling-event-index on page 3644
**rising-threshold (SNMP Health Monitor)**

**Syntax**  
`rising-threshold percentage;`

**Hierarchy Level**  
[edit snmp ]

**Release Information**  
Statement introduced in Junos OS Release 8.0.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
The upper threshold is expressed as a percentage of the maximum possible value for the sampled variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the **falling-threshold**.

**Options**  
`percentage`—The lower threshold for the alarm entry.  
**Range:** 1 through 100  
**Default:** 80 percent of the maximum possible value

**Required Privilege**  
- snmp—To view this statement in the configuration.  
- snmp-control—To add this statement to the configuration.

**Related Documentation**  
- [falling-threshold on page 3645](#)  
- *Configuring the Falling Threshold or Rising Threshold*
**rising-threshold (SNMP RMON)**

**Syntax**

```plaintext
rising-threshold integer;
```

**Hierarchy Level**

```plaintext
[edit snmp rmon alarm index]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Upper threshold for the sampled variable. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval is less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes valid is greater than or equal to this threshold, and the associated startup alarm value is equal to the falling alarm or rising or falling alarm value. After a rising event is generated, another rising event cannot be generated until the sampled value falls below this threshold and reaches the falling threshold.

**Options**

```plaintext
integer—The lower threshold for the alarm entry.
```

**Range:**

```plaintext
–2,147,483,648 through 2,147,483,647
```

**Required Privilege**

```plaintext
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.
```

**Related Documentation**

- Configuring the Falling Threshold or Rising Threshold
- falling-threshold on page 3646

---

**rmon**

**Syntax**

```plaintext
rmon { ... }
```

**Hierarchy Level**

```plaintext
[edit snmp]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Configure Remote Monitoring.

**Required Privilege**

```plaintext
snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.
```

**Related Documentation**

- Configuring an Alarm Entry and Its Attributes
rmon

Syntax

rmon {  
  history history-index {  
    interface (SNMP RMON History) interface-name;  
    bucket-size number;  
    interval seconds;  
    owner owner-name;  
  }  
}

Hierarchy Level
[edit snmp]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
RMON is an existing feature of Junos OS.

The RMON specification provides network administrators with comprehensive network fault diagnosis, planning, and performance tuning information. It delivers this information in nine groups of monitoring elements, each providing specific sets of data to meet common network monitoring requirements. Each group is optional, so that vendors do not need to support all the groups within the MIB.

Junos OS supports RMON Statistics, History, Alarm, and Event groups. The EX Series documentation describes only the rmon history statement, which was added with this release.

The statements are explained separately.

Default
Disabled.

Required Privilege
snmp—to view this statement in the configuration.
snmp-control—to add this statement to the configuration.

Related Documentation
• Configuring SNMP (J-Web Procedure) on page 3594
• Junos OS Network Management Configuration Guide
routing-instance (SNMP)

Syntax

routeing-instance routing-instance-name;

Hierarchy Level

[edit snmp community community-name],
[edit snmp community community-name logical-system logical-system-name],
[edit snmp trap-group group]

Release Information

Statement introduced in Junos OS Release 8.3.
Added to the [edit snmp community community-name] hierarchy level in Junos OS Release 8.4.
Added to the [edit snmp community community-name logical-system logical-system-name] hierarchy level in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description

Specify a routing instance for SNMPv1 and SNMPv2 trap targets. All targets configured in the trap group use this routing instance.

If the routing instance is defined within a logical system, include the logical-system logical-system-name statement at the [edit snmp community community-name] hierarchy level and specify the routing-instance statement under the [edit snmp community community-name logical-system logical-system-name] hierarchy level.

Options

routeing-instance-name—Name of the routing instance.

Required Privilege Level

snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation

• Configuring SNMP Trap Groups
• Configuring the Source Address for SNMP Traps
• Specifying a Routing Instance in an SNMPv1 or SNMPv2c Community
### routing-instance (SNMPv3)

**Syntax**
```
routing-instance routing-instance-name:
```

**Hierarchy Level**
```
[edit snmp v3 target-address target-address-name]
```

**Release Information**
Statement introduced in Junos OS Release 8.3.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Specify a routing instance for an SNMPv3 trap target.

**Options**
- **routing-instance-name**—Name of the routing instance.

To configure a routing instance within a logical system, specify the logical system name followed by the routing instance name. Use a slash (/) to separate the two names (for example, test-ls/test-ri). To configure the default routing instance on a logical system, specify the logical system name followed by **default** (for example, test-ls/default).

**Required Privilege**
- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

**Related Documentation**
- Configuring the Trap Target Address

### sample-type

**Syntax**
```
sample-type (absolute-value | delta-value);
```

**Hierarchy Level**
```
[edit snmp rmon alarm index]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Method of sampling the selected variable.

**Options**
- **absolute-value**—Actual value of the selected variable is used when comparing against the thresholds.
- **delta-value**—Difference between samples of the selected variable is used when comparing against the thresholds.

**Required Privilege**
- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

**Related Documentation**
- Configuring the Sample Type
security-level (Defining Access Privileges)

Syntax

```plaintext
security-level (authentication | none | privacy) {
  notify-view view-name;
  read-view view-name;
  write-view view-name;
}
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define the security level used for access privileges.

Default

none

Options

- **authentication**—Provide authentication but no encryption.
- **none**—No authentication and no encryption.
- **privacy**—Provide authentication and encryption.

Required Privilege

- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

Related Documentation

- Configuring the Security Level
security-level (Generating SNMP Notifications)

**Syntax**
security-level (authentication | none | privacy);

**Hierarchy Level**
[edit snmp v3 target-parameters target-parameters-name parameters]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Configure the security level to use when generating SNMP notifications.

**Default**
none

**Options**
- **authentication**—Provide authentication but no encryption.
- **none**—No authentication and no encryption.
- **privacy**—Provide authentication and encryption.

**Required Privilege**
- snmp—to view this statement in the configuration.
- snmp-control—to add this statement to the configuration.

**Related Documentation**
- Configuring the Security Level
security-model (Access Privileges)

**Syntax**

security-model (usm | v1 | v2c);

**Hierarchy Level**

[edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix)]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Configure the security model for an SNMPv3 group. The security model is used to determine access privileges for the group.

**Options**

- **usm**—SNMPv3 security model.
- **v1**—SNMPv1 security model.
- **v2c**—SNMPv2c security model.

**Required Privilege**

- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring the Security Model
security-model (Group)

Syntax

security-model (usm | v1 | v2c) {
  security-name security-name {
    group group-name;
  }
}

Hierarchy Level

[edit snmp v3 vacm security-to-group]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Define a security model for an SNMPv3 group and associate the security name of a user with the group. All users in the group have the same access privileges.

Options

usm—SNMPv3 security model.

v1—SNMPv1 security model.

v2c—SNMPv2c security model.

Required Privilege Level

snmp—To view this statement in the configuration.

snmp-control—To add this statement to the configuration.

Related Documentation

• Configuring the Security Model
security-model (SNMP Notifications)

Syntax

security-model (usm | v1 | v2c);

Hierarchy Level
[edit snmp v3 target-parameters target-parameters-name parameters]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure the security model for an SNMPv3 group. The security model is used for SNMP notifications.

Options
usm—SNMPv3 security model.
v1—SNMPv1 security model.
v2c—SNMPv2c security model.

Required Privilege
snmp—to view this statement in the configuration.
snmp-control—to add this statement to the configuration.

Related Documentation
• Configuring the Security Model
**security-name (Security Group)**

**Syntax**
```
security-name security-name {
  group group-name;
}
```

**Hierarchy Level**
```
[edit snmp v3 vacm security-to-group security-model (usm | v1 | v2c)]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Associate the security name of a user (for SNMPv3 clients) or a community string (for SNMPv1 and SNMPv2c clients) with a configured security group.

**Options**
- `security-name`—SNMPv3 secure username configured at the `[edit snmp v3 usm local-engine user username]` hierarchy level that is used for messaging security. For SNMPv1 and SNMPv2c, the security name is the community string configured at the `[edit snmp v3 snmp-community community-index]` hierarchy level.

**Required Privilege**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- Assigning Security Names to Groups
- Assigning a Security Name to a Group
security-name (Community String)

**Syntax**
security-name security-name;

**Hierarchy Level**
[edit snmp v3 snmp-community community-index]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Associate a community string with the security name of a user. The community string, which is used for SNMPv1 and SNMPv2c clients in an SNMPv3 system, is configured at the [edit snmp v3 snmp-community community-index] hierarchy level.

**Options**
security-name—Name that is used for messaging security and user access control.

**NOTE:** The security name must match the configured security name at the [edit snmp v3 target-parameters target-parameters-name parameters] hierarchy level when you configure traps or informs.

**Required Privilege**
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**
- Configuring the Security Names
security-name (SNMP Notifications)

Syntax

security-name security-name;

Hierarchy Level

[edit snmp v3 target-parameters target-parameters-name parameters]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description

Configure the security name used when generating SNMP notifications.

Options

security-name—If the SNMPv3 USM security model is used, identify the user when generating the SNMP notification. If the v1 or v2c security models are used, identify the SNMP community used when generating the notification.

NOTE: The access privileges for the group associated with this security name must allow this notification to be sent.

If you are using the v1 or v2 security models, the security name at the [edit snmp v3 vacm security-to-group] hierarchy level must match the security name at the [edit snmp v3 snmp-community community-index] hierarchy level.

Required Privilege

snmp—to view this statement in the configuration.

snmp-control—to add this statement to the configuration.

Related Documentation

• Configuring the Security Name
**security-to-group**

**Syntax**
```
security-to-group {
  security-model (usm | v1 | v2c) {
    group group-name;
    security-name security-name;
  }
}
```

**Hierarchy Level**
[edit snmpv3 vacm]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Configure the group to which a specific SNMPv3 security name belongs. The security name is used for messaging security.

The remaining statements are explained separately.

**Required Privilege**
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**
- Assigning Security Model and Security Name to a Group

**snmp**

**Syntax**
```
snmp{...}
```

**Hierarchy Level**
[edit]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure SNMP.

SNMP modules cannot have the slash (/) character or the @ character in the name.

**Required Privilege**
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**
- Configuring SNMP on a Device Running Junos OS
**snmp**

Syntax

```
snmp {
  rmon {
    history index {
      interface (SNMP RMON History) interface-name;
      bucket-size number;
      interval seconds;
      owner owner-name;
    }
  }
}
```

Hierarchy Level  [edit]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure SNMP.

The statements are explained separately.

Required Privilege Level

- snmp—to view this statement in the configuration.
- snmp-control—to add this statement to the configuration.

Related Documentation

- Configuring SNMP (J-Web Procedure) on page 3594
**snmp-community**

**Syntax**
```
snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
}
```

**Hierarchy Level**
```
[edit snmp v3]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Configure the SNMP community which authorizes SNMPv1 or SNMPv2c clients in an SNMPv3 system.

**Options**
- `community-index`—(Optional) String that identifies an SNMP community.

The remaining statements are explained separately.

**Required Privilege**
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**
- *Configuring the SNMPv3 Community*
source-address (SNMP)

**Syntax**
```
source-address address;
```

**Hierarchy Level**
```
[edit snmp trap-options]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Set the source address of every SNMP trap packet sent by this router to a single address regardless of the outgoing interface. If the source address is not specified, the default is to use the address of the outgoing interface as the source address.

**Options**
- **address**—Source address of SNMP traps. You can configure the source address of trap packets two ways: *lo0* or a valid IPv4 address configured on one of the router interfaces. The value *lo0* indicates that the source address of all SNMP trap packets is set to the lowest loopback address configured at interface *lo0*.

  **Default:** Disabled. (The source address is the address of the outgoing interface.)

**Required Privilege**
- **snmp**—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

**Related Documentation**
- Configuring the Source Address for SNMP Traps
**startup-alarm**

**Syntax**
startup-alarm (falling-alarm | rising-alarm | rising-or-falling-alarm);

**Hierarchy Level**
[edit snmp rmon alarm index]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
The alarm that can be sent upon entry startup.

**Options**
- **falling-alarm**—Generated if the first sample after the alarm entry becomes active is less than or equal to the falling threshold.
- **rising-alarm**—Generated if the first sample after the alarm entry becomes active is greater than or equal to the rising threshold.
- **rising-or-falling-alarm**—Generated if the first sample after the alarm entry becomes active satisfies either of the corresponding thresholds.

**Default:** rising-or-falling-alarm

**Required Privilege**
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**
- Configuring the Sample Type

**syslog-subtag**

**Syntax**
syslog-subtag syslog-subtag;

**Hierarchy Level**
[edit snmp rmon alarm index]

**Release Information**
Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Add a tag to the system log message.

**Options**
- **syslog-subtag syslog-subtag**—Tag of not more than 80 uppercase characters to be added to syslog messages.

**Default:** None

**Required Privilege**
- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**
- Configuring the System Log Tag
tag (SNMPv3)

Syntax:  tag tag-name;

Hierarchy Level: [edit snmp v3 notify name],
[edit snmp v3 snmp-community community-index]

Release Information: Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description: Configure a set of targets to receive traps or informs (for IPv4 packets only).

Options: tag-name—Identifies the address of managers that are allowed to use a community string.

Required Privilege Level: snmp—to view this statement in the configuration.
snmp-control—to add this statement to the configuration.

Related Documentation: • Configuring the Tag
• Configuring the SNMPv3 Trap Notification

tag-list

Syntax:  tag-list tag-list;

Hierarchy Level: [edit snmp v3 target-address target-address-name]

Release Information: Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description: Configure an SNMP tag list used to select target addresses.

Options: tag-list—Define sets of target addresses (tags). To specify more than one tag, specify the tag names as a space-separated list enclosed within double quotes.

Required Privilege Level: snmp—to view this statement in the configuration.
snmp-control—to add this statement to the configuration.

Related Documentation: • Configuring the Trap Target Address
target-address

Syntax  

```plaintext
target-address target-address-name {
  address address;
  address-mask address-mask;
  logical-system (SNMP logical-system;
  port (SNMP) port-number;
  retry-count (SNMPv3) number;
  routing-instance (SNMPv3) instance;
  tag-list tag-list;
  target-parameters target-parameters-name;
  timeout seconds;
}
```

Hierarchy Level  [edit snmp v3]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure the address of an SNMP management application and the parameters to be used in sending notifications.

Options  target-address-name—String that identifies the target address.

The remaining statements are explained separately.

Required Privilege Level  

- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

Related Documentation  

- Configuring the Trap Target Address
**target-parameters**

**Syntax**  At the [edit snmp v3] hierarchy level:

```plaintext
target-parameters target-parameters-name {
  profile-name;
  parameters {
    message-processing-model (v1 | v2c | V3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
```

At the [edit snmp v3 target-address target-address-name] hierarchy level:

```plaintext
target-parameters target-parameters-name;
```

**Hierarchy Level**  [edit snmp v3]
[edit snmp v3 target-address target-address-name]

**Release Information**  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**  Configure the message processing and security parameters for sending notifications to a particular management target. The target parameters are configured at the [edit snmp v3] hierarchy level. The remaining statements at this level are explained separately.

Then apply the target parameters configured at the [edit snmp v3 target-parameters target-parameters-name] hierarchy level to the target address configuration at the [edit snmp v3] hierarchy level.

**Required Privilege Level**  snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

**Related Documentation**  • Defining and Configuring the Trap Target Parameters
• Applying Target Parameters
targets

Syntax  targets {
       address;
    }

Hierarchy Level  [edit snmp trap-group group-name]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure one or more systems to receive SNMP traps.

Options  address—IPv4 or IPv6 address of the system to receive traps. You must specify an address, not a hostname.

Required Privilege Level  snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring SNMP Trap Groups
traceoptions (SNMP)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
```

Hierarchy Level

[edit snmp]

Release Information

Statement introduced before Junos OS Release 7.4.
```
file filename
```
option added in Junos OS Release 8.1.
```
world-readable | no-world-readable
```
option added in Junos OS Release 8.1.
```
match regular-expression
```
option added in Junos OS Release 8.1.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

The output of the tracing operations is placed into log files in the /var/log directory. Each log file is named after the SNMP agent that generates it. Currently, the following logs are created in the /var/log directory when the traceoptions statement is used:

- chassisd
- craftd
- ilmid
- mib2d
- rmopd
- serviced
- snmpd

Options

```
file filename
```
—By default, the name of the log file that records trace output is the name of the process being traced (for example, mib2d or snmpd). Use this option to specify another name.

```
files number
```
—(Optional) Maximum number of trace files per SNMP subagent. When a trace file (for example, snmpd) reaches its maximum size, it is archived by being renamed to snmpd.0. The previous snmpd.1 is renamed to snmpd.2, and so on. The oldest archived file is deleted.

Range: 2 through 1000 files

Default: 10 files

```
flag flag
```
—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements:

- all—Log all SNMP events.
- configuration—Log reading of configuration at the [edit snmp] hierarchy level.
- **database**—Log events involving storage and retrieval in the events database.
- **events**—Log important events.
- **general**—Log general events.
- **interface-stats**—Log physical and logical interface statistics.
- **nonvolatile-sets**—Log nonvolatile SNMP set request handling.
- **pdu**—Log SNMP request and response packets.
- **policy**—Log policy processing.
- **protocol-timeouts**—Log SNMP response timeouts.
- **routing-socket**—Log routing socket calls.
- **server**—Log communication with processes that are generating events.
- **subagent**—Log subagent restarts.
- **timer-events**—Log internally generated events.
- **varbind-error**—Log variable binding errors.

**match regular-expression**—(Optional) Refine the output to include lines that contain the regular expression.

**size size**—(Optional) Maximum size, in kilobytes (KB), of each trace file before it is closed and archived.

- **Range:** 10 KB through 1 GB
- **Default:** 1000 KB

**world-readable | no-world-readable**—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

**Required Privilege**
- **Level:** snmp—To view this statement in the configuration.
- **snmp-control**—To add this statement to the configuration.

**Related Documentation**
- *Tracing SNMP Activity on a Device Running Junos OS*
**trap-group**

**Syntax**

```
trap-group group-name {
  categories {
    category;
  }
  destination-port port-number;
  routing-instance instance;
  targets {
    address;
  }
  version (all | v1 | v2);
}
```

**Hierarchy Level**  [edit snmp]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Create a named group of hosts to receive the specified trap notifications. The name of the trap group is embedded in SNMP trap notification packets as one variable binding (varbind) known as the community name. At least one trap group must be configured for SNMP traps to be sent.

**Options**

`group-name`—Name of the trap group. If the name includes spaces, enclose it in quotation marks (" ").

The remaining statements are explained separately.

**Required Privilege**

- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

**Related Documentation**

- Configuring SNMP Trap Groups
trap-options

Syntax

```
trap-options {
    agent-address outgoing-interface;
    source-address address;
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Using SNMP trap options, you can set the source address of every SNMP trap packet sent by the router or switch to a single address, regardless of the outgoing interface. In addition, you can set the agent address of each SNMPv1 trap. For more information about the contents of SNMPv1 traps, see RFC 1157.

The remaining statements are explained separately.

Default

Disabled

Required Privilege

- snmp—to view this statement in the configuration.
- snmp-control—to add this statement to the configuration.

Related Documentation

- Configuring SNMP Trap Options
**type (SNMP RMON)**

**Syntax**

```plaintext
type type;
```

**Hierarchy Level**

```plaintext
[edit snmp rmon event index]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Type of notification generated when a threshold is crossed.

**Options**

- `type`—Type of notification:
  - `log`—Add an entry to `logTable`.
  - `log-and-trap`—Send an SNMP trap and make a log entry.
  - `none`—No notifications are sent.
  - `snmptrap`—Send an SNMP trap.

**Default:** `log-and-trap`

**Required Privilege**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- *Configuring an Event Entry and Its Attributes*
type (SNMPv3)

**Syntax**

```
type (inform | trap);
```

**Hierarchy Level**

```
[edit snmp v3 notify name]
```

**Release Information**

Statement introduced before Junos OS Release 7.4.

- `inform` option added in Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Configure the type of SNMP notification.

**Options**

- `inform`—Defines the type of notification as an inform. SNMP informs are confirmed notifications.
- `trap`—Defines the type of notification as a trap. SNMP traps are unconfirmed notifications.

**Required Privilege Level**

- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

**Related Documentation**

- [Configuring SNMP Informs](#)
- [Configuring the SNMPv3 Trap Notification](#)
v3

Syntax

```
v3 {
  notify name {
    tag tag-name;
    type trap;
  }
  notify-filter profile-name {
    oid object-identifier (include | exclude);
  }
  snmp-community community-index {
    community-name community-name;
    security-name security-name;
    tag tag-name;
  }
  target-address target-address-name {
    address address;
    address-mask address-mask;
    logical-system (SNMP logical-system;
    port port-number;
    retry-count number;
    routing-instance instance;
    tag-list tag-list;
    target-parameters target-parameters-name;
    timeout seconds;
  }
  target-parameters target-parameters-name {
    notify-filter profile-name;
    parameters {
      message-processing-model (v1 | v2c | V3);
      security-level (authentication | none | privacy);
      security-model (usm | v1 | v2c);
      security-name security-name;
    }
  }
  usm {
    local-engine {
      user username {
        authentication-md5 {
          authentication-password authentication-password;
        }
        authentication-sha {
          authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
        privacy-des {
          privacy-password privacy-password;
        }
      }
    }
  }
```
privacy-none;
}
}
remote-engine engine-id {
    user username {
        authentication-md5 {
            authentication-password authentication-password;
        }
        authentication-sha {
            authentication-password authentication-password;
        }
        authentication-none;
        privacy-aes128 {
            privacy-password privacy-password;
        }
        privacy-des {
            privacy-password privacy-password;
        }
        privacy-3des {
            privacy-password privacy-password;
        }
        privacy-none {
            privacy-password privacy-password;
        }
    }
}
}
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix)
            security-model (any | usm | v1 | v2c) {
                security-level (authentication | none | privacy) {
                    notify-view view-name;
                    read-view view-name;
                    write-view view-name;
                }
            }
        }
    }
}
security-to-group {
    security-model (usm | v1 | v2c) {
        security-name security-name {
            group group-name;
        }
    }
}
}

Hierarchy Level    [edit snmp]

Release Information  Statement introduced before Junos OS Release 7.4,
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description
Configure SNMPv3.

The remaining statements are explained separately.

Required Privilege
snmp—to view this statement in the configuration.

snmp-control—to add this statement to the configuration.

Related Documentation
- Minimum SNMPv3 Configuration on a Device Running Junos OS

Syntax
```yaml
vacm {
    access {
        group group-name {
            (default-context-prefix | context-prefix context-prefix) {
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    security-to-group {
        security-model (usm | v1 | v2c);
        security-name security-name {
            group group-name;
        }
    }
}
```

Hierarchy Level
```
[edit snmp v3]
```

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Configure view-based access control model (VACM) information, including access privileges such as security model and security level for a group of users.

The remaining statements are explained separately.

Required Privilege
snmp—to view this statement in the configuration.

snmp-control—to add this statement to the configuration.

Related Documentation
- Defining Access Privileges for an SNMP Group
variable

Syntax  variable oid-variable;

Hierarchy Level  [edit snmp rmon alarm index]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Object identifier (OID) of MIB variable to be monitored.

Options  oid-variable—OID of the MIB variable that is being monitored. The OID can be a dotted decimal (for example, 1.3.6.1.2.1.2.1.2.2.1.10.1). Alternatively, use the MIB object name (for example, ifInOctets.1).

Required Privilege Level  snmp—To view this statement in the configuration.
  snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring the Variable

version (SNMP)

Syntax  version (all | v1 | v2);

Hierarchy Level  [edit snmp trap-group group-name]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify the version number of SNMP traps.

Default  all—Send an SNMPv1 and SNMPv2 trap for every trap condition.

Options  all—Send an SNMPv1 and SNMPv2 trap for every trap condition.
  v1—Send SNMPv1 traps only.
  v2—Send SNMPv2 traps only.

Required Privilege Level  snmp—To view this statement in the configuration.
  snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring SNMP Trap Groups
view (Associating a MIB View with a Community)

Syntax  
```bash
view view-name;
```

Hierarchy Level  
```
[edit snmp community community-name]
```

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Associate a view with a community. A view represents a group of MIB objects.

Options  
- `view-name`—Name of the view. You must use a view name already configured in the `view` statement at the `[edit snmp]` hierarchy level.

Required Privilege  
- `snmp`—To view this statement in the configuration.
- `snmp-control`—To add this statement to the configuration.

Related Documentation  
- `Configuring the SNMP Community String`
view (Configuring a MIB View)

Syntax

```
view view-name {
    oid object-identifier (include | exclude);
}
```

Hierarchy Level

[edit snmp]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Define a MIB view. A MIB view identifies a group of MIB objects. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy. The `view` statement uses a view to specify a group of MIB objects on which to define access. To enable a view, you must associate the view with a community by including the `view` statement at the `[edit snmp community community-name]` hierarchy level.

NOTE: To remove an OID completely, use the `delete view all oid oid-number` command but omit the `include` parameter.

Options

`view-name`—Name of the view.

The remaining statement is explained separately.

Required Privilege Level

- snmp—To view this statement in the configuration.
- snmp-control—To add this statement to the configuration.

Related Documentation

- Configuring MIB Views
- Associating MIB Views with an SNMP User Group
- community on page 3638
write-view

Syntax  write-view view-name;

Hierarchy Level  [edit snmp v3 vacm access group group-name (default-context-prefix | context-prefix context-prefix) security-model (any | usm | v1 | v2c) security-level (authentication | none | privacy)]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series switches.

Description  Associate the write view with a community (for SNMPv1 or SNMPv2c clients) or a group name (for SNMPv3 clients).

Options  view-name—Name of the view for which the SNMP user group has write permission.

Required Privilege
Level  snmp—To view this statement in the configuration.
snmp-control—To add this statement to the configuration.

Related Documentation  • Configuring MIB Views
• Configuring the Write View

Configuration Statements: Analyzers and Port Mirroring

• [edit forwarding-options port-mirroring] Hierarchy Level on page 3700
• [edit forwarding-options analyzer] Hierarchy Level on page 3701

[edit forwarding-options port-mirroring] Hierarchy Level

forwarding-options {
  port-mirroring {
    family ethernet-switching {
      output {
        interface interface-name {
        }
      }
      no-filter-check;
      routing-instance instance-name {
        vlan vlan-name {
          no-tag;
        }
      }
      vlan vlan-name {
        no-tag;
      }
      instance instance-name {
      }
    }
  }
}
... same statements as at the [edit forwarding-options port-mirroring family ethernet-switching]...

}]
}
traceoptions {
   file filename{
      size maximum-file-size;
      files number
      no-world-readable | world-readable
      match regular-expression
   }
   no-remote-trace;
}

Related Documentation

- Notational Conventions Used in Junos OS Configuration Hierarchies
- [edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches

[edit forwarding-options analyzer] Hierarchy Level

forwarding-options {
   analyzer analyzer-name {
      input {
         egress {
            interface (all | interface-name);
         }
         ingress {
            interface (all | interface-name);
            routing-instance routing-instance-name {
               vlan (vlan-name | vlan-id | vlan-list);
            }
            vlan (vlan-name | vlan-id | vlan-list);
         }
      }
      output {
         interface interface-name;
         routing-instance routing-instance-name {
            vlan (vlan-name | vlan-id);
            no-tag;
         }
         vlan (vlan-name | vlan-id) {
            no-tag;
         }
      }
   }
}

Related Documentation

- Notational Conventions Used in Junos OS Configuration Hierarchies
**egress**

**Syntax**

```bash
text
```

**Hierarchy Level**

```
[edit vlans vlan-name vlan-id number interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 10.0 for EX Series switches.

**Description**

Specify that the member interface of the VLAN allows only egress traffic.

**Required Privilege Level**

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches](#)

---

**egress (Analyzer)**

**Syntax**

```bash
text
```

**Hierarchy Level**

```
[edit forwarding-options analyzer on page 3701 name input]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Specify ports for which traffic exiting the interface is mirrored in a mirroring configuration.

The remaining statements are explained separately.

**Required Privilege Level**

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

**Related Documentation**

- [Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches](#)
ingress (vlans)

Syntax

```plaintext
ingress;
```

Hierarchy Level

```plaintext
[edit vlans vlan-name vlan-id number interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description

Specify that the member interface of the VLAN allows only ingress traffic.

Required Privilege

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

Related Documentation

- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX Series Switches

ingress (Analyzer)

Syntax

```plaintext
ingress {
  interface (all | interface-name);
  routing-instance routing-instance-name {
    vlan (vlan-name | vlan-id | vlan-list);
  }
  vlan (vlan-id | vlan-name);
}
```

Hierarchy Level

```plaintext
[edit forwarding-options analyzer on page 3701 name input]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.


Description

Configure ports, routing instances, or VLANs for which the entering traffic is mirrored as part of a mirroring configuration.

The remaining statements are explained separately.

Required Privilege

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

Related Documentation

- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches on page 3580
input (Analyzer)

Syntax

```plaintext
input {
    ingress {
        interface (all | interface-name);
        routing-instance routing-instance-name {
            vlan (vlan-name | vlan-id | vlan-list);
        }
        vlan (vlan-id | vlan-name);
    }
    egress {
        interface (all | interface-name);
    }
}
```

Hierarchy Level
[edit forwarding-options analyzer on page 3701 name]

Release Information

Description
Define the traffic to be mirrored in a mirroring configuration—the definition can be a combination of:

- Packets entering or exiting a port
- Packets entering a VLAN

The remaining statements are explained separately.

Default
No default.

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570
- Understanding Port Mirroring and Analyzers on EX4300 Switches on page 3544
## interface

**Syntax**  
interface (all | interface-name);

**Hierarchy Level**  
[edit forwarding-options analyzer on page 3701 name input egress],  
[edit forwarding-options analyzer on page 3701 name input ingress],  
[edit forwarding-options analyzer on page 3701 name output]

**Release Information**  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  

**Description**  
Configure the interfaces for which traffic is mirrored.

**Options**  
- all—Apply mirroring to all interfaces on the switch. Mirroring a high volume of traffic can be performance intensive for the switch. Therefore, you should generally select specific input interfaces in preference to using the all keyword, or use the all keyword in combination with setting a ratio for statistical sampling.
- interface-name—Apply mirroring to the specified interface only.

**Required Privilege Level**  
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**  
- Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570
- Understanding Port Mirroring and Analyzers on EX4300 Switches on page 3544
no-tag

Syntax  no-tag;

Hierarchy Level  [edit forwarding-options analyzer on page 3701 name output vlan (vlan-id | vlan-name)]

Release Information  Statement introduced in Junos OS Release 11.3 for EX Series switches.

Description  Specify that remote mirroring packets are not tagged.

Required Privilege  Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
• Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570

output (Mirroring)

Syntax  output {
  interface interface-name;
  vlan (vlan-id | vlan-name) {
    no-tag;
  }
}

Hierarchy Level  [edit forwarding-options analyzer on page 3701 name]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Configure the destination for mirrored traffic, either an interface on the switch, for local monitoring, or a VLAN, for remote monitoring. You can optionally configure the no-tag statement so that remote port mirroring packets are not tagged.

The remaining statements are explained separately.

Required Privilege  Level  system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring Mirroring for Local Monitoring of Employee Resource Use on EX4300 Switches on page 3564
• Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570
### vlan (Mirroring)

**Syntax**

```plaintext
vlan (vlan-id | vlan-name) {
  no-tag;
}
```

**Hierarchy Level**

[edit forwarding-options analyzer on page 3701 name output]

**Release Information**


**Description**

Configure mirrored traffic to be sent to a VLAN for remote monitoring. On a destination (output) VLAN, you can also configure the no-tag statement.

**Options**

- `vlan-id`—Numeric VLAN identifier.
- `vlan-name`—Name of the VLAN.

The remaining statement is explained separately.

**Required Privilege Level**

- system—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use Through a Transit Switch on EX4300 Switches on page 3580
- Example: Configuring Mirroring for Remote Monitoring of Employee Resource Use on EX4300 Switches on page 3570

### Configuration Statements: sFlow Technology

- [edit protocols] Configuration Statement Hierarchy on EX4300 Switches on page 3707
- [edit protocols sflow] Configuration Statement Hierarchy on EX Series Switches on page 3708

### [edit protocols] Configuration Statement Hierarchy on EX4300 Switches

Each of the following topics lists the statements at a subhierarchy of the [edit protocols] hierarchy:

- [edit protocols bfd] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols bgp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches on page 1769
- [edit protocols igmp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols igmp-snooping] Configuration Statement Hierarchy on page 3329
[edit protocols isis] Configuration Statement Hierarchy on EX Series Switches

[edit protocols lacp] Configuration Statement Hierarchy on EX Series Switches on page 2398

[edit protocols l2-learning] Configuration Statement Hierarchy on EX Series Switches

[edit protocols layer2-control] Configuration Statement Hierarchy on EX Series Switches

[edit protocols lldp] Configuration Statement Hierarchy on EX Series Switches

[edit protocols lldp-med] Configuration Statement Hierarchy on EX Series Switches

[edit protocols mstp] Configuration Statement Hierarchy on EX Series Switches

[edit protocols mvrp] Configuration Statement Hierarchy on EX Series Switches

[edit protocols neighbor-discovery] Configuration Statement Hierarchy on EX Series Switches

[edit protocols oam] Configuration Statement Hierarchy on EX Series Switches

[edit protocols ospf] Configuration Statement Hierarchy on EX Series Switches

[edit protocols ospf3] Configuration Statement Hierarchy on EX Series Switches

[edit protocols pim] Configuration Statement Hierarchy on EX Series Switches

[edit protocols rip] Configuration Statement Hierarchy on EX Series Switches

[edit protocols ripng] Configuration Statement Hierarchy on EX Series Switches

[edit protocols router-advertisement] Configuration Statement Hierarchy on EX Series Switches

[edit protocols router-discovery] Configuration Statement Hierarchy on EX Series Switches

[edit protocols rstp] Configuration Statement Hierarchy on EX Series Switches

[edit protocols sflow] Configuration Statement Hierarchy on EX Series Switches on page 3708

[edit protocols uplink-failure-detection] Configuration Statement Hierarchy on EX Series Switches

[edit protocols vrrp] Configuration Statement Hierarchy on EX Series Switches

[edit protocols vstp] Configuration Statement Hierarchy on EX Series Switches

Related Documentation

EX Series Switch Software Features Overview

This topic lists supported and unsupported configuration statements in the [edit protocols sflow] hierarchy level on EX Series switches.

Supported statements are those that you can use to configure some aspect of a software feature on the switch.
• **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

• **Supported Statements in the [edit protocols sflow] Hierarchy Level**

• **Unsupported Statements in the [edit sflow] Hierarchy Level**

**Supported Statements in the [edit protocols sflow] Hierarchy Level**

The following hierarchy shows the [edit protocols sflow] configuration statements supported on EX Series switches:

```plaintext
sflow {
  agent-id;
  collector {
    ip-address;
    udp-port port-number;
  }
  interfaces interface-name {
    polling-interval seconds;
    sample-rate {
      egress number;
      ingress number;
    }
  }
  polling-interval seconds;
  sample-rate {
    egress number;
    ingress number;
  }
  source-ip;
}
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable >;
  flag (all | client-server | configuration | interface | rtsock);
}
```

**Unsupported Statements in the [edit sflow] Hierarchy Level**

All statements in the [edit protocols sflow] hierarchy level that are displayed in the command-line interface (CLI) on the EX Series switch are supported on the switch and operate as documented.

**Related Documentation**

• Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603

• [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
agent-id

Syntax
agent-id ip-address;

Hierarchy Level [edit protocols sflow]

Release Information Statement introduced in JUNOS Release 10.2 for EX Series switches.

Description Configure the IP address to be assigned as the agent ID for the sFlow agent. By assigning an IP address, you ensure that the IP address is not dynamic.

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603

collector

Syntax collector {
  ip-address;
  udp-port port-number;
}

Hierarchy Level [edit protocols sflow]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description Configure a remote collector for sFlow network traffic monitoring. The switch sends sFlow UDP datagrams to this collector for analysis. You can configure up to four collectors on the switch. You configure a collector by specifying its IP address and a UDP port.

The remaining statements are explained separately.

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
disable (sFlow Monitoring Technology)

**Syntax**
```plaintext
disable;
```

**Hierarchy Level**
```
[edit protocols sflow],
[edit protocols sflow interfaces interface-name]
```

**Release Information**
Statement introduced in Junos OS Release 9.3 for EX Series switches.

**Description**
Disable the sFlow monitoring protocol on all interfaces on the switch or on the specified interface.

**Required Privilege**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
interfaces (sFlow Monitoring Technology)

Syntax

```plaintext
interfaces interface-name {
  disable;
  polling-interval seconds;
  sample-rate {
    egress number;
    ingress number;
  }
}
```

Hierarchy Level

[edit protocols sflow]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description

Configure sFlow network traffic monitoring on the specified interface on the switch. You can configure sFlow parameters such as polling interval and sample rate with different values on different interfaces, and you can also disable sFlow monitoring on individual interfaces.

The remaining statements are explained separately.

Options

`interface-name`—Name of the interface on which to configure sFlow parameters.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
polling-interval

Syntax polling-interval seconds;

Hierarchy Level [edit protocols sflow],
              [edit protocols sflow interfaces interface-name]

Description Configure the interval (in seconds) that the switch waits between port statistics update messages. “Polling” refers to the switch's gathering various statistics for the network interfaces configured for sFlow monitoring and exporting the statistics to the configured sFlow collector.

Default If no polling interval is configured for a particular interface, the switch waits the number of seconds that is configured for the global sFlow configuration. If no global interval is configured, the switch waits 20 seconds between messages.

Options seconds—Number of seconds between port statistics update messages. A 0 (zero) value specifies that polling is disabled.

Range: 0–3600 seconds
Default: 20 seconds

Required Privilege Level routing—To view this statement in the configuration.
            routing-control—To add this statement to the configuration.

Related Documentation • [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
• Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
• Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
sample-rate

Syntax

```
sample-rate {
    egress number;
    ingress number;
}
```

Hierarchy Level

[edit protocols sflow],
[edit protocols sflow interfaces interface-name]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Option number (directly following sample-rate) deprecated and options egress number
and ingress number added in Junos OS Release 10.4 for EX Series switches.

Description

Set the ratios of the number of packets to be sampled in sFlow network traffic monitoring.
For example, if you specify a rate of 1000, every thousandth packet (1 packet out of 1000)
is sampled.

Default

By default, both ingress and egress sample rates are disabled if no global sample rate is
configured.

NOTE: The sample-rate number (the global sample-rate) statement has been
deprecated and might be removed from future product releases. We strongly
recommend that you phase out its use.

Options

egress number—Egress qualifier for the sample rate.
Range: 100–1073741823
Default: 2048

ingress number—Ingress qualifier for the sample rate.
Range: 100–1073741823
Default: 2048

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series
  Switches on page 3559
sflow

Syntax

```
sflow {
  agent-id ip-address;
  collector {
    ip-address;
    udp-port port-number;
  }
  disable;
  interfaces interface-name {
    disable;
    polling-interval seconds;
    sample-rate number;
  }
  polling-interval seconds;
  sample-rate number;
  source-ip ip-address;
}
```

Hierarchy Level

[edit protocols]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Options `agent-id` and `source-ip` added in Junos OS Release 10.2 for EX Series switches.

Description

Configure sFlow technology, designed for monitoring high-speed switched or routed networks, to continuously monitor traffic at wire speed on specified interfaces simultaneously. sFlow data can be used to provide network traffic visibility information.

The remaining statements are explained separately.

Default

The sFlow protocol is disabled by default.

Required Privilege Level

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

Related Documentation

- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
source-ip

Syntax  
source-ip ip-address;

Hierarchy Level  
[edit protocols sflow]

Release Information  
Statement introduced in JUNOS Release 10.2 for EX Series switches.

Description  
Configure the IP address to be used for the sFlow datagrams. By configuring an IP address, you ensure that the IP address is not dynamic.

Required Privilege Level  
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation  
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603

udp-port

Syntax  
udp-port port-number;

Hierarchy Level  
[edit protocols sflow collector]

Release Information  
Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description  
Configure the UDP port for a remote collector for sFlow network traffic monitoring. The switch sends sFlow UDP datagrams to the collector for analysis.

Options  
- port-number—UDP port number for this collector.
  Default: 6343

Required Privilege Level  
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation  
- [edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 3327
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603
Configuration Statements: Ethernet OAM Connectivity Fault Management

action-profile (Applying to OAM CFM, for EX Series Switch Only)

Syntax

```
action-profile profile-name {
  action {
    interface-down;
  }
  default-actions {
    interface-down;
  }
  event {
    adjacency-loss;
  }
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management]
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name mep mep-id remote-mep mep-id]
```

Release Information

Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description

Configure a name and default action for an action profile.

Options

- **profile-name**—Name of the action profile.
- **action**—Defines the action to be taken when connectivity to the remote MEP is lost.
- **interface-down**—Brings the interface down when a remote MEP connectivity failure is detected.
- **default-actions**—Defines the default action to be taken when connectivity to the remote MEP is lost.
- **interface-down**—Brings the interface down when a remote MEP connectivity failure is detected.
- **event**—Defines the event to be monitored when a remote MEP connectivity failure is detected.
- **adjacency-loss**—Defines the connectivity loss to the remote MEP.

Required Privilege

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

Related Documentation

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide
**age (EX Series Switch Only)**

**Syntax**

```plaintext
age (30m | 10m | 1m | 30s | 10s);
```

**Hierarchy Level**

```plaintext
[edit protocols oam ethernet connectivity-fault-management linktrace]
```

**Release Information**

Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Configure the time to wait (in minutes or seconds) for a response. If no response is received, the request and response entry is deleted from the linktrace database.

**Default**

10 minutes

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide

---

**auto-discovery (EX Series Switch Only)**

**Syntax**

```plaintext
auto-discovery;
```

**Hierarchy Level**

```plaintext
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]
```

**Release Information**

Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Enable the MEP to accept continuity check messages from all remote MEPs.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide
calculation-weight

Syntax  
\[
\text{calculation-weight} \{ \\
\text{delay} \text{delay-value} ; \\
\text{delay-variation} \text{delay-variation-value} ; \\
\}\n\]

Hierarchy Level  
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]

Release Information  
Statement introduced in Junos OS Release 11.1.  
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description  
Configure the calculation weight for delay and delay variation.

NOTE: This option is applicable only for two-way delay measurement.

The remaining statements are explained separately.

Required Privilege

Level

Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation

• Configuring an Iterator Profile
• Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621
• delay on page 3723
• delay-variation on page 3724
connectivity-fault-management (EX Series Switch Only)

**Syntax**

connectivity-fault-management {
  action-profile profile-name {
    action {
      interface-down;
    }
    default-actions {
      interface-down;
    }
    event {
      adjacency-loss;
    }
  }
}
linktrace {
  age (30m | 10m | 1m | 30s | 10s);
  path-database-size path-database-size;
}
maintenance-domain domain-name {
  level number;
  mip-half-function (none | default | explicit);
  name-format (character-string | none | dns | mac+2oct);
  maintenance-association ma-name {
    continuity-check {
      hold-interval minutes;
      interface-status-tlv;
      interval (10m | 10s | 1m | 1s | 100ms);
      loss-threshold number;
      port-status-tlv;
    }
    mep mep-id {
      auto-discovery;
      direction down;
      interface interface-name;
      remote-mep mep-id {
        action-profile profile-name;
      }
    }
  }
}
performance-monitoring {
  sla-iterator-profiles {
    profile-name {
      calculation-weight {
        delay delay-value;
        delay-variation delay-variation-value;
      }
      cycle-time cycle-time-value;
      iteration-period iteration-period-value;
      measurement-type two-way-delay;
      passive;
    }
  }
}
Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Configure connectivity fault management for IEEE 802.1ag Operation, Administration, and Management (OAM) support.

The remaining statements are explained separately.

Required Privilege
route—To view this statement in the configuration.
route-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide

continuity-check (EX Series Switch Only)

Syntax
continuity-check {
  hold-interval minutes;
  interface-status-tlv;
  interval (10m | 10s | 1m | 1s | 100ms);
  loss-threshold number;
  port-status-tlv;
}

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
  domain-name maintenance-association ma-name]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Specify continuity check protocol options.

The remaining statements are explained separately.

Options
interface-status-tlv—Includes interface status TLV in CCM.

port-status-tlv—Includes port status TLV in CCM.

The remaining statements are explained separately.

Required Privilege
route—To view this statement in the configuration.
route-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide
cycle-time

Syntax  
cycle-time cycle-time-value;

Hierarchy Level  
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]

Release Information  
Statement introduced in Junos OS Release 11.1.  
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description  
Configure the time (in milliseconds) taken between back-to-back transmissions of SLA frames for a single connection.

Options  
cycle-time-value—Cycle time value in milliseconds.  
Range: 10 through 3,600,000  
Default: 1000

Required Privilege Level  
Configure—To enter configuration mode.  
Control—To modify any configuration.

Related Documentation  
• Configuring an Iterator Profile  
• Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621
**delay**

**Syntax**  
`delay delay-value;`

**Hierarchy Level**  
`[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name calculation-weight]`

**Release Information**  
Statement introduced in Junos OS Release 11.1.  
Statement introduced in Junos OS Release 11.4 for EX Series switches.

**Description**  
Configure the calculation weight for delay.

**Options**  
`delay-value`—Calculation weight for delay.

---

**NOTE:** This option is applicable only for two-way delay measurement.

**Range:** 1 through 65,535  
**Default:** 1

**Required Privilege Level**  
Configure—To enter configuration mode.  
Control—To modify any configuration.

**Related Documentation**  
- Configuring an Iterator Profile  
- Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621  
- `calculation-weight` on page 3719
**delay-variation**

**Syntax**

```
delay-variation delay-variation-value;
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management performance-monitoring
  sla-iterator-profiles profile-name calculation-weight]
```

**Release Information**

Statement introduced in Junos OS Release 11.1.
Statement introduced in Junos OS Release 11.4 for EX Series switches.

**Description**

Configure the calculation weight for delay variation.

**Options**

```
delay-variation-value—Calculation weight for delay variation.
```

**NOTE:** This option is applicable only for two-way delay measurement.

**Range:** 1 through 65,535

**Default:** 1

**Required Privilege Level**

Configure—To enter configuration mode.
Control—To modify any configuration.

**Related Documentation**

- Configuring an Iterator Profile
- Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621
- calculation-weight on page 3719
direction (EX Series Switch Only)

Syntax
direction down;

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name mep mep-id]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Specify that connectivity fault management (CFM) packets (CCMs) be transmitted only in one direction for the MEP, that is, the direction be set as down so that CCMs are transmitted only out of (not into) the interface configured on this MEP.

Options
down—Down MEP CCMs are transmitted only out (not into) of the interface configured on this MEP.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide

hold-interval (OAM CFM, for EX Series Switch Only)

Syntax
hold-interval minutes;

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name continuity-check]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Configure the time to wait before flushing the maintenance association end point (MEP) database, if no updates occur.

Options
minutes—Time to wait, in minutes.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide
interface (OAM CFM, for EX Series Switch Only)

Syntax:  
interface (interface-name | ((ge- | xe-) (fpc/pic/port | fpc/pic/port.unit-number | fpc/pic/port.unit-number vlan vlan-id)));

Hierarchy Level:  
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name mep mep-id]

Release Information:  
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description:  
Configure IEEE 802.1ag Operation, Administration, and Management (OAM) Connectivity Fault Management (CFM) support for the specified interface.

Options:  
interface-name—Interface to which the MEP is attached. It can be a physical Ethernet interface or a logical interface. If the interface is a trunk interface, the VLAN associated with the interface must have a VLAN ID.

Required Privilege Level:  
routing—To view this statement in the configuration.
network-control—To add this statement to the configuration.

Related Documentation:  
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide
interval (EX Series Switch Only)

Syntax
interval (10m | 10s | 1m | 1s | 100ms | 10ms);

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name continuity-check]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Configure the time between continuity check messages.

Options
10m—10 minutes.
10s—10 seconds.
1m—1 minute.
1s—1 second.
100ms—100 milliseconds.
10ms—10 milliseconds.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide
iteration-period

Syntax  
iteration-period iteration-period-value;

Hierarchy Level  
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]

Release Information  
Statement introduced in Junos OS Release 11.1.  
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description  
Configure the iteration period, which is the maximum number of cycles per iteration (that is, the number of connections registered to an iterator cannot exceed this value).

Options  
iteration-period-value—Maximum number of cycles per iteration.  
Range: 1 through 2000  
Default: 2000

Required Privilege  
Level  
Configure—To enter configuration mode.  
Control—To modify any configuration.

Related Documentation  
• Configuring an Iterator Profile  
• Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621

level (EX Series Switch Only)

Syntax  
level number;

Hierarchy Level  
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]

Release Information  
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description  
Configure a number to be used in CFM messages to identify the maintenance association.

Options  
number—Number used to identify the maintenance domain to which the CFM message belongs.  
Range: 0 through 7

Required Privilege  
Level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

Related Documentation  
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612  
• Junos OS Network Interfaces Configuration Guide
**linktrace (EX Series Switch Only)**

**Syntax**

```plaintext
linktrace {
  age (30m | 10m | 1m | 30s | 10s);
  path-database-size <path-database-size>;
}
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management]
```

**Release Information**

Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Configure connectivity fault management linktrace parameters.

The remaining statements are explained separately.

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide

**loss-threshold (EX Series Switch Only)**

**Syntax**

```plaintext
loss-threshold number;
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name <domain-name> maintenance-association ma-name <ma-name> continuity-check]
```

**Release Information**

Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Configure the number of continuity check messages that can be lost before the remote MEP is marked as down.

**Options**

- **number**—Number of continuity check messages that can be lost before the remote MEP is marked down.

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide
maintenance-association (EX Series Switch Only)

Syntax

maintenance-association ma-name {
  continuity-check {
    hold-interval minutes;
    interface-status-tlv;
    interval (10m | 10s | 1m | 1s| 100ms);
    loss-threshold number;
    port-status-tlv;
  }
  mep mep-id {
    auto-discovery;
    direction down;
    interface interface-name;
    remote-mep mep-id {
      action-profile profile-name;
    }
  }
}

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Configure the name of the maintenance association in IEEE-compliant format.

Options
ma-name—The name of the maintenance association within the maintenance domain.

The remaining statements are explained separately.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide
maintenance-domain (EX Series Switch Only)

Syntax

```
maintenance-domain domain-name {
  level number;
  mip-half-function (none | default | explicit);
  name-format (character-string | none | dns | mac+2oct);
  maintenance-association ma-name {
    continuity-check {
      hold-interval minutes;
      interface-status-tlv;
      interval (10m | 10s | 1m | 1s | 100ms);
      loss-threshold number;
      port-status-tlv;
    }
    mep mep-id {
      auto-discovery;
      direction down;
      interface interface-name;
      remote-mep mep-id {
        action-profile profile-name;
      }
    }
  }
}
```

Hierarchy Level

```
[edit protocols oam ethernet connectivity-fault-management ]
```

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Configure the name of the maintenance domain in IEEE-compliant format.

Options
```
domain-name—The name for the maintenance domain.
```

The remaining statements are explained separately.

Required Privilege
```
 routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.
```

Related Documentation
```
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide
```
measurement-type (OAM LFM)

Syntax
measurement-type two-way-delay;

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management performance-monitoring sla-iterator-profiles profile-name]

Release Information
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description
Configure the measurement type for the service-level agreement (SLA) frames. An SLA frame is a type of packet used to measure frame loss in Ethernet connections.

Options
two-way-delay—Use Y.1731-compliant two-way ETH-DM frames to measure frame loss.

Required Privilege
Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation
• Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) on page 3619
• Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620
• Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3623
mep (EX Series Switch Only)

Syntax

mep mep-id {
  auto-discovery;
  direction down;
  interface interface-name;
  remote-mep mep-id {
    action-profile profile-name;
  }
}

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance-association ma-name]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Configure the numeric identifier of the maintenance association end point (MEP) within the maintenance association.

Options
mep-id—Numeric identifier of the MEP.
Range: 1 through 8191

The remaining statements are explained separately.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
• Junos OS Network Interfaces Configuration Guide
mip-half-function (EX Series Switch Only)

Syntax
mip-half-function (none | default | explicit);

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name]

Release Information
Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description
Specify the OAM Ethernet CFM maintenance domain MIP half functions.

NOTE: Whenever a MIP is configured, the MIP half function value for all maintenance domains and maintenance associations must be the same.

Options
- none—Specify to not use the mip-half-function.
- default—Specify to use the default mip-half-function.
- explicit—Specify an explicit mip-half-function.

Required Privilege
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide
name-format (EX Series Switch Only)

Syntax

```plaintext
name-format (character-string | none | dns | mac+2oct);
```

Hierarchy Level

```plaintext
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name]
```

Release Information

Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description

Specify the format of the maintenance domain name.

Options

- **character-string**—The name is an ASCII character string.
- **none**—Name format none means that maintenance domain name is not used.
- **dns**—Name is in domain name service (DNS) format. For example: www.juniper.net.
- **mac+2oct**—Name is the MAC address plus a two-octet maintenance association identifier. For example: 08:00:22:33:44:55.100.

Default: character-string

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide

path-database-size (EX Series Switch Only)

Syntax

```plaintext
path-database-size path-database-size;
```

Hierarchy Level

```plaintext
[edit protocols oam ethernet connectivity-fault-management linktrace]
```

Release Information

Statement introduced in Junos OS Release 10.2 for EX Series switches.

Description

Specify the number of linktrace reply entries to be stored per linktrace request.

Options

- **path-database-size**—Database size (number of entries stored per request).
  - **Range:** 1 through 500
  - **Default:** 100

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- Junos OS Network Interfaces Configuration Guide
performance-monitoring (OAM LFM)

Syntax

```
performance-monitoring {
  sla-iterator-profiles {
    profile-name {
      calculation-weight {
        delay delay-value;
        delay-variation delay-variation-value;
      }
      cycle-time cycle-time-value;
      iteration-period iteration-period-value;
      measurement-type two-way-delay;
      passive;
    }
  }
}
```

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management]

Release Information
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description
Specify performance monitoring support for Ethernet frame delay measurement.

The remaining statements are explained separately.

Required Privilege
Level
Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation
• Configuring MEP Interfaces on Switches to Support Ethernet Frame Delay Measurements (CLI Procedure) on page 3619
• Configuring One-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3620
• Configuring Two-Way Ethernet Frame Delay Measurements on Switches (CLI Procedure) on page 3623
remote-mep (EX Series Switch Only)

**Syntax**

```
remote-mep mep-id {
  action-profile profile-name;
}
```

**Hierarchy Level**

```
[edit protocols oam ethernet connectivity-fault-management maintenance-domain
domain-name maintenance-association ma-name mep mep-id]
```

**Release Information**

Statement introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Specify the numeric identifier of the remote maintenance association end point (MEP) within the maintenance association.

**Options**

- **mep-id**—Specify the numeric identifier of the MEP.
  - Range: 1 through 8191

The remaining statement is explained separately.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
- *Junos OS Network Interfaces Configuration Guide*
sla-iterator-profiles (OAM LFM)

Syntax

sla-iterator-profiles {
    profile-name {
        calculation-weight {
            delay delay-value;
            delay-variation delay-variation-value;
        }
        cycle-time cycle-time-value;
        iteration-period iteration-period-value;
        measurement-type two-way-delay;
        passive;
    }
}

Hierarchy Level
[edit protocols oam ethernet connectivity-fault-management performance-monitoring]

Release Information
Statement introduced in Junos OS Release 11.4 for EX Series switches.

Description
Configure an iterator application and specify the iterator profile options.

Options

profile-name—Name of the iterator profile.

The remaining statements are explained separately.

Required Privilege

Configure—To enter configuration mode.
Control—To modify any configuration.

Related Documentation

- Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621
Configuration Statements: Ethernet OAM Link Fault Management

action (OAM LFM)

Syntax

action {
syslog;
link-down;
}

Hierarchy Level
[edit protocols oam ethernet link-fault-management]

Release Information
Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description
Define the action or actions to be taken when the OAM link fault management (LFM) fault event occurs.

The remaining statements are explained separately.

Required Privilege
Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
### action-profile

**Syntax**

```
action-profile profile-name;
action {
  syslog;
  link-down;
}
event {
  link-adjacency-loss;
  link-event-rate {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
  }
}
```

**Hierarchy Level**

`[edit protocols oam ethernet link-fault-management]`

**Release Information**

Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

Configure an Ethernet OAM link fault management (LFM) action profile by specifying a profile name.

The remaining statements are explained separately.

**Options**

- `profile-name`—Name of the action profile.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
allow-remote-loopback

**Syntax**
allow-remote-loopback;

**Hierarchy Level**
[edit protocols oam ethernet link-fault-management interface interface-name]

**Release Information**
Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**
Advertise that the interface is capable of getting into loopback mode. Enable remote loopback in Ethernet OAM link fault management (LFM) on all Ethernet interfaces or the specified interface on the EX Series switch.

**Required Privilege Level**
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
ethernet (OAM LFM)

Syntax

```
ethernet {
  connectivity-fault-management {
    action-profile profile-name {
      action {
        interface-down;
      }
      default-actions {
        interface-down;
      }
      event {
        adjacency-loss;
      }
    }
    esp-traceoptions {
      file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
      flag (all | error | esp | interface | krt | lib | normal | task | timer);
    }
    linktrace {
      age (30m | 10m | 1m | 30s | 10s);
      path-database-size path-database-size;
    }
    maintenance-domain domain-name {
      level number;
      mip-half-function (none | default | explicit);
      name-format (character-string | none | dns | mac+2oct);
      maintenance-association ma-name {
        continuity-check {
          hold-interval minutes;
          interface-status-tlv;
          interval (10m | 10s | 1m | 1s | 100ms);
          loss-threshold number;
          port-status-tlv;
        }
        mep mep-id {
          auto-discovery;
          direction down;
          interface interface-name;
          priority
          remote-mep mep-id {
            action-profile profile-name;
            sla-iterator-profile profile-name {
              data-tlv-size size;
              iteration-count count-value;
              priority priority-value;
            }
          }
        }
      }
      short-name-format (character-string | vlan | 2octet | rfc-2685-vpn-id);
    }
    performance-monitoring {
  }
}
```
sla-iterator-profiles {
    profile-name {
        calculation-weight {
            delay delay-value;
            delay-variation delay-variation-value;
        }
        cycle-time cycle-time-value;
        iteration-period iteration-period-value;
        measurement-type two-way-delay;
        passive;
    }
}

traceoptions {
    file filename <files number> <match regex> <size> <world-readable> |
    no-world-readable>;
    flag flag ;
    no-remote-trace;
}

link-fault-management {
    action-profile profile-name;
    action {
        syslog;
        link-down;
    }
    event {
        link-adjacency-loss;
        link-event-rate {
            frame-error count;
            frame-period count;
            frame-period-summary count;
            symbol-period count;
        }
    }
    interface interface-name {
        link-discovery (active | passive);
        pdu-interval interval;
        pdu-threshold threshold-value;
        remote-loopback;
        event-thresholds {
            frame-error count;
            frame-period count;
            frame-period-summary count;
            symbol-period count;
        }
        negotiation-options {
            allow-remote-loopback;
            no-allow-link-events;
        }
    }
}

traceoptions {
    file filename <files number> <match regex> <size> <world-readable> |
    no-world-readable>;
    flag flag ;
    no-remote-trace;
Hierarchy Level [edit protocols oam]


Description Provide IEEE 802.3ah Operation, Administration, and Maintenance (OAM) support for Ethernet interfaces on EX Series switches or configure connectivity fault management (CFM) for IEEE 802.1ag Operation, Administration, and Management (OAM) support on the switches.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation • Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591

• Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 3587

• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

• Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612
event (OAM LFM)

Syntax

event {
  link-adjacency-loss;
  link-event-rate {
    frame-error count;
    frame-period count;
    frame-period-summary count;
    symbol-period count;
  }
}

Hierarchy Level [edit protocols oam ethernet link-fault-management action-profile profile-name]

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description Configure link events in an action profile for Ethernet OAM link fault management (LFM).

The remaining statements are explained separately.

Required Privilege Level routinglevel—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

event-thresholds

Syntax

event-thresholds {
  frame-error count;
  frame-period count;
  frame-period-summary count;
  symbol-period count;
}

Hierarchy Level [edit protocols oam ethernet link-fault-management interface interface-name]

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description Configure threshold limit values for link events in periodic OAM PDUs.

The remaining statements are explained separately.

Required Privilege Level routinglevel—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation • Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
### frame-error

**Syntax**

```
frame-error count;
```

**Hierarchy Level**

```
[edit protocols oam ethernet link-fault-management event link-event-rate],
[edit protocols oam ethernet link-fault-management interface interface-name event-thresholds]
```

**Release Information**

Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

Configure the threshold value for sending frame error events or taking the action specified in the action profile.

Frame errors occur on the underlying physical layer. The threshold is reached when the number of frame errors reaches the configured value.

**Options**

- `count`—Threshold count in seconds for frame error events.
  - **Range**: 1 through 100 seconds
  - **Default**: 1 second

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

### frame-period

**Syntax**

```
frame-period count;
```

**Hierarchy Level**

```
[edit protocols oam ethernet link-fault-management event link-event-rate],
[edit protocols oam ethernet link-fault-management interface interface-name event-thresholds]
```

**Release Information**

Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

Configure the number of frame errors within the last N frames that has exceeded a threshold.

Frame errors occur on the underlying physical layer. The threshold is reached when the number of frame errors reaches the configured value.

**Options**

- `count`—Threshold count in seconds for frame error events.
  - **Range**: 1 through 100 seconds

**Required Privilege Level**

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
frame-period-summary

Syntax

frame-period-summary count;

Hierarchy Level

[edit protocols oam ethernet link-fault-management event link-event-rate],
[edit protocols oam ethernet link-fault-management interface interface-name
event-thresholds]

Release Information

Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description

Configure the threshold value for sending frame period summary error events or taking
the action specified in the action profile.

An errored frame second is any 1-second period that has at least one errored frame. This
event is generated if the number of errored frame seconds is equal to or greater than the
specified threshold for that period.

Options

count—Threshold count in seconds for frame period summary error events.

Range: 1 through 100 seconds

Required Privilege

Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation

• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
interface (OAM LFM)

Syntax

interface interface-name {  
  link-discovery (active | passive);  
  pdu-interval interval;  
  pdu-threshold threshold-value;  
  remote-loopback;  
  event-thresholds {  
    frame-error count;  
    frame-period count;  
    frame-period-summary count;  
    symbol-period count;  
  }  
  negotiation-options {  
    allow-remote-loopback;  
    no-allow-link-events;  
  }  
}

Hierarchy Level
[edit protocols oam ethernet link-fault-management]

Release Information
Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description
Configure Ethernet OAM link fault management (LFM) for all interfaces or for specific interfaces.

The remaining statements are explained separately.

Options
interface-name—Name of the interface to be enabled for IEEE 802.3ah OAM link fault management (LFM) support.

Required Privilege Level
routing—To view this statement in the configuration.
route-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
link-adjacency-loss

**Syntax**  
link-adjacency-loss;

**Hierarchy Level**  
[edit protocols oam ethernet link-fault-management action-profile event]

**Release Information**  
Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**  
Configure loss of adjacency event with the IEEE 802.3ah link fault management (LFM) peer. When included, the loss of adjacency event triggers the action specified under the action statement.

**Required Privilege Level**  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**  
- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591  
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

link-discovery

**Syntax**  
link-discovery (active | passive);

**Hierarchy Level**  
[edit protocols oam ethernet link-fault-management interface interface-name]

**Release Information**  
Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**  
Specify the discovery mode used for IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support. The discovery process is triggered automatically when OAM 802.3ah functionality is enabled on an interface. Link monitoring is done when the interface sends periodic OAM PDUs.

**Options**  
- **active**—In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality.
- **passive**—In passive mode, the peer initiates the discovery process.

Once the discovery process is initiated, both sides participate in discovery.

**Required Privilege Level**  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**  
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
link-down

Syntax

```
link-down;
```

Hierarchy Level

[edit protocols oam ethernet link-fault-management action-profile action]

Release Information

Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description

Mark the interface as down for transit traffic.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

link-event-rate

Syntax

```
link-event-rate {
  frame-error count;
  frame-period count;
  frame-period-summary count;
  symbol-period count;
}
```

Hierarchy Level

[edit protocols oam ethernet link-fault-management action-profile event]

Release Information

Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description

Configure the number of link fault management (LFM) events per second.

The remaining statements are explained separately.

Required Privilege

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
**link-fault-management**

**Syntax**

```plaintext
link-fault-management {
  action-profile profile-name;
  action {
    syslog;
    link-down;
  }
  event {
    link-adjacency-loss;
    link-event-rate {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
  }
  interface interface-name {
    link-discovery (active | passive);
    pdq-interval interval;
    pdq-threshold threshold-value;
    remote-loopback;
    event-thresholds {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
    negotiation-options {
      allow-remote-loopback;
      no-allow-link-events;
    }
  }
}
```

**Hierarchy Level**

[edit protocols oam ethernet]

**Release Information**

Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

Configure Ethernet OAM link fault management (LFM) for all interfaces or for specific interfaces.

The remaining statements are explained separately.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
**negotiation-options**

Syntax

```plaintext
negotiation-options {
  allow-remote-loopback;
  no-allow-link-events;
}
```

Hierarchy Level

```
[edit protocols oam ethernet link-fault-management interface interface-name]
```

Release Information

Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description

Enable and disable IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) features for Ethernet interfaces.

The remaining statements are explained separately.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

**no-allow-link-events**

Syntax

```plaintext
no-allow-link-events;
```

Hierarchy Level

```
[edit protocols oam ethernet link-fault-management interface interface-name negotiation-options]
```

Release Information

Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description

Disable the sending of link event TLVs.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
Syntax

```plaintext
oam {
  ethernet {
    connectivity-fault-management {
      action-profile profile-name {
        action {
          interface-down;
        }
        default-actions {
          interface-down;
        }
        event {
          adjacency-loss;
        }
      }
    }
    linktrace {
      age (30m | 10m | 1m | 30s | 10s);
      path-database-size path-database-size;
    }
    maintenance-domain domain-name {
      level number;
      mip-half-function (none | default | explicit);
      name-format (character-string | none | dns | mac+2oct);
      maintenance-association ma-name {
        continuity-check {
          hold-interval minutes;
          interface-status-tlv;
          interval (10m | 10s | 1m | 1s | 100ms);
          loss-threshold number;
          port-status-tlv;
        }
        mep mep-id {
          auto-discovery;
          direction down;
          interface interface-name;
          remote-mep mep-id {
            action-profile profile-name;
          }
        }
      }
    }
    performance-monitoring {
      sla-iterator-profiles {
        profile-name {
          calculation-weight {
            delay delay-value;
            delay-variation delay-variation-value;
          }
          cycle-time cycle-time-value;
          iteration-period iteration-period-value;
          measurement-type two-way-delay;
          passive;
        }
      }
    }
  }
}
```
link-fault-management {
  action-profile profile-name;
  action {
    syslog;
    link-down;
  }
  event {
    link-adjacency-loss;
    link-event-rate {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
  }
  interface interface-name {
    link-discovery (active | passive);
    pdu-interval interval;
    pdu-threshold threshold-value;
    remote-loopback;
    event-thresholds {
      frame-error count;
      frame-period count;
      frame-period-summary count;
      symbol-period count;
    }
    negotiation-options {
      allow-remote-loopback;
      no-allow-link-events;
    }
  }
}

Hierarchy Level [edit protocols]


Description Provide IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support for Ethernet interfaces on EX Series switches or configure connectivity fault management (CFM) for IEEE 802.1ag Operation, Administration, and Management (OAM) support on the switches.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation

- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Example: Configuring Ethernet OAM Connectivity Fault Management on EX Series Switches on page 3587
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
- Configuring Ethernet OAM Connectivity Fault Management (CLI Procedure) on page 3612

**pdu-interval**

**Syntax**

```
pdu-interval interval;
```

**Hierarchy Level**

```
[edit protocols oam ethernet link-fault-management interface interface-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

Specify the periodic OAM PDU sending interval for fault detection. It is used for IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support.

**Options**

- `interval`—Periodic OAM PDU sending interval.
  - **Range:** 400 through 1000 milliseconds
  - **Default:** 1000 milliseconds

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
### pdu-threshold

<table>
<thead>
<tr>
<th>Syntax</th>
<th>pdu-threshold threshold-value;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit protocols oam ethernet link-fault-management interface interface-name]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 9.4 for EX Series switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Configure how many protocol data units (PDUs) are missed before declaring the peer lost in Ethernet OAM link fault management (LFM) for all interfaces or for specific interfaces.</td>
</tr>
<tr>
<td>Options</td>
<td><strong>threshold-value</strong> — Number of PDUs missed before declaring the peer lost.</td>
</tr>
<tr>
<td></td>
<td>Range: 3 through 10 PDUs</td>
</tr>
<tr>
<td></td>
<td>Default: 3 PDUs</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>routing—To view this statement in the configuration.</td>
</tr>
<tr>
<td></td>
<td>routing-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

### remote-loopback

<table>
<thead>
<tr>
<th>Syntax</th>
<th>remote-loopback;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit protocols oam ethernet link-fault-management interface interface-name]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 9.4 for EX Series switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Set the data terminal equipment (DTE) in loopback mode. Remove the statement from the configuration to take the DTE out of loopback mode. It is used for IEEE 802.3ah Operation, Administration, and Maintenance (OAM) link fault management (LFM) support.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>routing—To view this statement in the configuration.</td>
</tr>
<tr>
<td></td>
<td>routing-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>

### Related Documentation

- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
symbol-period

Syntax
symbol-period count;

Hierarchy Level
[edit protocols oam ethernet link-fault-management action-profile profile-name; event link-event-rate],
[edit protocols oam ethernet link-fault-management interface interface-name event-thresholds]

Release Information
Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description
Configure the threshold for sending symbol period events or taking the action specified in the action profile.

Symbol code errors occur on the underlying physical layer. The symbol period threshold is reached when the number of symbol errors reaches the configured value within the period. You cannot configure the default value to a different value.

Options
count—Threshold count in seconds for symbol period events.
Range: 1 through 100 seconds

Required Privilege
level routing—To view this statement in the configuration.
level routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

syslog (OAM LFM)

Syntax
syslog;

Hierarchy Level
[edit protocols oam ethernet link-fault-management action-profile profile-name; action]

Release Information
Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description
Generate a system log message for the Ethernet Operation, Administration, and Maintenance (OAM) link fault management (LFM) event.

Required Privilege
level routing—To view this statement in the configuration.
level routing-control—To add this statement to the configuration.

Related Documentation
• Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616
# Configuration Statements: RPM

## data-fill

<table>
<thead>
<tr>
<th>Syntax</th>
<th>data-fill data;</th>
</tr>
</thead>
</table>

### Hierarchy Level

[edit services rpm bgp],
[edit services rpm probe owner test test-name]

### Release Information

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.3 for EX Series switches.
- Statement introduced in Junos OS Release 93. for PTX Series Packet Transport Routers.

### Description

Specify the contents of the data portion of Internet Control Message Protocol (ICMP) probes. The `data-fill` statement is not valid with the `http-get` or `http-metadata-get` probe types.

### Options

- **data**—A hexadecimal value; for example, 0-9, A-F.

### Required Privilege Level

- system—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

### Related Documentation

- Configuring BGP Neighbor Discovery Through RPM
- Configuring RPM Probes
data-size

Syntax: data-size size;

Hierarchy Level: [edit services rpm bgp],
[edit services rpm probe owner test test-name]

Release Information: Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description: Specify the size of the data portion of ICMP probes. The data-size statement is not valid with the http-get or http-metadata-get probe type.

Options: data—The size can be from 0 through 65507
Default: 0

NOTE: If you configure the hardware timestamp feature (see Configuring RPM Timestamping), the data-size default value is 32 bytes and 32 is the minimum value for explicit configuration. The UDP timestamp probe type is an exception; it requires a minimum data size of 52 bytes.

Required Privilege Level: system—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation: • Configuring BGP Neighbor Discovery Through RPM
destination-port

Syntax
destination-port port;

Hierarchy Level
[edit services rpm bgp],
[edit services rpm probe owner test test-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description
Specify the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port
to which a probe is sent. This statement is used only for TCP or UDP probe types.

The value for the destination-port can be only 7 when you configure along with hardware
timestamping. A constraint check prevents you for configuring any other value for the
destination port in this case.

This constraint does not apply when you are using one-way hardware timestamping
along with destination-port and either probe-type udp-ping or probe-type
udp-ping-timestamp.

Options
port—The port number can be 7 or from 49,160 to 65,535.

Required Privilege
Level
system—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring BGP Neighbor Discovery Through RPM
• Configuring RPM Probes
### dscp-code-point

**Syntax**
```
dscp-code-point dscp-bits;
```

**Hierarchy Level**
```
[edit services rpm probe owner test test-name]
```

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.3 for EX Series switches.
- Statement introduced in Junos OS Release for PTX Series Packet Transport Routers.

**Description**
Specify the value of the Differentiated Services (DiffServ) field within the IP header. The DiffServ code point (DSCP) bits value must be set to a valid 6-bit pattern.

**Options**
- **dscp-bits**—A valid 6-bit pattern; for example, **001111** or one of the following configured DSCP aliases:
  - **af1**—Default: 001010
  - **af2**—Default: 001100
  - **af3**—Default: 001110
  - **af21**—Default: 010010
  - **af22**—Default: 010100
  - **af23**—Default: 010110
  - **af31**—Default: 011010
  - **af32**—Default: 011100
  - **af33**—Default: 011110
  - **af41**—Default: 100010
  - **af42**—Default: 100100
  - **af43**—Default: 100110
  - **be**—Default: 000000
  - **cs1**—Default: 001000
  - **cs2**—Default: 010000
  - **cs3**—Default: 011000
  - **cs4**—Default: 100000
  - **cs5**—Default: 101000
  - **cs6**—Default: 110000
  - **cs7**—Default: 111000
  - **ef**—Default: 101110
  - **nc1**—Default: 110000
• nc2—Default: 111000

Required Privilege
Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring RPM Probes

hardware-timestamp

Syntax
hardware-timestamp;

Hierarchy Level
[edit services rpm probe owner test test-name]

Release Information
Statement introduced in Junos OS Release 8.1.
Statement applied to MX Series routers in Junos OS Release 10.0.
Statement introduced in Junos OS Release 10.3 for EX Series switches.

Description
On MX Series routers and EX Series switches only, enable timestamping of RPM probe messages in the Packet Forwarding Engine host processor. This feature is supported only with icmp-ping, icmp-ping-timestamp, udp-ping, and udp-ping-timestamp probe types.

When you configure either probe-type udp-ping or probe-type udp-ping-timestamp along with the hardware-timestamp command, the value for the destination-port can be only 7. A constraint check prevents you for configuring any other value for the destination port in this case.

This constraint does not apply when you are configuring one-way-hardware-timestamp.

Required Privilege
Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring RPM Timestamping
**history-size**

**Syntax**

```
history-size size;
```

**Hierarchy Level**

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.3 for EX Series switches.
- Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description**

Specify the number of stored history entries.

**Options**

- **size**—A value from 0 to 255.
- **Default:** 50

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring BGP Neighbor Discovery Through RPM
- Configuring RPM Probes

---

**moving-average-size**

**Syntax**

```
moving-average-size number;
```

**Hierarchy Level**

```
[edit services rpm bgp],
[edit services rpm probe owner test test-name]
```

**Release Information**

- Statement introduced in Junos OS Release 8.5.
- Statement introduced in Junos OS Release 9.3 for EX Series switches.
- Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description**

Enable statistical calculation operations to be performed across a configurable number of the most recent samples.

**Options**

- **number**—Number of samples to be used in calculations.
- **Range:** 0 through 255

**Required Privilege Level**

- **interface**—To view this statement in the configuration.
- **interface-control**—To add this statement to the configuration.

**Related Documentation**

- Configuring RPM Probes
one-way-hardware-timestamp

Syntax
one-way-hardware-timestamp;

Hierarchy Level
[edit services rpm probe owner test test-name]

Release Information
Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description
Enable timestamping of RPM probe messages for one-way delay and jitter measurements.
You must configure this statement along with the destination-interface statement to invoke timestamping. This feature is supported only with icmp-ping, icmp-ping-timestamp, udp-ping, and udp-ping-timestamp probe types.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation
- Configuring RPM Timestamping
- destination-interface
- hardware-timestamp on page 3762

port (RPM)

Syntax
port number;

Hierarchy Level
[edit services rpm probe-server (tcp | udp)]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description
Specify the port number for the probe server.

Options
number—Port number for the probe server. The value can be 7 or 49,160 through 65,535.

Required Privilege Level
interface—to view this statement in the configuration.
interface-control—to add this statement to the configuration.

Related Documentation
- Configuring RPM Receiver Servers
probe

Syntax

```plaintext
probe owner {
    test test-name {
        data-fill data;
        data-size size;
        destination-interface interface-name;
        destination-port port;
        dscp-code-point dscp-bits;
        hardware-timestamp;
        history-size size;
        moving-average-size number;
        one-way-hardware-timestamp;
        probe-count count;
        probe-interval seconds;
        probe-type type;
        routing-instance instance-name;
        source-address address;
        target (url | address);
        test-interval interval;
        thresholds thresholds;
        traps traps;
    }
}
```

Hierarchy Level  [edit services rpm]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description  Specify an owner name. The owner name combined with the test name represent a single RPM configuration instance.

Options

- **owner**—Specify an owner name up to 32 characters in length.

The remaining statements are explained separately.

Required Privilege

- **Level**
  - system—To view this statement in the configuration.
  - interface-control—To add this statement to the configuration.

Related Documentation

- Configuring RPM Probes
probe-count

Syntax probe-count count;

Hierarchy Level [edit services rpm bgp],
[edit services rpm probe owner test test-name]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description Specify the number of probes within a test.

Options count—A value from 1 through 15.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation • Configuring BGP Neighbor Discovery Through RPM
• Configuring RPM Probes

probe-interval

Syntax probe-interval interval;

Hierarchy Level [edit services rpm bgp],
[edit services rpm probe owner test test-name]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description Specify the time to wait between sending packets, in seconds.

Options interval—Number of seconds, from 1 through 255.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation • Configuring BGP Neighbor Discovery Through RPM
• Configuring RPM Probes
# probe-limit

**Syntax**

```
probe-limit limit;
```

**Hierarchy Level**

```
[edit services rpm]
```

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.3 for EX Series switches.
- Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description**

Configure the maximum number of concurrent probes allowed.

**Options**

- `limit` — Maximum number of concurrent probes allowed.
  - **Range:** 1 through 500 (PTX Series Packet Transport Routers only) 1 through 200
  - **Default:** 100

**Required Privilege Level**

- `interface` — To view this statement in the configuration.
- `interface-control` — To add this statement to the configuration.

**Related Documentation**

- [Limiting the Number of Concurrent RPM Probes](#)
probe-server

Syntax

```
probe-server {
  tcp {
    destination-interface interface-name;
    port number;
  }
  udp {
    destination-interface interface-name;
    port number;
  }
}
```

Hierarchy Level
[edit services rpm]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description
Specify the server to act as a receiver for the probes.

The remaining statements are explained separately.

NOTE: The destination-interface statement is not supported on PTX Series routers.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring RPM Receiver Servers
probe-type

Syntax  
proble-type type;

Hierarchy Level  
[edit services rpm bgp],  
[edit services rpm probe owner test test-name]

Release Information  
Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.3 for EX Series switches.  
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description  
Specify the packet and protocol contents of a probe.

Options  
type—Specify one of the following probe type values:

- http-get—(Not available at the [edit services rpm bgp] hierarchy level.) Sends a Hypertext Transfer Protocol (HTTP) get request to a target URL.
- http-metadata-get—(Not available at the [edit services rpm bgp] hierarchy level.) Sends an HTTP get request for metadata to a target URL.
- icmp-ping—Sends ICMP echo requests to a target address.
- icmp-ping-timestamp—Sends ICMP timestamp requests to a target address.
- tcp-ping—Sends TCP packets to a target.
- udp-ping—Sends UDP packets to a target.
- udp-ping-timestamp—Sends UDP timestamp requests to a target address.

Required Privilege Level  
interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  
- Configuring BGP Neighbor Discovery Through RPM
**routing-instance**

**Syntax**
```
routing-instance instance-name;
```

**Hierarchy Level**
[edit services rpm probe owner test test-name]

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description**
Specify the routing instance used by the probes.

**Options**
- `instance-name`—A routing instance configured at the `[edit routing-instance]` hierarchy level.
  
  **Default:** Internet routing table inet.0.

**Required Privilege**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring RPM Probes

**routing-instances**

**Syntax**
```
routing-instances instance-name;
```

**Hierarchy Level**
[edit services rpm bgp],
[edit services rpm bgp logical-system logical-system-name]

**Release Information**
Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description**
Specify the routing instance used by the probes.

**Options**
- `instance-name`—A routing instance configured at the `[edit routing-instances]` hierarchy level.
  
  **Default:** Internet routing table inet.0.

**Required Privilege**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring BGP Neighbor Discovery Through RPM
rpm

Syntax  rpm (client | server);

Hierarchy Level  [edit interfaces interface-name unit logical-unit-number]

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description  Associate an RPM client (router or switch that originates RPM probes) or RPM server
with a specified interface.

Options  
  client—Identifier for RPM client router or switch.
  server—Identifier for RPM server.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  • Configuring RPM Timestamping

source-address

Syntax  source-address address;

Hierarchy Level  [edit services rpm probe owner test test-name]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description  Specify the source IP address used for probes. If the source IP address is not one of the
router’s or switch’s assigned addresses, the packet will use the outgoing interface’s
address as its source.

Options  address—Valid IP address.

Required Privilege Level  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  • Configuring RPM Probes
**tcp**

**Syntax**
```
tcp {
    destination-interface interface-name;
    port port;
}
```

**Hierarchy Level**
[edit services rpm probe-server]

**Release Information**
- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.3 for EX Series switches.
- Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

**Description**
Specify the port information for the TCP server.

The remaining statements are explained separately.

**Required Privilege**
- `interface`—To view this statement in the configuration.
- `interface-control`—To add this statement to the configuration.

**Related Documentation**
- Configuring RPM Receiver Servers
test

Syntax  test test-name {
    data-fill data;
    data-size size;
    destination-interface interface-name;
    destination-port port;
    dscp-code-point dscp-bits;
    hardware-timestamp;
    history-size size;
    moving-average-size number;
    one-way-hardware-timestamp;
    probe-count count;
    probe-interval seconds;
    probe-type type;
    routing-instance instance-name;
    source-address address;
    target (url | address address);
    test-interval interval;
    thresholds thresholds;
    traps traps;
}

Hierarchy Level  [edit services rpm probe owner]

Release Information  Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description  Specify the range of probes over which the standard deviation, average, and jitter are calculated. The test name combined with the owner name represent a single RPM configuration instance.

Options  test-name—Specify a test name. The name can be up to 32 characters in length.

The remaining statements are explained separately.

Required Privilege  interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation  • Configuring RPM Probes
**test-interval**

Syntax  

test-interval *frequency*;

Hierarchy Level  

[edit services rpm bgp],  
[edit services rpm probe owner test test-name]

Release Information  

Statement introduced before Junos OS Release 7.4.  
Statement introduced in Junos OS Release 9.3 for EX Series switches.  
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description  

Specify the time to wait between tests, in seconds.

Options  

*frequency*—Number of seconds, from 0 through 86400.

Required Privilege Level  

interface—To view this statement in the configuration.  
interface-control—To add this statement to the configuration.

Related Documentation  

• [Configuring BGP Neighbor Discovery Through RPM](#)  
• [Configuring RPM Probes](#)
thresholds

Syntax

thresholds thresholds;

Hierarchy Level

[edit services rpm probe owner test test-name]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Packet Series Transport Routers.

Description

Specify thresholds used for the probes. A system log message is generated when the configured threshold is exceeded. Likewise, an SNMP trap (if configured) is generated when a threshold is exceeded.

Options

thresholds—Specify one or more threshold measurements. The following options are supported:

- **egress-time**—Measures maximum source-to-destination time per probe.
- **ingress-time**—Measures maximum destination-to-source time per probe.
- **jitter-egress**—Measures maximum source-to-destination jitter per test.
- **jitter-ingress**—Measures maximum destination-to-source jitter per test.
- **jitter-rtt**—Measures maximum jitter per test, from 0 through 60,000,000 microseconds.
- **rtt**—Measures maximum round-trip time per probe, in microseconds.
- **std-dev-egress**—Measures maximum source-to-destination standard deviation per test.
- **std-dev-ingress**—Measures maximum destination-to-source standard deviation per test.
- **std-dev-rtt**—Measures maximum standard deviation per test, in microseconds.
- **successive-loss**—Measures successive probe loss count, indicating probe failure.
- **total-loss**—Measures total probe loss count indicating test failure, from 0 through 15.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring RPM Probes
traps

Syntax 
traps traps;

Hierarchy Level 
[edit services rpm probe owner test test-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description
Set the trap bit to generate traps for probes. Traps are sent if the configured threshold is met or exceeded.

Options
traps—Specify one or more traps. The following options are supported:

- egress-jitter-exceeded—Generates traps when the jitter in egress time threshold is met or exceeded.
- egress-std-dev-exceeded—Generates traps when the egress time standard deviation threshold is met or exceeded.
- egress-time-exceeded—Generates traps when the maximum egress time threshold is met or exceeded.
- ingress-jitter-exceeded—Generates traps when the jitter in ingress time threshold is met or exceeded.
- ingress-std-dev-exceeded—Generates traps when the ingress time standard deviation threshold is met or exceeded.
- ingress-time-exceeded—Generates traps when the maximum ingress time threshold is met or exceeded.
- jitter-exceeded—Generates traps when the jitter in round-trip time threshold is met or exceeded.
- probe-failure—Generates traps for successive probe loss thresholds crossed.
- rtt-exceeded—Generates traps when the maximum round-trip time threshold is met or exceeded.
- std-dev-exceeded—Generates traps when the round-trip time standard deviation threshold is met or exceeded.
- test-completion—Generates traps when a test is completed.
- test-failure—Generates traps when the total probe loss threshold is met or exceeded.

NOTE: For RPM traps to be generated, you must configure the remote-operations SNMP trap category by including the categories statement at the [edit snmp trap-group trap-group-name hierarchy level.]
Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring RPM Probes
• categories on page 3635

udp

Syntax
udp {
    destination-interface interface-name;
    port port;
}

Hierarchy Level [edit services rpm probe-server]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description
Specify the port information for the UDP server.

The remaining statements are explained separately.

NOTE: The destination-interface statement is not supported on PTX Series routers.

Required Privilege Level
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
• Configuring RPM Receiver Servers
Configuration Statements: Uplink Failure Detection

action (Uplink Failure Detection)

Syntax

```
action {
    log;
}
```

Hierarchy Level  [edit protocols uplink-failure-detection]

Release Information  Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description  Define an action on uplink-failure-detection group state change.

Options  log—Generate a system log message.

Required Privilege Level  admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Related Documentation  • Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618

group (Uplink Failure Detection)

Syntax

```
 group group-name {
    link-to-monitor interface-name;
    link-to-disable interface-name;
}
```

Hierarchy Level  [edit protocols uplink-failure-detection]

Release Information  Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description  Configure a group of uplink and downlink interfaces for uplink failure detection.

Options  group-name—Name of the uplink-failure-detection group.

The remaining statements are explained separately.

Required Privilege Level  admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Related Documentation  • Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618
link-to-disable

Syntax  link-to-disable interface-name;

Hierarchy Level  [edit protocols uplink-failure-detection group group-name]

Release Information  Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description  Configure the downlink interfaces to be disabled when the switch detects an uplink failure. The switch can monitor a maximum of 48 downlink interfaces in a group.

Options  interface-name—Name of the downlink interface or interface range in the group. The interface can be a physical interface or a logical interface.

Required Privilege Level  admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Related Documentation  • Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618

link-to-monitor

Syntax  link-to-monitor interface-name;

Hierarchy Level  [edit protocols uplink-failure-detection group group-name]

Release Information  Statement introduced in Junos OS Release 11.1 for EX Series switches.

Description  Configure the uplink interfaces to be monitored for uplink failure detection. The switch can monitor a maximum of 48 uplink interfaces in a group.

An interface can be configured as link-to-monitor in multiple groups.

Options  interface-name—Name of the uplink interface or interface range in the group. The interface can be a physical interface or a logical interface.

Required Privilege Level  admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Related Documentation  • Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618
traceoptions (Uplink Failure Detection)

Syntax

```
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
  flag flag;
}
```

Hierarchy Level

[edit protocols uplink-failure-detection]

Release Information

Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Define tracing operations for uplink failure detection.

Default

The traceoptions feature is disabled by default.

Options

- **file filename** — Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks.
- **files number** — (Optional) Maximum number of trace files. When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached ( `xk` to specify KB, `xm` to specify MB, or `xg` to specify gigabytes), at which point the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.
  
  **Range:** 2 through 1000
  
  **Default:** 3 files

- **flag flag** — Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:
  
  - `all` — Trace everything.
  - `dcd` — Trace ufdd interaction with dcd.
  - `groups` — Trace uplink-failure-detection group handling.
  - `interface` — Trace interface notification handlers of ufdd.
  - `parse` — Trace configuration parsing.
  
  **no-stamp** — (Optional) Do not place a timestamp on any trace file.

  **no-world-readable** — (Optional) Restricted file access to the user who created the file.

  **size size** — (Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the `files` option.

  **Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify gigabytes
Range: 10 KB through 1 GB
Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

**Required Privilege Level**
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618

```plaintext
uplink-failure-detection
```

**Syntax**
```
uplink-failure-detection {
    action {
        log;
    }
    group group-name {
        link-to-monitor interface-name;
        link-to-disable interface-name;
    }
    traceoptions {
        file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
        flag flag);
    }
}
```

**Hierarchy Level**
[edit protocols]

**Release Information**
Statement introduced in Junos OS Release 11.1 for EX Series switches.

**Description**
Configure uplink and downlink interfaces in a group to monitor uplink failures and to propagate uplink failures to the downlink interfaces.

The remaining statements are explained separately.

**Required Privilege Level**
admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618
CHAPTER 68

Administration

- Routine Monitoring on page 3783
- Operational Commands: General on page 3789
- Operational Commands: RPM on page 3812
- Operational Commands: SNMP on page 3822
- Operational Commands: Analyzers and Port Mirroring on page 3858
- Operational Commands: sFlow on page 3862
- Operational Commands: Ethernet OAM Connectivity Fault Management on page 3868
- Operational Commands: Ethernet OAM Link Fault Management on page 3906
- Operational Commands: Uplink Failure Detection on page 3911

Routine Monitoring

- Monitoring Hosts Using the J-Web Ping Host Tool on page 3783
- Monitoring Network Traffic Using Traceroute on page 3785
- Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches on page 3786
- Viewing Real-Time Performance Monitoring Information on page 3787
- Verifying That Uplink Failure Detection Is Working Correctly on page 3788

Monitoring Hosts Using the J-Web Ping Host Tool

**Purpose**
Use the J-Web ping host tool to verify that the host can be reached over the network. The output is useful for diagnosing host and network connectivity problems. The switch sends a series of ICMP echo (ping) requests to a specified host and receives ICMP echo responses.

**Action**
To use the J-Web ping host tool:

1. Select **Troubleshoot>Ping Host**.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Ping Host page, as described in Table 438 on page 3784.
   The Remote Host field is the only required field.
4. Click **Start**.
The results of the ping operation are displayed in the main pane. If no options are specified, each ping response is in the following format:

```
bytes bytes from ip-address: icmp_seq=number ttl=number time=time
```

5. To stop the ping operation before it is complete, click **OK**.

**Meaning**

Table 438 on page 3784 lists the fields.

### Table 438: J-Web Ping Host Field Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Host</td>
<td>Identifies the host to ping.</td>
<td>Type the hostname or IP address of the host to ping.</td>
</tr>
<tr>
<td>Advanced Options</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Don't Resolve Addresses | Determines whether to display hostnames of the hops along the path. | • To suppress the display of the hop hostnames, select the check box.  
• To display the hop hostnames, clear the check box. |
| Interface            | Specifies the interface on which the ping requests are sent. | Select the interface on which ping requests are sent from the list. If you select any, the ping requests are sent on all interfaces. |
| Count                | Specifies the number of ping requests to send.     | Select the number of ping requests to send from the list. |
| Don't Fragment       | Specifies the Don't Fragment (DF) bit in the IP header of the ping request packet. | • To set the DF bit, select the check box.  
• To clear the DF bit, clear the check box. |
| Record Route         | Sets the record route option in the IP header of the ping request packet. The path of the ping request packet is recorded within the packet and displayed in the main pane. | • To record and display the path of the packet, select the check box.  
• To suppress the recording and display of the path of the packet, clear the check box. |
| Type-of-Service      | Specifies the type-of-service (TOS) value in the IP header of the ping request packet. | Select the decimal value of the TOS field from the list. |
| Routing Instance     | Name of the routing instance for the ping attempt. | Select the routing instance name from the list. |
| Interval             | Specifies the interval, in seconds, between transmissions of individual ping requests. | Select the interval from the list. |
| Packet Size          | Specifies the size of the ping request packet. | Type the size, in bytes, of the packet. The size can be from 0 through 65468. The switch adds 8 bytes of ICMP header to the size. |
| Source Address       | Specifies the source address of the ping request packet. | Type the source IP address. |
| Time-to-Live         | Specifies the time-to-live (TTL) hop count for the ping request packet. | Select the TTL value from the list. |
Table 438: J-Web Ping Host Field Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass Routing</td>
<td>Determines whether ping requests are routed by means of the routing table.</td>
<td>• To bypass the routing table and send the ping requests to hosts on the specified interface only, select the check box.</td>
</tr>
<tr>
<td></td>
<td>If the routing table is not used, ping requests are sent only to hosts on the interface specified in the Interface box. If the host is not on that interface, ping responses are not sent.</td>
<td>• To route the ping requests using the routing table, clear the check box.</td>
</tr>
</tbody>
</table>

Related Documentation

- Monitoring Interface Status and Traffic on page 2463

Monitoring Network Traffic Using Traceroute

**Purpose**

Use the Traceroute page in the J-Web interface to trace a route between the switch and a remote host. You can use a traceroute task to display a list of waypoints between the switch and a specified destination host. The output is useful for diagnosing a point of failure in the path from the switch platform to the destination host and addressing network traffic latency and throughput problems.

**Action**

To use the traceroute tool:

1. Select Troubleshoot > Traceroute.
2. Next to Advanced options, click the expand icon.
3. Enter information into the Traceroute page.
   - The Remote Host field is the only required field.
4. Click Start.
5. To stop the traceroute operation before it is complete, click OK while the results of the traceroute operation are being displayed.

**Meaning**

The switch generates the list of waypoints by sending a series of ICMP traceroute packets in which the time-to-live (TTL) value in the messages sent to each successive waypoint is incremented by 1. (The TTL value of the first traceroute packet is set to 1.) In this manner, each waypoint along the path to the destination host replies with a Time Exceeded packet from which the source IP address can be obtained.

The results of the traceroute operation are displayed in the main pane. If no options are specified, each line of the traceroute display is in the following format:

```
hop-number host (ip-address) [as-number] time1 time2 time3
```

The switch sends a total of three traceroute packets to each waypoint along the path and displays the round-trip time for each traceroute operation. If the switch times out before receiving a Time Exceeded message, an asterisk (*) is displayed for that round-trip time.
Table 439: Traceroute field summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Host</td>
<td>Identifies the destination host of the traceroute.</td>
<td>Type the hostname or IP address of the destination host.</td>
</tr>
<tr>
<td></td>
<td><strong>Advanced Options</strong></td>
<td></td>
</tr>
<tr>
<td>Don't Resolve</td>
<td>Determines whether hostnames of the hops along the path are displayed,</td>
<td>To suppress the display of the hop hostnames, select the check box.</td>
</tr>
<tr>
<td>Addresses</td>
<td>in addition to IP addresses.</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>Specifies the IP address of the gateway to route through.</td>
<td>Type the gateway IP address.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Specifies the source address of the outgoing traceroute packets.</td>
<td>Type the source IP address.</td>
</tr>
<tr>
<td>Bypass Routing</td>
<td>Determines whether traceroute packets are routed by means of the routing</td>
<td>To bypass the routing table and send the traceroute packets to hosts on the</td>
</tr>
<tr>
<td></td>
<td>table. If the routing table is not used, traceroute packets are sent only</td>
<td>specified interface only, select the check box.</td>
</tr>
<tr>
<td></td>
<td>to hosts on the interface specified in the Interface box. If the host is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not on that interface, traceroute responses are not sent.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interface on which the traceroute packets are sent.</td>
<td>From the list, select the interface on which traceroute packets are sent.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select any, the traceroute requests are sent on all interfaces.</td>
</tr>
<tr>
<td>Time-to-live</td>
<td>Specifies the maximum time-to-live (TTL) hop count for the traceroute</td>
<td>From the list, select the TTL.</td>
</tr>
<tr>
<td></td>
<td>request packet.</td>
<td></td>
</tr>
<tr>
<td>Type-of-Service</td>
<td>Specifies the type-of-service (TOS) value to include in the IP header of</td>
<td>From the list, select the decimal value of the TOS field.</td>
</tr>
<tr>
<td></td>
<td>the traceroute request packet.</td>
<td></td>
</tr>
<tr>
<td>Resolve AS Numbers</td>
<td>Determines whether the autonomous system (AS) number of each intermediate</td>
<td>To display the AS numbers, select the check box.</td>
</tr>
<tr>
<td></td>
<td>hop between the router and the destination host is displayed.</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- [Connecting and Configuring an EX Series Switch (CLI Procedure)](Connecting and Configuring an EX Series Switch (CLI Procedure))
- [Connecting and Configuring an EX Series Switch (J-Web Procedure)](Connecting and Configuring an EX Series Switch (J-Web Procedure))
- [Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289](Configuring Gigabit Ethernet Interfaces (J-Web Procedure) on page 2289)
- [Monitoring Interface Status and Traffic on page 2463](Monitoring Interface Status and Traffic on page 2463)

**Verifying Input and Output for Port Mirroring Analyzers on EX Series Switches**

**Purpose**
Verify that an analyzer has been created on the switch and has the appropriate output interfaces, and appropriate output interface.
Action

You can verify the port mirror analyzer is configured as expected using the `show analyzer` command.

```
[edit]
user@switch> show analyzer
Analyzer name                  : employee-monitor
Output VLAN                  : remote-analyzer
Mirror ratio                 : 1
Loss priority                : High
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
```

You can view all of the port mirror analyzers configured on the switch, including any that are disabled, using the `show ethernet-switching-options` command in configuration mode.

```
user@switch# show ethernet-switching-options
inactive: analyzer employee-web-monitor {
    loss-priority high;
    output {
        analyzer employee-monitor {
            loss-priority high;
            input {
                ingress {
                    interface ge-0/0/0.0;
                    interface ge-0/0/1.0;
                }
            }
            output {
                vlan {
                    remote-analyzer;
                }
            }
        }
    }
}
```

Meaning

This output shows that the employee-monitor analyzer has a ratio of 1 (mirroring every packet, the default), a loss priority of high (set this option to high whenever the analyzer output is to a VLAN), is mirroring the traffic entering `ge-0/0/0` and `ge-0/0/1`, and sending the mirrored traffic to the analyzer called remote-analyzer.

Related Documentation

- Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 3601
- Configuring Port Mirroring to Analyze Traffic (CLI Procedure)
- Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches
- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches
- Understanding Port Mirroring on EX Series Switches

Viewing Real-Time Performance Monitoring Information

Real-time performance monitoring (RPM) on EX Series switches enables you to configure and send probes to a specified target and monitor the analyzed results to determine...
packet loss, round-trip time, and jitter. The J-Web interface provides a graphical view of RPM information for EX Series switches.

To view the RPM information using the J-Web interface:

1. Select Troubleshoot > RPM > View RPM.
2. Select the Round Trip Time check box to display the graph with round-trip time included. Clear the check-box to view the graph without the round-trip time.
3. From the Refresh Time list, select a refresh time interval for the graph.

Verifying That Uplink Failure Detection Is Working Correctly

Purpose Verify that the switch disables the downlink interface when it detects an uplink failure.

Action 1. View the current uplink-failure-detection status:

```
user@switch> show uplink-failure-detection
Group : group1
Uplink : ge-0/0/0*
Downlink : ge-0/0/1*
Failure Action : Inactive
```

**NOTE:** The asterisk (*) indicates that the link is up.

2. Disable the uplink interface:

```
[edit]
user@switch# set interface ge-0/0/0 disable
```
3. Save the configuration on the switch.
4. View the current uplink-failure-detection status:

```
user@switch> show uplink-failure-detection
Group : group1
Uplink : ge-0/0/0
Downlink : ge-0/0/1
Failure Action : Active
```

Meaning The output in Step 1 shows that the uplink interface is up, and hence that the downlink interface is also up, and that the status of Failure Action is Inactive.

The output in Step 4 shows that both the uplink and downlink interfaces are down and that the status of Failure Action is changed to Active. This output shows that uplink failure detection is working.

Related Documentation

- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618
- Understanding Uplink Failure Detection on page 3556
Operational Commands: General
# monitor traffic

## Syntax

```plaintext
monitor traffic
  <brief | detail | extensive>
  <absolute-sequence>
  <count count>
  <interface interface-name>
  <layer2-headers>
  <matching matching>
  <no-domain-names>
  <no-promiscuous>
  <no-resolve>
  <no-timestamp>
  <print-ascii>
  <print-hex>
  <resolve-timeout>
  <size size>
```

## Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

## Description

Display packet headers or packets received and sent from the Routing Engine.

### NOTE:

- Using the `monitor-traffic` command can degrade router or switch performance.
- Delays from DNS resolution can be eliminated by using the `no-resolve` option.

### NOTE: This command is not supported on the QFabric system.

## Options

- **none**—(Optional) Display packet headers transmitted through `fp0`. On a TX Matrix Plus router, display packet headers transmitted through `em0`.
- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **absolute-sequence**—(Optional) Display absolute TCP sequence numbers.
- **count count**—(Optional) Specify the number of packet headers to display (0 through 1,000,000). The monitor traffic command quits automatically after displaying the number of packets specified.
interface interface-name—(Optional) Specify the interface on which the monitor traffic command displays packet data. If no interface is specified, the monitor traffic command displays packet data arriving on the lowest-numbered interface.

layer2-headers—(Optional) Display the link-level header on each line.

matching matching—(Optional) Display packet headers that match a regular expression. Use matching expressions to define the level of detail with which the monitor traffic command filters and displays packet data.

no-domain-names—(Optional) Suppress the display of the domain portion of hostnames. With the no-domain-names option enabled, the monitor traffic command displays only team for the hostname team.company.net.

no-promiscuous—(Optional) Do not put the interface into promiscuous mode.

no-resolve—(Optional) Suppress reverse lookup of the IP addresses.

no-timestamp—(Optional) Suppress timestamps on displayed packets.

print-ascii—(Optional) Display each packet in ASCII format.

print-hex—(Optional) Display each packet, except the link-level header, in hexadecimal format.

resolve-timeout timeout—(Optional) Amount of time the router or switch waits for each reverse lookup before timing out. You can set the timeout for 1 through 4,294,967,295 seconds. The default is 4 seconds. To display each packet, use the print-ascii, print-hex, or extensive option.

size size—(Optional) Read but do not display up to the specified number of bytes for each packet. When set to brief output, the default packet size is 96 bytes and is adequate for capturing IP, ICMP, UDP, and TCP packet data. When set to detail and extensive output, the default packet size is 1514. The monitor traffic command truncates displayed packets if the matched data exceeds the configured size.

Additional Information

In the monitor traffic command, you can specify an expression to match by using the matching option and including the expression in quotation marks:

```
monitor traffic matching "expression"
```

Replace expression with one or more of the match conditions listed in Table 440 on page 3792.
## Table 440: Match Conditions for the monitor traffic Command

<table>
<thead>
<tr>
<th>Match Type</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Entity**    | `host [address | hostname]` | Matches packets that contain the specified address or hostname.  
|               |                         | The protocol match conditions `arp`, `ip`, or `rarp`, or any of the directional match conditions can be prepended to the `host` match condition. |
|               | `net address`           | Matches packets with source or destination addresses containing the specified network address. |
|               | `net address mask mask` | Matches packets containing the specified network address and subnet mask. |
|               | `port (port-number | port-name)`           | Matches packets containing the specified source or destination TCP or UDP port number or port name.  
|               |                         | In place of the numeric port address, you can specify a text synonym, such as `bgp` (179), `dhcp` (67), or `domain` (53) (the port numbers are also listed). |
| **Directional** | `dst`                   | Matches packets going to the specified destination. This match condition can be prepended to any of the entity type match conditions. |
|               | `src`                   | Matches packets from a specified source. This match condition can be prepended to any of the entity type match conditions. |
|               | `src and dst`           | Matches packets that contain the specified source and destination addresses. This match condition can be prepended to any of the entity type match conditions. |
|               | `src or dst`            | Matches packets containing either of the specified addresses. This match condition can be prepended to any of the entity type match conditions. |
| **Packet Length** | `less value`           | Matches packets shorter than or equal to the specified value, in bytes. |
|               | `greater value`         | Matches packets longer than or equal to the specified value, in bytes. |
Table 440: Match Conditions for the monitor traffic Command  *(continued)*

<table>
<thead>
<tr>
<th>Match Type</th>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>amt</td>
<td>Matches all AMT packets. Use the extensive level of output to decode the inner IGMP packets in addition to the AMT outer packet.</td>
</tr>
<tr>
<td></td>
<td>arp</td>
<td>Matches all ARP packets.</td>
</tr>
<tr>
<td></td>
<td>ether</td>
<td>Matches all Ethernet packets.</td>
</tr>
<tr>
<td></td>
<td>ether (broadcast</td>
<td>Matches broadcast or multicast Ethernet frames. This match condition can be prepended with <code>src</code> and <code>dst</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>multic)</td>
</tr>
<tr>
<td></td>
<td>ether protocol</td>
<td>Matches packets with the specified Ethernet address or Ethernet packets of the specified protocol type. The <code>ether protocol</code> arguments <code>arp</code>, <code>ip</code>, and <code>rarp</code> are also independent match conditions, so they must be preceded by a backslash (<code>\</code>) when used in the <code>ether protocol</code> match condition.</td>
</tr>
<tr>
<td></td>
<td>(address</td>
<td>Matches packets with the specified address or protocol type. The <code>ip protocol</code> arguments <code>icmp</code>, <code>tcp</code>, and <code>udp</code> are also independent match conditions, so they must be preceded by a backslash (<code>\</code>) when used in the <code>ip protocol</code> match condition.</td>
</tr>
<tr>
<td></td>
<td>(icmp</td>
<td>Matches all IS-IS routing messages.</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
<td>Matches all TCP datagrams.</td>
</tr>
<tr>
<td></td>
<td>udp</td>
<td>Matches all UDP datagrams.</td>
</tr>
</tbody>
</table>

To combine expressions, use the logical operators listed in Table 441 on page 3793.

Table 441: Logical Operators for the monitor traffic Command

<table>
<thead>
<tr>
<th>Logical Operator (Highest to Lowest Precedence)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>!</code></td>
<td>Logical NOT. If the first condition does not match, the next condition is evaluated.</td>
</tr>
</tbody>
</table>
Table 441: Logical Operators for the monitor traffic Command (continued)

<table>
<thead>
<tr>
<th>Logical Operator (Highest to Lowest Precedence)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;&amp;</td>
<td>Logical AND. If the first condition matches, the next condition is evaluated. If the first condition does not match, the next condition is skipped.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>()</td>
<td>Group operators to override default precedence order. Parentheses are special characters, each of which must be preceded by a backslash ().</td>
</tr>
</tbody>
</table>

You can use relational operators to compare arithmetic expressions composed of integer constants, binary operators, a length operator, and special packet data accessors. The arithmetic expression matching condition uses the following syntax:

```
monitor traffic matching "ether[0] & 1 != 0" "arithmetic_expression relational_operator arithmetic_expression"
```

The packet data accessor uses the following syntax:

```
protocol [byte-offset <size>]
```

The optional size field represents the number of bytes examined in the packet header. The available values are 1, 2, or 4 bytes. The following sample command captures all multicast traffic:

```
user@host> monitor traffic matching "ether[0] & 1 != 0"
```

To specify match conditions that have a numeric value, use the arithmetic and relational operators listed in Table 442 on page 3795.

**NOTE:** Because the Packet Forwarding Engine removes Layer 2 header information before sending packets to the Routing Engine:

- The monitor traffic command cannot apply match conditions to inbound traffic.
- The monitor traffic interface command also cannot apply match conditions for Layer 3 and Layer 4 packet data, resulting in the match pipe option (|) for this command for Layer 3 and Layer 4 packets not working either. Therefore, ensure that you specify match conditions as described in this command summary. For more information about match conditions, see Table 440 on page 3792.
- The 802.1Q VLAN tag information included in the Layer 2 header is removed from all inbound traffic packets. Because the monitor traffic interface ae[x] command for aggregated Ethernet interfaces (such as ae0) only shows inbound traffic data, the command does not show VLAN tag information in the output.
Table 442: Arithmetic and Relational Operators for the monitor traffic Command

<table>
<thead>
<tr>
<th>Arithmetic or Relational Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arithmetic Operator</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Addition operator.</td>
</tr>
<tr>
<td>-</td>
<td>Subtraction operator.</td>
</tr>
<tr>
<td>/</td>
<td>Division operator.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Bitwise AND.</td>
</tr>
<tr>
<td>*</td>
<td>Bitwise exclusive OR.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Relational Operator (Highest to Lowest Precedence)</td>
<td></td>
</tr>
<tr>
<td>&lt;=</td>
<td>If the first expression is less than or equal to the second, the packet matches.</td>
</tr>
<tr>
<td>&gt;=</td>
<td>If the first expression is greater than or equal to the second, the packet matches.</td>
</tr>
<tr>
<td>&lt;</td>
<td>If the first expression is less than the second, the packet matches.</td>
</tr>
<tr>
<td>&gt;</td>
<td>If the first expression is greater than the second, the packet matches.</td>
</tr>
<tr>
<td>=</td>
<td>If the compared expressions are equal, the packet matches.</td>
</tr>
<tr>
<td>!=</td>
<td>If the compared expressions are unequal, the packet matches.</td>
</tr>
</tbody>
</table>

Required Privilege Level
- trace
- maintenance

List of Sample Output
- monitor traffic count on page 3796
- monitor traffic detail count on page 3796
- monitor traffic extensive (Absolute Sequence) on page 3796
- monitor traffic extensive (Relative Sequence) on page 3796
- monitor traffic extensive count on page 3796
- monitor traffic interface on page 3797
- monitor traffic matching on page 3797
- monitor traffic (TX Matrix Plus Router) on page 3797
- monitor traffic (QFX3500 Switch) on page 3798

Output Fields
When you enter this command, you are provided feedback on the status of your request.
Sample Output

monitor traffic count

```
user@host>  monitor traffic count 2
listening on fxp0
04:35:49.814125  In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529478 win 16798 (DF)
04:35:49.814185
Out my-server.work.net.telnet > my-server.home.net.1295: P
1:38(37) ack 0 win 17680 (DF) [tos 0x10]
```

monitor traffic detail count

```
user@host>  monitor traffic detail count 2
listening on fxp0
04:38:16.265864  In my-server.home.net.1295 > my-server.work.net.telnet: . ack
4122529971 win 17678 (DF) (ttl 121, id 6812)
04:38:16.265926
Out my-server.work.net.telnet > my-server.home.net.1295: P 1:38(37) ack 0
win 17680 (DF) [tos 0x10]  (ttl 6)
```

monitor traffic extensive (Absolute Sequence)

```
user@host>  monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp" absolute-sequence
listening on fxp0
In 207.17.136.193.179 > 192.168.4.227.1024: . 4042780859:4042780859(0)
ack 1845421797 win 16384 <nop,nop,timestamp 4935628 965951>: BGP (|BGP UPDAT)
In 207.168.4.227.1024 > 207.17.136.193.179: P 1845421797:1845421852(55) ack 4042780912 win 16384 <nop,nop,timestamp 965951 4935628>: BGP (|BGP UPDAT)
...
```

monitor traffic extensive (Relative Sequence)

```
user@host>  monitor traffic extensive no-domain-names no-resolve no-timestamp count 20
matching "tcp"
listening on fxp0
In 172.24.248.221.1680 > 192.168.4.210.23: . 396159737:396159737(0)
ack 1664980689 win 17574 (DF) (ttl 121, id 50003)
ack 0 win 17680 (DF) [tos 0x10]  (ttl 64, id 5394)
In 207.17.136.193.179 > 192.168.4.227.1024: P 4042775817:4042775874(57)
ack 18454216593 win 16384 <nop,nop,timestamp 965951 4935379>: BGP (|BGP UPDAT)
...
```

monitor traffic extensive count

```
user@host>  monitor traffic extensive count 5 no-domain-names no-resolve
listening on fxp0:13:18:17.406933
In 172.17.28.8.2049 > 192.168.4.206.2723610880:
```
In 0:e0:1e:42:9c:e0 0:e0:1e:42:9c:e0 9000 60:
0000 0100 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
0000 0000 0000 0000
ack 295526518 win 17601 (DF)
(ttl 121, id 14)

Out 192.168.4.210.23 >
172.24.248.156.4139: P 1:40(39)
ack 0 win 17680 (DF) [tos 0x10]
(ttl 64, id 52376)

monitor traffic interface

user@host> monitor traffic interface fxp0
listening on fxp0.0
18:17:28.800650  In server.home.net.723 > host1-0.lab.home.net.log
18:17:28.800733 Out host2-0.lab.home.net.login > server.home.net.7
18:17:28.817813  In host30.lab.home.net.syslog > host40.home0
18:17:28.817846  In host30.lab.home.net.syslog > host40.home0
...

monitor traffic matching

user@host> monitor traffic matching "net 192.168.1.0/24"
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on fxp0, capture size 96 bytes
Reverse lookup for 192.168.1.255 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use no-resolve to avoid reverse lookups on IP addresses.

21:55:54.003511  In IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003585 Out IP truncated-ip - 18 bytes missing!
192.168.1.17.netbios-ns > 192.168.1.255.netbios-ns: UDP, length 50
21:55:54.003864  In arp who-has 192.168.1.17 tell 192.168.1.9
21:55:54.003889  In IP truncated-ip - 18 bytes missing!
...

monitor traffic (TX Matrix Plus Router)

user@host> monitor traffic
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on em0, capture size 96 bytes
04:11:59.862303 Out IP truncated-ip - 25 bytes missing!
summit-em0.englab.juniper.net.syslog > sv-log-01.englab.juniper.net.syslog:
SYSLOG kernel.info, length: 57
04:11:59.862303 Out IP truncated-ip - 25 bytes missing!
summit-em0.englab.juniper.net.syslog >
sv-log-02.englab.juniper.net.syslog: SYSLOG kernel.info, length: 57
04:11:59.923948 In IP aj-em0.englab.juniper.net.65235 >
monitor traffic (QFX3500 Switch)

user@switch> monitor traffic
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on me4, capture size 96 bytes
Reverse lookup for 172.22.16.246 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use <no-resolve> to avoid reverse lookups on IP addresses.
16:35:32.240873 Out IP truncated-ip - 112 bytes missing!
labqfx-me0.lab4.juniper.net.ssh >
172.22.16.246.telefinder: P 4200727624:4200727756(132) ack 2889954831 win 65535
16:35:32.240900 Out IP truncated-ip - 176 bytes missing!
labqfx-me0.lab4.juniper.net.ssh >
172.22.16.246.telefinder: P 132:328(196) ack 1 win 65535
...
ping

Syntax

```plaintext
ping host
  <bypass-routing>
  <count requests>
  <detail>
  <do-not-fragment>
  <inet | inet6>
  <interface source-interface>
  <interval seconds>
  <logical-system logical-system-name>
  <loose-source value>
  <mac-address mac-address>
  <no-resolve>
  <pattern string>
  <rapid>
  <record-route>
  <routing-instance routing-instance-name>
  <size bytes>
  <source source-address>
  <strict>
  <strict-source value>
  <tos type-of-service>
  <ttl value>
  <verbose>
  <vpls instance-name>
  <wait seconds>
```

Syntax (QFX Series)

```plaintext
ping host
  <bypass-routing>
  <count requests>
  <detail>
  <do-not-fragment>
  <inet>
  <interface source-interface>
  <interval seconds>
  <logical-system logical-system-name>
  <loose-source value>
  <mac-address mac-address>
  <no-resolve>
  <pattern string>
  <rapid>
  <record-route>
  <routing-instance routing-instance-name>
  <size bytes>
  <source source-address>
  <strict>
  <strict-source value>
  <tos type-of-service>
  <ttl value>
  <verbose>
  <wait seconds>
```

**Release Information**

Command introduced before Junos OS Release 7.4.

**Description**
Check host reachability and network connectivity. The **ping** command sends Internet Control Message Protocol (ICMP) ECHO_REQUEST messages to elicit ICMP ECHO_RESPONSE messages from the specified host. Press Ctrl+c to interrupt a ping command.

**Options**

- **host**—IP address or hostname of the remote system to ping.

- **bypass-routing**—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

- **count requests**—(Optional) Number of ping requests to send. The range of values is 1 through 2,000,000,000. The default value is an unlimited number of requests.

- **detail**—(Optional) Include in the output the interface on which the ping reply was received.

- **do-not-fragment**—(Optional) Set the do-not-fragment (DF) flag in the IP header of the ping packets. For IPv6 packets, this option disables fragmentation.

**NOTE:** In Junos OS Release 11.1 and later, when issuing the **ping** command for an IPv6 route with the **do-not-fragment** option, the maximum ping packet size is calculated by subtracting 48 bytes (40 bytes for the IPv6 header and 8 bytes for the ICMP header) from the MTU. Therefore, if the ping packet size (including the 48-byte header) is greater than the MTU, the ping operation might fail.

- **inet**—(Optional) Ping Packet Forwarding Engine IPv4 routes.

- **inet6**—(Optional) Ping Packet Forwarding Engine IPv6 routes.

- **interface source-interface**—(Optional) Interface to use to send the ping requests.

- **interval seconds**—(Optional) How often to send ping requests. The range of values, in seconds, is 1 through infinity. The default value is 1.

- **logical-system logical-system-name**—(Optional) Name of logical system from which to send the ping requests. Alternatively, enter the **set cli logical-system logical-system-name** command and then run the **ping** command. To return to the main router or switch, enter the **clear cli logical-system** command.

- **loose-source value**—(Optional) Intermediate loose source route entry (IPv4). Open a set of values.
mac-address mac-address—(Optional) Ping the physical or hardware address of the remote system you are trying to reach.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

pattern string—(Optional) Specify a hexadecimal fill pattern to include in the ping packet.

rapid—(Optional) Send ping requests rapidly. The results are reported in a single message, not in individual messages for each ping request. By default, five ping requests are sent before the results are reported. To change the number of requests, include the count option.

record-route—(Optional) Record and report the packet’s path (IPv4).

routing-instance routing-instance-name—(Optional) Name of the routing instance for the ping attempt.

size bytes—(Optional) Size of ping request packets. The range of values, in bytes, is 0 through 65,468. The default value is 56, which is effectively 64 bytes because 8 bytes of ICMP header data are added to the packet.

source source-address—(Optional) IP address of the outgoing interface. This address is sent in the IP source address field of the ping request. If this option is not specified, the default address is usually the loopback interface (lo.0).

strict—(Optional) Use the strict source route option (IPv4).

strict-source value—(Optional) Intermediate strict source route entry (IPv4). Open a set of values.

tos type-of-service—(Optional) Set the type-of-service (ToS) field in the IP header of the ping packets. The range of values is 0 through 255. If the device configuration includes the dscp-code-point value statement at the [edit class-of-service host-outbound-traffic] hierarchy level, the configured DSCP value overrides the value specified in this command option. In this case, the ToS field of ICMP echo request packets sent on behalf of this command carries the DSCP value specified in the dscp-code-point configuration statement instead of the value you specify in this command option.

ttl value—(Optional) Time-to-live (TTL) value to include in the ping request (IPv6). The range of values is 0 through 255.

verbose—(Optional) Display detailed output.

vpls instance-name—(Optional) Ping the instance to which this VPLS belongs.

wait seconds—(Optional) Maximum wait time, in seconds, after the final packet is sent. If this option is not specified, the default delay is 10 seconds. If this option is used without the count option, a default count of 5 packets is used.
**Required Privilege**

- network

**Level**

**Related Documentation**

- Configuring the Junos OS ICMPv4 Rate Limit for ICMPv4 Routing Engine Messages

**List of Sample Output**

- ping hostname on page 3803
- ping hostname rapid on page 3803
- ping hostname size count on page 3803

**Output Fields**

When you enter this command, you are provided feedback on the status of your request. An exclamation point (!) indicates that an echo reply was received. A period (.) indicates that an echo reply was not received within the timeout period. An x indicates that an echo reply was received with an error code. These packets are not counted in the received packets count. They are accounted for separately.

**Sample Output**

**ping hostname**

user@host> ping skye
PING skye.net (192.168.169.254): 56 data bytes
64 bytes from 192.168.169.254: icmp_seq=0 ttl=253 time=1.028 ms
64 bytes from 192.168.169.254: icmp_seq=1 ttl=253 time=1.053 ms
64 bytes from 192.168.169.254: icmp_seq=2 ttl=253 time=1.025 ms
64 bytes from 192.168.169.254: icmp_seq=3 ttl=253 time=1.098 ms
64 bytes from 192.168.169.254: icmp_seq=4 ttl=253 time=1.032 ms
64 bytes from 192.168.169.254: icmp_seq=5 ttl=253 time=1.044 ms
^C [abort]

**ping hostname rapid**

user@host> ping skye rapid
PING skye.net (192.168.169.254): 56 data bytes
!!!!!
--- skye.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.956/0.974/1.025/0.026 ms

**ping hostname size count**

user@host> ping skye size 200 count 5
PING skye.net (192.168.169.254): 200 data bytes
208 bytes from 192.168.169.254: icmp_seq=0 ttl=253 time=1.759 ms
208 bytes from 192.168.169.254: icmp_seq=1 ttl=253 time=2.075 ms
208 bytes from 192.168.169.254: icmp_seq=2 ttl=253 time=1.843 ms
208 bytes from 192.168.169.254: icmp_seq=3 ttl=253 time=1.803 ms
208 bytes from 192.168.169.254: icmp_seq=4 ttl=253 time=17.898 ms
--- skye.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.759/5.075/17.898 ms
**show pfe statistics bridge**

**Syntax**
```
show pfe statistics bridge
<fpc slot>
```

**Release Information**
Command introduced in Junos OS Release 12.1 for EX Series switches.

**Description**
Display information about the number of packets discarded in the ingress pipeline of the Packet Forwarding Engine, packets discarded because of egress filtering or congestion filtering, number of control packets, and general counters for dropped packets. You can use this information to inform troubleshooting investigations.

**Options**
- **none**—Display bridge counter statistics for all Flexible PIC Concentrator (FPC) slots.
- **fpc slot**—(Optional) Display bridge counter statistics for a specific FPC slot.

**Required Privilege Level**
view

**Related Documentation**
- Monitoring System Process Information on page 718
- Monitoring Switch Control Traffic on page 712

**List of Sample Output**
- show pfe statistics bridge (EX3200 and EX4200 Switches) on page 3805
- show pfe statistics bridge (EX8200 Switches and EX8200 Virtual Chassis) on page 3806
- show pfe statistics bridge fpc (EX8200 Switches and EX8200 Virtual Chassis) on page 3807
- show pfe statistics bridge fpc (EX8200-40XS (40-port SFP+) Line Card) on page 3807

**Output Fields**
Table 443 on page 3804 lists the output fields for the `show pfe statistics bridge` command. Output fields are listed in the approximate order in which they appear.

### Table 443: show pfe statistics bridge Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Counters</td>
<td>Information about ingress counters:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Received</strong>—Number of packets received by the bridge.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VLAN Filtered</strong>—Number of packets discarded because of VLAN filtering.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Security Filtered</strong>—Number of packets discarded because of security filtering.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Other Discards</strong>—Number of packets dropped by the bridge for reasons other than VLAN or security filtering.</td>
</tr>
</tbody>
</table>
### Table 443: show pfe statistics bridge Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Egress Counters</strong></td>
<td>Information about egress counters:</td>
</tr>
<tr>
<td>Unicast</td>
<td>Number of unicast packets transmitted.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Number of multicast packets transmitted.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>Number of broadcast packets transmitted.</td>
</tr>
<tr>
<td>Egress Filtered</td>
<td>Number of egress-filtered packets (regardless of port, priority, or mode).</td>
</tr>
<tr>
<td>TailDrop</td>
<td>Number of packets filtered because of egress queue congestion.</td>
</tr>
<tr>
<td>Forward Restrict</td>
<td>Number of packets filtered because of egress forward restrictions.</td>
</tr>
<tr>
<td>Congestion Filtered</td>
<td>Number of packets filtered because of transmit queue (TxQ) congestion.</td>
</tr>
<tr>
<td>Control Packets</td>
<td>Number of control packets (sent to CPU, received from CPU, and sent to analyzer).</td>
</tr>
<tr>
<td><strong>Drop Counters</strong></td>
<td>Information about drop counters:</td>
</tr>
<tr>
<td>Drop Mode</td>
<td>Count mode of the counter.</td>
</tr>
<tr>
<td>Drop Counter</td>
<td>Counter value.</td>
</tr>
<tr>
<td><strong>General Counters</strong></td>
<td>Information about general counters:</td>
</tr>
<tr>
<td>Drop Mode</td>
<td>Count mode of the counter.</td>
</tr>
<tr>
<td>Drop Counter</td>
<td>Counter value.</td>
</tr>
<tr>
<td>Source Not Learnt</td>
<td>Number of source addresses that were not learnt because of internal congestion.</td>
</tr>
<tr>
<td><strong>MUX PFE</strong></td>
<td>Information about multiplexer PFE for oversubscribed cards:</td>
</tr>
<tr>
<td>Drop Mode</td>
<td>Count mode of the counter.</td>
</tr>
<tr>
<td>Drop Count</td>
<td>Counter value.</td>
</tr>
</tbody>
</table>

### Sample Output

**show pfe statistics bridge (EX3200 and EX4200 Switches)**

```
user@switch> show pfe statistics bridge
Slot 0
PFE:                        0           1           2
-------------------------------------------------------------------------
---- Ingress Counters ----
  Received:                       0          52           0
  VLAN Filtered:                  0           0           0
  Security Filtered:              0           0           0
  Other Discards:                 0           0           0
---- Egress Counters ----
  Unicast:                        0         104          52
  Multicast:                      0           0           0
  Broadcast:                      0           0           0
  Egress Filtered:                0           0           0
  Congestion Filtered:            0           0           0
  Control Packets:                5           0           0
---- General Counters ----
  Drop Mode:                  0           0           0
```
show pfe statistics bridge (EX8200 Switches and EX8200 Virtual Chassis)

user@switch> show pfe statistics bridge
Slot 0
PFE: 0 1

---- Ingress Counters ----
Received: 946 48
VLAN Filtered: 0 0
Security Filtered: 0 0
Other Discards: 0 0

---- Egress Counters ----
Unicast: 0 0
Multicast: 0 0
Broadcast: 0 0
Egress Filtered: 0 0
TailDrop: 0 0
Forward Restrict: 0 0
Congestion Filtered: 0 0
Control Packets: 4103 896

---- Drop Counters ----
Drop Mode: 0 0
Drop Counter: 12528 2

Slot 1
PFE: 0 1

---- Ingress Counters ----
Received: 0 0
VLAN Filtered: 0 0
Security Filtered: 0 0
Other Discards: 0 0

---- Egress Counters ----
Unicast: 0 0
Multicast: 0 0
Broadcast: 0 0
Egress Filtered: 0 0
TailDrop: 0 0
Forward Restrict: 0 0
Congestion Filtered: 0 0
Control Packets: 0 0

---- Drop Counters ----
Drop Mode: 0 0
Drop Counter: 0 0

Slot 2
PFE: 0 1

---- Ingress Counters ----
Received: 0 0
VLAN Filtered: 0 0
Security Filtered: 0 0
Other Discards: 0 0

---- Egress Counters ----
Unicast: 0 0
Multicast: 0 0
Broadcast: 0 0
Egress Filtered: 0 0
TailDrop: 0 0
Forward Restrict: 0 0
Congestion Filtered: 0 0
Control Packets: 0 0
---- Drop Counters ----
Drop Mode: 0 0
Drop Counter: 0 0

show pfe statistics bridge fpc (EX8200 Switches and EX8200 Virtual Chassis)

user@switch> show pfe statistics bridge fpc 2
Slot 2
PFE: 0 1

---- Ingress Counters ----
Received: 0 0
VLAN Filtered: 0 0
Security Filtered: 0 0
Other Discards: 0 0

---- Egress Counters ----
Unicast: 0 0
Multicast: 0 0
Broadcast: 0 0
Egress Filtered: 0 0
TailDrop: 0 0
Forward Restrict: 0 0
Congestion Filtered: 0 0
Control Packets: 0 0
---- Drop Counters ----
Drop Mode: 0 0
Drop Counter: 0 0

show pfe statistics bridge fpc (EX8200-40XS (40-port SFP+) Line Card)

user@switch> show pfe statistics bridge fpc 8
Slot 8
PFE: 0 1 2 3

---- Ingress Counters ----
Received: 0 3 0 0
VLAN Filtered: 0 0 0 0
Security Filtered: 0 0 0 0
Other Discards: 0 1 0 0

---- Egress Counters ----
Unicast: 0 0 0 0
Multicast: 0 0 0 0
Broadcast: 0 0 0 0
Egress Filtered: 0 0 0 0
TailDrop: 0 0 0 0
Forward Restrict: 0 0 0 0
Congestion Filtered: 0 2 0 0
Control Packets: 4 0 0 0
---- Drop Counters ----
Drop Mode: 0 0 0 0
Drop Counter: 0 1 0 0

MUX PFE: 4 5
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop Mode:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drop Count:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
traceroute

Syntax
traceroute host
<as-number-lookup>
<bypass-routing>
<clns>
<gateway address>
<inet | inet6>
<interface interface-name>
<logical system logical-system-name>
<monitor host>
<mpls (ldp FEC address | rsvp label-switched-path-name)>
<no-resolve>
<propagate-ttl>
<routing-instance routing-instance-name>
<source source-address>
<tos value>
<ttl value>
<wait seconds>

Syntax (QFX Series)
traceroute host
<as-number-lookup>
<bypass-routing>
<gateway address>
<inet>
<interface interface-name>
<monitor host>
<no-resolve>
<routing-instance routing-instance-name>
<source source-address>
<tos value>
<ttl value>
<wait seconds>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
mpls option introduced in Junos OS Release 9.2.
Command introduced in Junos OS Release 11.1 for the QFX Series.
propagate-ttl option introduced in Junos OS Release 12.1.

Description
Display the route that packets take to a specified network host. Use traceroute as a debugging tool to locate points of failure in a network.

Options
host—IP address or name of remote host.

as-number-lookup—(Optional) Display the autonomous system (AS) number of each intermediate hop on the path from the host to the destination.

bypass-routing—(Optional) Bypass the normal routing tables and send requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to display a route to a local system through an interface that has no route through it.
clns—(Optional) Trace the route belonging to the Connectionless Network Service (CLNS).

gateway address—(Optional) Address of a router or switch through which the route transits.

inet | inet6—(Optional) Trace the route belonging to IPv4 or IPv6, respectively.

interface interface-name—(Optional) Name of the interface over which to send packets.

logical-system logical-system-name—(Optional) Perform this operation on all logical systems or on a particular logical system.

monitor host—(Optional) Display real-time monitoring information for the specified host.

mpls (ldp FEC address | rsvp label-switched-path name)—(Optional) See traceroute mpls ldp and traceroute mpls rsvp.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

propagate-ttl—(Optional) On the PE routing device, use this option to view locally generated Routing Engine transit traffic. This is applicable for MPLS L3VPN traffic only.

Use for troubleshooting, when you want to view hop-by-hop information from the local provider router to the remote provider router, when TTL decrementing is disabled on the core network using the no-propagate-ttl configuration statement.

NOTE: Using propagate-ttl with traceroute on the CE router does not show hop-by-hop information.

routing-instance routing-instance-name—(Optional) Name of the routing instance for the traceroute attempt.

source source-address—(Optional) Source address of the outgoing traceroute packets.

tos value—(Optional) Value to include in the IP type-of-service (ToS) field. The range of values is 0 through 255.

ttl value—(Optional) Maximum time-to-live value to include in the traceroute request. The range of values is 0 through 128.

wait seconds—(Optional) Maximum time to wait for a response to the traceroute request.
traceroute as-number-lookup host on page 3811
traceroute no-resolve on page 3811
traceroute propogate-ttl on page 3812
traceroute (Between CE Routers, Layer 3 VPN) on page 3812
traceroute (Through an MPLS LSP) on page 3812

Output Fields Table 444 on page 3811 describes the output fields for the traceroute command. Output fields are listed in the approximate order in which they appear.

Table 444: traceroute Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute to</td>
<td>IP address of the receiver.</td>
</tr>
<tr>
<td>hops max</td>
<td>Maximum number of hops allowed.</td>
</tr>
<tr>
<td>byte packets</td>
<td>Size of packets being sent.</td>
</tr>
<tr>
<td>number-of-hops</td>
<td>Number of hops from the source to the named router or switch.</td>
</tr>
<tr>
<td>router-name</td>
<td>Name of the router or switch for this hop.</td>
</tr>
<tr>
<td>address</td>
<td>Address of the router or switch for this hop.</td>
</tr>
<tr>
<td>Round trip time</td>
<td>Average round-trip time, in milliseconds (ms).</td>
</tr>
</tbody>
</table>

Sample Output

ttraceroute

user@host> traceroute santacruz
traceroute to green.company.net (10.156.169.254), 30 hops max, 40 byte packets
1 blue23 (10.168.1.254) 2.370 ms 2.853 ms 0.367 ms
2 red14 (10.168.255.250) 0.778 ms 2.937 ms 0.446 ms
3 yellow (10.156.169.254) 7.737 ms 89.905 ms 0.834 ms

ttraceroute as-number-lookup host

user@host> traceroute as-number-lookup 10.100.1.1
traceroute to 10.100.1.1 (10.100.1.1), 30 hops max, 40 byte packets
1  10.39.1.1 (10.39.1.1) 0.779 ms 0.728 ms 0.562 ms
2  10.39.1.6 (10.39.1.6) [AS  32] 0.657 ms 0.611 ms 0.446 ms
3  10.100.1.1 (10.100.1.1) [AS  10, 40, 50] 0.880 ms 0.808 ms 0.774 ms

ttraceroute no-resolve

user@host> traceroute santacruz no-resolve
traceroute to green.company.net (10.156.169.254), 30 hops max, 40 byte packets
1  10.168.1.254 0.458 ms 0.370 ms 0.365 ms
2  10.168.255.250 0.474 ms 0.450 ms 0.444 ms
traceroute propogate-ttl

user@host> traceroute propogate-ttl 100.200.2.2 routing-instance VPN-A
traceroute to 100.200.2.2 (100.200.2.2) from 1.1.0.2, 30 hops max, 40 byte packets

1  1.2.0.2 (1.2.0.2)  2.456 ms  1.753 ms  1.672 ms
   MPLS Label=299776 CoS=0 TTL=1 S=0
   MPLS Label=299792 CoS=0 TTL=1 S=1
2  1.3.0.2 (1.3.0.2)  1.213 ms  1.225 ms  1.166 ms
   MPLS Label=299792 CoS=0 TTL=1 S=1
3  100.200.2.2 (100.200.2.2)  1.422 ms  1.521 ms  1.443 ms

traceroute (Between CE Routers, Layer 3 VPN)

user@host> traceroute vpn09
traceroute to vpn09.skybank.net (10.255.14.179), 30 hops max, 40 byte packets
1  10.39.10.21 (10.39.10.21)  0.598 ms  0.500 ms  0.461 ms
2  10.39.1.13 (10.39.1.13)  0.796 ms  0.775 ms  0.806 ms
   MPLS Label=100006 CoS=0 TTL=1 S=1
3  vpn09.skybank.net (10.255.14.179)  0.783 ms  0.716 ms  0.686

traceroute (Through an MPLS LSP)

user@host> traceroute mpls1
traceroute to 10.168.1.224 (10.168.1.224), 30 hops max, 40 byte packets
1  mpls1-sr0.company.net (10.168.200.101)  0.555 ms  0.393 ms  0.367 ms
   MPLS Label=1024 CoS=0 TTL=1
2  mpls5-lo0.company.net (10.168.1.224)  0.420 ms  0.394 ms  0.401 ms

Operational Commands: RPM
show services rpm active-servers

Syntax
show services rpm active-servers

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description
Display the protocols and corresponding ports for which a router or switch is configured as a real-time performance monitoring (RPM) server.

Options
This command has no options.

Required Privilege Level
view

List of Sample Output
show services rpm active-servers on page 3813

Output Fields
Table 445 on page 3813 lists the output fields for the show services rpm active-servers command. Output fields are listed in the approximate order in which they appear.

Table 445: show services rpm active-servers Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol configured on the receiving probe server. The protocol can be the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP).</td>
</tr>
<tr>
<td>Port</td>
<td>Port configured on the receiving probe server.</td>
</tr>
<tr>
<td>Destination interface name</td>
<td>Output interface name for the probes.</td>
</tr>
</tbody>
</table>

Sample Output
show services rpm active-servers

user@host>  show services rpm active-servers
  Protocol: TCP, Port: 50000, Destination interface name: lt-0/0/0.0
  Protocol: UDP, Port: 50001, Destination interface name: lt-0/0/0.0
show services rpm history-results

Syntax

show services rpm history-results
  <brief | detail>
  <owner owner>
  <since time>
  <test name>

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 13.2 for PTX Series Packet Transport Routers.

Description

Display standard information about the results of the last 50 probes for each real-time performance monitoring (RPM) instance.

Options

none—Display the results of the last 50 probes for all RPM instances.

brief | detail—(Optional) Display the specified level of output.

owner owner—(Optional) Display information for the specified probe owner.

since time—(Optional) Display information from the specified time. Specify time as yyyy-mm-dd.hh:mm:ss.

test name—(Optional) Display information for the specified test.

Required Privilege Level

view

List of Sample Output

show services rpm history-results on page 3815
show services rpm history-results detail on page 3815

Output Fields

Table 446 on page 3814 lists the output fields for the show services rpm history-results command. Output fields are listed in the approximate order in which they appear.

Table 446: show services rpm history-results Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Probe owner.</td>
<td>All levels</td>
</tr>
<tr>
<td>Test</td>
<td>Name of a test for a probe instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Probe received</td>
<td>Timestamp when the probe result was determined.</td>
<td>All levels</td>
</tr>
<tr>
<td>Round trip time</td>
<td>Average ping round-trip time (RTT), in microseconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Probe results</td>
<td>Result of a particular probe performed by a remote host. The following information is contained in the results:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Response received—Timestamp when the probe result was determined.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rtt—Average ping round-trip time (RTT), in microseconds.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 446: show services rpm history-results Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results over current test</td>
<td>Displays the results for the current test by probe at the time each probe was completed, as well as the status of the current test at the time the probe was completed.</td>
<td>detail</td>
</tr>
<tr>
<td>Probes sent</td>
<td>Number of probes sent with the current test.</td>
<td>detail</td>
</tr>
<tr>
<td>Probes received</td>
<td>Number of probe responses received within the current test.</td>
<td>detail</td>
</tr>
<tr>
<td>Loss percentage</td>
<td>Percentage of lost probes for the current test.</td>
<td>detail</td>
</tr>
<tr>
<td>Measurement</td>
<td>Increment of measurement. Possible values are round-trip time delay and, for the probe type icmp-ping-timestamp, the egress and ingress delay:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>- <strong>Minimum</strong>—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Maximum</strong>—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Average</strong>—Average RTT, ingress delay, or egress delay measured over the course of the current test.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Jitter</strong>—Difference, in microseconds, between the maximum and minimum RTT measured over the course of the current test.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Stddev</strong>—Standard deviation of the round-trip time, in microseconds, measured over the course of the current test.</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Output

**show services rpm history-results**

```
user@host> show services rpm history-results
Owner, Test                 Probe received              Round trip time
p1, t1                      Wed Aug 12 01:02:35 2009              315 usec
p1, t1                      Wed Aug 12 01:02:36 2009              266 usec
p1, t1                      Wed Aug 12 01:02:37 2009              314 usec
p1, t1                      Wed Aug 12 01:02:38 2009              388 usec
p1, t1                      Wed Aug 12 01:02:39 2009              316 usec
p1, t1                      Wed Aug 12 01:02:40 2009              271 usec
p1, t1                      Wed Aug 12 01:02:41 2009              314 usec
p1, t1                      Wed Aug 12 01:02:42 2009              1180 usec
```

**show services rpm history-results detail**

```
user@host> show services rpm history-results detail
Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
  Response received, Wed Aug 12 01:02:35 2009,
  Client and server hardware timestamps
  Rtt: 315 usec
Results over current test:
  Probes sent: 1, Probes received: 1, Loss percentage: 0
  Measurement: Round trip time
    Samples: 1, Minimum: 315 usec, Maximum: 315 usec, Average: 315 usec,
    Peak to peak: 0 usec, Stddev: 0 usec, Sum: 315 usec
```
Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
Response received, Wed Aug 12 01:02:36 2009,
Client and server hardware timestamps
Rtt: 266 usec, Round trip jitter: -50 usec,
Round trip interarrival jitter: 3 usec
Results over current test:
Probes sent: 2, Probes received: 2, Loss percentage: 0
Measurement: Round trip time
Samples: 2, Minimum: 266 usec, Maximum: 315 usec, Average: 291 usec,
Peak to peak: 49 usec, Stddev: 24 usec, Sum: 581 usec
Measurement: Negative round trip jitter
Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
Response received, Wed Aug 12 01:02:37 2009,
Client and server hardware timestamps
Rtt: 314 usec, Round trip jitter: 49 usec,
Round trip interarrival jitter: 6 usec
Results over current test:
Probes sent: 3, Probes received: 3, Loss percentage: 0
Measurement: Round trip time
Samples: 3, Minimum: 266 usec, Maximum: 315 usec, Average: 298 usec,
Peak to peak: 49 usec, Stddev: 23 usec, Sum: 895 usec
Measurement: Positive round trip jitter
Samples: 1, Minimum: 49 usec, Maximum: 49 usec, Average: 49 usec,
Peak to peak: 0 usec, Stddev: 0 usec, Sum: 49 usec
Measurement: Negative round trip jitter
Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec

Owner: p1, Test: t1, Probe type: icmp-ping-timestamp
Probe results:
Response received, Wed Aug 12 01:02:38 2009,
Client and server hardware timestamps
Rtt: 388 usec, Round trip jitter: 74 usec,
Round trip interarrival jitter: 10 usec
Results over current test:
Probes sent: 4, Probes received: 4, Loss percentage: 0
Measurement: Round trip time
Samples: 4, Minimum: 266 usec, Maximum: 388 usec, Average: 321 usec,
Peak to peak: 122 usec, Stddev: 44 usec, Sum: 1283 usec
Measurement: Positive round trip jitter
Samples: 2, Minimum: 49 usec, Maximum: 74 usec, Average: 62 usec,
Peak to peak: 25 usec, Stddev: 12 usec, Sum: 123 usec
Measurement: Negative round trip jitter
Samples: 1, Minimum: 50 usec, Maximum: 50 usec, Average: 50 usec,
Peak to peak: 0 usec, Stddev: 0 usec, Sum: 50 usec
show services rpm probe-results

Syntax

```
show services rpm probe-results
<owner owner>
<test name>
```

Release Information

- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the results of the most recent real-time performance monitoring (RPM) probes.

Options

- **none**—Display all results of the most recent RPM probes.
- **owner owner**—(Optional) Display information for the specified probe owner.
- **test name**—(Optional) Display information for the specified test.

Required Privilege Level

- **view**

List of Sample Output

- show services rpm probe-results on page 3820
- show services rpm probe-results (BGP Neighbor Discovery) on page 3821

Output Fields

Table 447 on page 3817 lists the output fields for the `show services rpm probe-results` command. Output fields are listed in the approximate order in which they appear.

Table 447: show services rpm probe-results Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Owner name. When you configure the probe owner statement at the [edit services rpm] hierarchy level, this field displays the configured owner name. When you configure BGP neighbor discovery through RPM, the output for this field is <code>Rpm-Bgp-Owner</code>.</td>
</tr>
<tr>
<td>Test</td>
<td>Name of a test representing a collection of probes. When you configure the test test-name statement at the [edit services rpm probe owner] hierarchy level, the field displays the configured test name. When you configure BGP neighbor discovery through RPM, the output for this field is <code>Rpm-BGP-Test-n</code>, where <code>n</code> is a cumulative number.</td>
</tr>
<tr>
<td>Target address</td>
<td>Destination address used for the probes.</td>
</tr>
<tr>
<td>Source address</td>
<td>Source address used for the probes.</td>
</tr>
<tr>
<td>Test size</td>
<td>Number of probes within a test.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Routing Instance Name</strong></td>
<td>(BGP neighbor discovery) Name of the configured (if any) routing instance, logical system name, or both, in which the probe is configured:</td>
</tr>
<tr>
<td></td>
<td>• When a routing instance is defined within a logical system, the logical system name is followed by the routing instance name. A slash (/) is used to separate the two entities. For example, if the routing instance called RI is configured within the logical system called LS, the name in the output field is LS/RI.</td>
</tr>
<tr>
<td></td>
<td>• When a routing instance is configured but the default logical system is used, the name in the output field is the name of the routing instance.</td>
</tr>
<tr>
<td></td>
<td>• When a logical system is configured but the default routing instance is used, the name in the output field is the name of the logical system followed by default. A slash (/) is used to separate the two entities. For example, LS/default.</td>
</tr>
<tr>
<td><strong>Probe results</strong></td>
<td>Raw measurement of a particular probe sample done by a remote host. This data is provided separately from the calculated results. The following information is contained in the raw measurement:</td>
</tr>
<tr>
<td></td>
<td>• Response received—Timestamp when the probe result was determined.</td>
</tr>
<tr>
<td></td>
<td>• Client and server hardware timestamps—if timestamps are configured, an entry appears at this point.</td>
</tr>
<tr>
<td></td>
<td>• Rtt—Average ping round-trip time (RTT), in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Egress jitter—Egress jitter, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Ingress jitter—Ingress jitter, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Round trip jitter—Round-trip jitter, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Egress interarrival jitter—Egress interarrival jitter, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Ingress interarrival jitter—Ingress interarrival jitter, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Round trip interarrival jitter—Round-trip interarrival jitter, in microseconds.</td>
</tr>
<tr>
<td><strong>Results over current test</strong></td>
<td>Probes are grouped into tests, and the statistics are calculated for each test. If a test contains 10 probes, the average, minimum, and maximum results are calculated from the results of those 10 probes. If the command is issued while the test is in progress, the statistics use information from the completed probes.</td>
</tr>
<tr>
<td></td>
<td>• Probes sent—Number of probes sent within the current test.</td>
</tr>
<tr>
<td></td>
<td>• Probes received—Number of probe responses received within the current test.</td>
</tr>
<tr>
<td></td>
<td>• Loss percentage—Percentage of lost probes for the current test.</td>
</tr>
<tr>
<td></td>
<td>• Measurement—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type icmp-ping-timestamp, the egress delay and ingress delay.</td>
</tr>
<tr>
<td></td>
<td>For each measurement type, the following individual calculated results are provided:</td>
</tr>
<tr>
<td></td>
<td>• Samples—Number of probes.</td>
</tr>
<tr>
<td></td>
<td>• Minimum—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</td>
</tr>
<tr>
<td></td>
<td>• Maximum—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</td>
</tr>
<tr>
<td></td>
<td>• Average—Average RTT, ingress delay, or egress delay measured over the course of the current test.</td>
</tr>
<tr>
<td></td>
<td>• Peak to peak—Peak-to-peak difference, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Stddet—Standard deviation, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Sum—Statistical sum.</td>
</tr>
</tbody>
</table>
Table 447: show services rpm probe-results Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results over last test</td>
<td>Results for the most recently completed test. If the command is issued while the first test is in progress, this information is not displayed.</td>
</tr>
<tr>
<td></td>
<td>• Probes sent—Number of probes sent for the most recently completed test.</td>
</tr>
<tr>
<td></td>
<td>• Probes received—Number of probe responses received for the most recently completed test.</td>
</tr>
<tr>
<td></td>
<td>• Loss percentage—Percentage of lost probes for the most recently completed test.</td>
</tr>
<tr>
<td></td>
<td>• Test completed—Time the most recent test was completed.</td>
</tr>
<tr>
<td></td>
<td>• Measurement—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe type <code>icmp-ping-timestamp</code>, the egress delay and ingress delay.</td>
</tr>
<tr>
<td></td>
<td>For each measurement type, the following individual calculated results are provided:</td>
</tr>
<tr>
<td></td>
<td>• Samples—Number of probes.</td>
</tr>
<tr>
<td></td>
<td>• Minimum—Minimum RTT, ingress delay, or egress delay measured for the most recently completed test.</td>
</tr>
<tr>
<td></td>
<td>• Maximum—Maximum RTT, ingress delay, or egress delay measured for the most recently completed test.</td>
</tr>
<tr>
<td></td>
<td>• Average—Average RTT, ingress delay, or egress delay measured for the most recently completed test.</td>
</tr>
<tr>
<td></td>
<td>• Peak to peak—Peak-to-peak difference, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Stddev—Standard deviation, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Sum—Statistical sum.</td>
</tr>
<tr>
<td>Results over all tests</td>
<td>Displays statistics made for all the probes, independently of the grouping into tests, as well as statistics for the current test.</td>
</tr>
<tr>
<td></td>
<td>• Probes sent—Number of probes sent in all tests.</td>
</tr>
<tr>
<td></td>
<td>• Probes received—Number of probe responses received in all tests.</td>
</tr>
<tr>
<td></td>
<td>• Loss percentage—Percentage of lost probes in all tests.</td>
</tr>
<tr>
<td></td>
<td>• Measurement—Measurement type. Possible values are round-trip time, positive round-trip jitter, negative round-trip jitter, egress time, positive egress jitter, negative egress jitter, ingress time, positive ingress jitter, negative ingress jitter, and, for the probe types <code>icmp-ping-timestamp</code> and <code>udp-ping-timestamp</code>, the egress delay and ingress delay.</td>
</tr>
<tr>
<td></td>
<td>For each measurement type, the following individual calculated results are provided:</td>
</tr>
<tr>
<td></td>
<td>• Samples—Number of probes.</td>
</tr>
<tr>
<td></td>
<td>• Minimum—Minimum RTT, ingress delay, or egress delay measured over the course of the current test.</td>
</tr>
<tr>
<td></td>
<td>• Maximum—Maximum RTT, ingress delay, or egress delay measured over the course of the current test.</td>
</tr>
<tr>
<td></td>
<td>• Average—Average RTT, ingress delay, or egress delay measured over the course of the current test.</td>
</tr>
<tr>
<td></td>
<td>• Peak to peak—Peak-to-peak difference, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Stddev—Standard deviation, in microseconds.</td>
</tr>
<tr>
<td></td>
<td>• Sum—Statistical sum.</td>
</tr>
</tbody>
</table>
Sample Output

show services rpm probe-results

user@host> show services rpm probe-results
Owner: ADSN-J4300.ADSN-J2300.D2, Test: 75300002
Target address: 172.16.54.172, Source address: 10.206.0.1,
Probe type: udp-ping-timestamp, Test size: 10 probes
Probe results:
  Response received, Tue Feb 6 14:53:15 2007,
  Client and server hardware timestamps
  Rtt: 575 usec, Egress jitter: 5 usec, Ingress jitter: 8 usec,
  Round trip jitter: 12 usec, Egress interarrival jitter: 8 usec,
  Ingress interarrival jitter: 7 usec, Round trip interarrival jitter: 7 usec,

  Round trip interarrival jitter: 669 usec

Results over current test:
  Probes sent: 10, Probes received: 10, Loss percentage: 0
  Measurement: Round trip time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stdddev: 738 usec, Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stdddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stdddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stdddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stdddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stdddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stdddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stdddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Ingress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stdddev: 665 usec, Sum: xxxx usec

Results over last test:
  Probes sent: 10, Probes received: 10, Loss percentage: 0
  Test completed on Tue Feb 6 14:53:16 2007
  Measurement: Round trip time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stdddev: 738 usec, Sum: xxxx usec
  Measurement: Positive round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stdddev: 679 usec, Sum: xxxx usec
  Measurement: Negative round trip jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stdddev: 665 usec, Sum: xxxx usec
  Measurement: Egress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
    Peak to peak: 2054 usec, Stdddev: 738 usec, Sum: xxxx usec
  Measurement: Positive Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
    Peak to peak: 2049 usec, Stdddev: 679 usec, Sum: xxxx usec
  Measurement: Negative Egress jitter
    Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
    Peak to peak: 1807 usec, Stdddev: 665 usec, Sum: xxxx usec
  Measurement: Ingress time
    Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
Peak to peak: 2049 usec, Stdev: 679 usec, Sum: xxxx usec
Measurement: Negative Egress  jitter
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
Peak to peak: 1807 usec, Stdev: 665 usec, Sum: xxxx usec
Measurement: Ingress time
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
Peak to peak: 2054 usec, Stdev: 738 usec, Sum: xxxx usec
Measurement: Positive Ingress  jitter
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
Peak to peak: 2049 usec, Stdev: 679 usec, Sum: xxxx usec
Measurement: Negative Ingress  jitter
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
Peak to peak: 1807 usec, Stdev: 665 usec, Sum: xxxx usec
Results over all tests:
Probes sent: 560, Probes received: 560, Loss percentage: 0
Measurement: Round trip time
Samples: 560, Minimum: 805 usec, Maximum: 3114 usec, Average: 1756 usec,
Peak to peak: 2309 usec, Stdev: 519 usec, Sum: xxxx usec
Measurement: Positive round trip jitter
Samples: 257, Minimum: 0 usec, Maximum: 2054 usec, Average: 597 usec,
Peak to peak: 2054 usec, Stdev: 427 usec, Sum: xxxx usec
Measurement: Negative round trip jitter
Samples: 302, Minimum: 1 usec, Maximum: 1812 usec, Average: 511 usec,
Peak to peak: 1811 usec, Stdev: 408 usec, Sum: xxxx usec
Measurement: Egress time
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
Peak to peak: 2054 usec, Stdev: 738 usec, Sum: xxxx usec
Measurement: Positive Egress  jitter
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
Peak to peak: 2049 usec, Stdev: 679 usec, Sum: xxxx usec
Measurement: Negative Egress  jitter
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
Peak to peak: 1807 usec, Stdev: 665 usec, Sum: xxxx usec
Measurement: Ingress time
Samples: 10, Minimum: 805 usec, Maximum: 2859 usec, Average: 1644 usec,
Peak to peak: 2054 usec, Stdev: 738 usec, Sum: xxxx usec
Measurement: Positive Ingress  jitter
Samples: 5, Minimum: 5 usec, Maximum: 2054 usec, Average: 876 usec,
Peak to peak: 2049 usec, Stdev: 679 usec, Sum: xxxx usec
Measurement: Negative Ingress  jitter
Samples: 5, Minimum: 5 usec, Maximum: 1812 usec, Average: 926 usec,
Peak to peak: 1807 usec, Stdev: 665 usec, Sum: xxxx usec

show services rpm probe-results (BGP Neighbor Discovery)

user@host> show services rpm probe-results
Owner: Rpm-Bgp-Owner, Test: Rpm-Bgp-Test-1
Target address: 10.209.152.37, Probe type: icmp-ping, Test size: 5 probes
Routing Instance Name: LS1/RI1
Probe results:
Response received, Fri Oct 28 05:20:23 2005
Rtt: 662 usec
Results over current test:
Probes sent: 5, Probes received: 5, Loss percentage: 0
Measurement: Round trip time
Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
Jitter: 133 usec, Stdev: 53 usec
Results over all tests:
Probes sent: 5, Probes received: 5, Loss percentage: 0
Measurement: Round trip time
Minimum: 529 usec, Maximum: 662 usec, Average: 585 usec,
Jitter: 133 usec, Stddev: 53 usec

Operational Commands: SNMP
## clear snmp rmon history

**Syntax**
```
clear snmp rmon history <interface-name | all>
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Delete the samples of Ethernet statistics collected, but do not delete the RMON history configuration.

The `clear snmp rmon history` command deletes all the samples collected for the interface configured for the history group, but not the configuration of that group. If you want to delete the RMON history group configuration, you must use the `delete snmp rmon history` configuration-mode command.

**Options**
- `interface-name`—Delete the samples of Ethernet statistics collected for this interface.
- `all`—Delete the samples of Ethernet statistics collected for all interfaces that have been configured for RMON monitoring.

**Required Privilege Level**
clear

**Related Documentation**
- show snmp rmon history on page 3848
### clear snmp statistics

**Syntax**
```
clear snmp statistics
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

**Options**
This command has no options.

**Required Privilege**
`clear`

**Related Documentation**
- show snmp statistics on page 3852

**List of Sample Output**
clear snmp statistics on page 3824

**Output Fields**
See show snmp statistics for an explanation of output fields.

#### Sample Output

**clear snmp statistics**

In the following example, SNMP statistics are displayed before and after the `clear snmp statistics` command is issued:

```bash
user@host> show snmp statistics
SNMP statistics:
Input:
  Packets: 8, Bad versions: 0, Bad community names: 0,
  Bad community uses: 0, ASN parse errors: 0,
  Too bigs: 0, No such names: 0, Bad values: 0,
  Read onlys: 0, General errors: 0,
  Total request varbinds: 8, Total set varbinds: 0,
  Get requests: 0, Get nexts: 8, Set requests: 0,
  Get responses: 0, Traps: 0,
  Silent drops: 0, Proxy drops 0
Output:
  Packets: 2298, Too bigs: 0, No such names: 0,
  Bad values: 0, General errors: 0,
  Get requests: 0, Get nexts: 0, Set requests: 0,
  Get responses: 8, Traps: 2290

user@host> clear snmp statistics

user@host> show snmp statistics
SNMP statistics:
Input:
  Packets: 0, Bad versions: 0, Bad community names: 0,
  Bad community uses: 0, ASN parse errors: 0,
  Too bigs: 0, No such names: 0, Bad values: 0,
  Read onlys: 0, General errors: 0,
```
Total request varbinds: 0, Total set varbinds: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0,
Silent drops: 0, Proxy drops 0
Output:
Packets: 0, Too bigs: 0, No such names: 0,
Bad values: 0, General errors: 0,
Get requests: 0, Get nexts: 0, Set requests: 0,
Get responses: 0, Traps: 0
**request snmp spoof-trap**

**Syntax**

```plaintext
request snmp spoof-trap<br>variable-bindings<br>object<br>instance<br>value
```

**Release Information**

Command introduced in Junos OS Release 8.2.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Spoof (mimic) the behavior of a Simple Network Management Protocol (SNMP) trap.

**Options**

- `<trap>`—Name of the trap to spoof.
- `variable-bindings object instance value`—(Optional) List of variables and values to include in the trap. Each variable binding is specified as an object name, the object instance, and the value (for example, `ifIndex[14] = 14`). Enclose the list of variable bindings in quotation marks (" " ) and use a comma to separate each object name, instance, and value definition (for example, `variable-bindings "ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2"`). Objects included in the trap definition that do not have instances and values specified as part of the command are included in the trap and spoofed with automatically generated instances and values.
- `<dummy name>`—A dummy trap name to display the list of available traps.
- `?`—Question mark (?) to display possible completions.

**Required Privilege Level**

`request`

**List of Sample Output**

`request snmp spoof-trap (with Variable Bindings)` on page 3826
`request snmp spoof-trap (Illegal Trap Name)` on page 3826
`request snmp spoof-trap (Question Mark ?)` on page 3830

**Sample Output**

**request snmp spoof-trap (with Variable Bindings)**

```plaintext
user@host> request snmp spoof-trap linkUp variable-bindings "ifIndex[14] = 14, ifAdminStatus[14] = 1, ifOperStatus[14] = 2"
Spoof trap request result: trap sent successfully
```

**request snmp spoof-trap (Illegal Trap Name)**

```plaintext
user@host> request snmp spoof-trap xx
Spoof trap request result: trap not found
```

Allowed Traps:
- adslAtucInitFailureTrap
- adslAtucPerfESSThreshTrap
- adslAtucPerfLofsThreshTrap
- adslAtucPerfLolsThreshTrap
- adslAtucPerfLossThreshTrap
- adslAtucPerfLprsThreshTrap
- adslAtucRateChangeTrap
- adslAturPerfESSThreshTrap
adslAturPerfLofsThreshTrap
adslAturPerfLossThreshTrap
adslAturPerfLprsThreshTrap
adslAturRateChangeTrap
apsEventChannelMismatch
apsEventFEPLF
apsEventModeMismatch
apsEventPSBF
apsEventSwitchover
authenticationFailure
bfdSessDown
bfdSessUp
bgpBackwardTransition
bgpEstablished
coldStart
dlswrTrapCircuitDown
dlswrTrapCircuitUp
dlswrTrapTConnDown
dlswrTrapTConnPartnerReject
dlswrTrapTConnProtViolation
dlswrTrapTConnUp
dsx1LineStatusChange
dsx3LineStatusChange
entConfigChange
fallingAlarm
frDLICStatusChange
ggsnTrapChanged
ggsnTrapCleared
ggsnTrapNew
gmplsTunnelDown
ifMauJabberTrap
ipv6IfStateChange
isisAreaMismatch
isisAttemptToExceedMaxSequence
isisAuthenticationFailure
isisAuthenticationTypeFailure
isisCorruptedLSPDetected
isisDatabaseOverload
isisDLenMismatch
isisLSPTooLargeToPropagate
isisManualAddressDrops
isisMaxAreaAddressesMismatch
isisOriginatingLSPBufferSizeMismatch
isisOwnLSPPurge
isisProtocolsSupportedMismatch
isisRejectedAdjacency
isisSequenceNumberSkip
isisVersionSkew
jnxAcessAuthServerDisabled
jnxAcessAuthServerEnabled
jnxAcessAuthServiceDown
jnxAcessAuthServiceUp
jnxBfdSessDetectionTimeHigh
jnxBfdSessTxIntervalHigh
jnxBgpM2BackwardTransition
jnxBgpM2Established
jnxCmCfgChange
jnxCmRescueChange
jnxCollFlowOverload
jnxCollFlowOverloadCleared
jnxCollFtpSwitchover
jnxCollMemoryAvailable
jnxCollMemoryUnavailable
jnxCollUnavailableDest
jnxCollUnavailableDestCleared
jnxCollUnsuccessfulTransfer
jnxDfcHardMemThresholdExceeded
jnxDfcHardMemUnderThreshold
jnxDfcHardPpsThresholdExceeded
jnxDfcHardPpsUnderThreshold
jnxDfcSoftMemThresholdExceeded
jnxDfcSoftMemUnderThreshold
jnxDfcSoftPpsThresholdExceeded
jnxDfcSoftPpsUnderThreshold
jnxEventTrap
jnxEEventTrap
jnxFEBSwitchover
jnxFanFailure
jnxFanOK
jnxFruCheck
jnxFruFailed
jnxFruInsertion
jnxFruOK
jnxFruOffline
jnxFruOnline
jnxFruPowerOff
jnxFruPowerOn
jnxFruRemoval
jnxDiskFailed
jnxDiskMissinjx
jnxDiscPatternUpdateTrap
jnxJsChassisClusterSwitchover
jnxFwAuthCapacityExceeded
jnxFwAuthFailure
jnxFwAuthServiceDown
jnxFwAuthServiceUp
jnxFwAddrPoolThresholdStatus
jnxFwScreenAttack
jnxFwScreenCfgChange
jnxDpdLspDown
jnxDpdLspUp
jnxDpdSesDown
jnxDpdSesUp
jnXMStCistPortLoopProtectStateChangeTrap
jnXMStCistPortRootProtectStateChangeTrap
jnXMStErrTrap
jnXMStGenTrap
jnXMStInvalidBdpduRxdTrap
jnXMStMstiPortLoopProtectStateChangeTrap
jnXMStMstiPortRootProtectStateChangeTrap
jnXMStNewRootTrap
jnXMStProtocolMigrationTrap
jnXMStRegionConfigChangeTrap
jnXMStTopologyChgTrap
jnXMStChassisClusterSwitchover
jnXMStIfConfigError
jnXMStIfRxPacket
jnXMStIfStateChange
jnXMStIfStateChange
jnXospfv3LsdbApproachingOverflow
jnXospfv3LsdbOverflow
jnXospfv3NbrRestartHelperStatusChange
jnXospfv3NbrStateChange
jnXospfv3NssaTranslatorStatusChange
jnXospfv3RestartStatusChange
jnXospfv3VirtIfConfigError
jnXospfv3VirtIfRxBadPacket
jnXospfv3VirtIfStateChange
jnXospfv3VirtNbrRestartHelperStatusChange
jnXospfv3VirtNbrStateChange
jnOtnAlarmCleared
jnOtnAlarmSet
jnOverTemperature
jnPMonOverloadCleared
jnPMonOverloadSet
jnPingEgressJitterThresholdExceeded
jnPingEgressStdDevThresholdExceeded
jnPingEgressThresholdExceeded
jnPingIngressJitterThresholdExceeded
jnPingIngressStdDevThresholdExceeded
jnPingIngressThresholdExceeded
jnPingRttJitterThresholdExceeded
jnPingRttStdDevThresholdExceeded
jnPingRttThresholdExceeded
jnPortBpduErrorStatusChangeTrap
jnPortLoopProtectStateChangeTrap
jnPortRootProtectStateChangeTrap
jnPowerSupplyFailure
jnPowerSupplyOK
jnRedundancySwitchover
jnRmonAlarmGetFailure
jnRmonGetOk
jnSecAccessIfMacLimitExceeded
jnSecAccessdsRateLimitCrossed
jnSonetAlarmCleared
jnSonetAlarmSet
jnSpSvcSetCpuExceeded
jnSpSvcSetCpuOk
jnSpSvcSetZoneEntered
jnSpSvcSetZoneExited
jnStormEventNotification
jnSyslogTrap
jnTemperatureOK
jnVccpPortDown
jnVccpPortUp
jnVpnIfDown
jnVpnIfUp
jnVpnPwDown
jnVpnPwUp
jnX2aldGlobalMacLimit
jnX2aldInterfaceMacLimit
jnX2aldRoutingInstMacLimit
linkDown
linkUp
lldpRemTablesChange
mfrMibTrapBundleLinkMismatch
mplsLspChange
mplsLspDown
mplsLspInfoChange
mplsLspInfoDown
mplsLspInfoPathDown
mplsLspInfoPathUp
mplsLspInfoUp
mplsLspPathDown
mplsLspPathUp
mplsLspUp
mplsNumVrfRouteMaxThreshExceeded
mplsNumVrfRouteMidThreshExceeded
mplsNumVrfSecIlglLblThrshExcd
mplsTunnelDown
mplsTunnelReoptimized
mplsTunnelRerouted
mplsTunnelUp
mplsVrfIFDown
mplsVrfIFUp
mplsXCDown
mplsXCUp
msdpBackwardTransition
msdpEstablished
newRoot
ospfIfAuthFailure
ospfIfConfigError
ospfIfRxBadPacket
ospfIfStateChange
ospfLsdbApproachingOverflow
ospfLsdbOverflow
ospfMaxAgeLsa
ospfNbrStateChange
ospfOriginateLsa
ospfTxRetransmit
ospfVirtIfAuthFailure
ospfVirtIfConfigError
ospfVirtIfRxBadPacket
ospfVirtIfStateChange
ospfVirtIfTxRetransmit
ospfVirtNbrStateChange
pethMainPowerUsageOffNotification
pethMainPowerUsageOnNotification
pethPsePortOnOffNotification
pingProbeFailed
pingTestCompleted
pingTestFailed
ptopoConfigChange
risingAlarm
rpMauJabberTrap
sdlcLSStatusChange
sdlcPortStatusChange
topologyChange
traceRoutePathChange
traceRouteTestCompleted
traceRouteTestFailed
vrrpTrapAuthFailure
vrrpTrapNewMaster
warmStart

request snmp spoof-trap (Question Mark ?)

user@host> request snmp spoof-trap ?
Possible completions:
<trap> The name of the trap to spoof
adslAtucInitFailureTrap
adslAtucPerfESsThreshTrap
adslAtucPerfLofsThreshTrap
adslAtucPerfLolsThreshTrap
adslAtucPerfLossThreshTrap
adslAtucPerfLprsThreshTrap
adslAtucRateChangeTrap
adslAturPerfESsThreshTrap
adslAturPerfLofsThreshTrap
adslAturPerfLolsThreshTrap
adslAturPerfLossThreshTrap
adslAturPerfLprsThreshTrap
adslAturRateChangeTrap
apsEventChannelMismatch
apsEventFEPLF
apsEventModeMismatch
apsEventPSBF
apsEventSwitchover
authenticationFailure
bfdSessDown
bfdSessUp
bgpBackwardTransition
bgpEstablished
coldStart
dlswTrapCircuitDown
dlswTrapCircuitUp
---(more 10%)--
show snmp health-monitor

Syntax
show snmp health-monitor
<alarms <detail>> | <logs>

Release Information
Command introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description
Display information about Simple Network Management Protocol (SNMP) health monitor alarms and logs.

Options
none—Display information about all health monitor alarms and logs.
alarms <detail>—(Optional) Display detailed information about health monitor alarms.
logs—(Optional) Display information about health monitor logs.

Required Privilege Level
view

List of Sample Output
show snmp health-monitor on page 3834
show snmp health-monitor alarms detail on page 3836

Output Fields
Table 448 on page 3832 describes the output fields for the show snmp health-monitor command. Output fields are listed in the approximate order in which they appear.

Table 448: show snmp health-monitor Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Index</td>
<td>Alarm identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Variable description</td>
<td>Description of the health monitor object instance being monitored.</td>
<td>All levels</td>
</tr>
<tr>
<td>Variable name</td>
<td>Name of the health monitor object instance being monitored.</td>
<td>All levels</td>
</tr>
<tr>
<td>Value</td>
<td>Current value of the monitored variable in the most recent sample interval.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 448: show snmp health-monitor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the alarm or event entry:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- Alarms:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• active—Entry is fully configured and activated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• falling threshold crossed—Value of the variable has crossed the lower threshold limit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rising threshold crossed—Value of the variable has crossed the upper threshold limit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• under creation—Entry is being configured and is not yet activated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• startup—Alarm is waiting for the first sample of the monitored variable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• object not available—Monitored variable of that type is not available to the health monitor agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• instance not available—Monitored variable's instance is not available to the health monitor agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• object type invalid—Monitored variable is not a numeric value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• object processing errored—An error occurred when the monitored variable was processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unknown—State is not one of the above.</td>
<td></td>
</tr>
<tr>
<td>Variable OID</td>
<td>Object ID to which the variable name is resolved. The format is x.x.x.x.</td>
<td>detail</td>
</tr>
<tr>
<td>Sample type</td>
<td>Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of absolute value or delta value.</td>
<td>detail</td>
</tr>
<tr>
<td>Startup alarm</td>
<td>Alarm that might be sent when this entry is first activated, depending on the following criteria:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Alarm is sent when one of the following situations exists:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is above or equal to the rising threshold and the startup type is either rising alarm or rising or falling alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is below or equal to the falling threshold and the startup type is either falling alarm or rising or falling alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Alarm is not sent when one of the following situations exists:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is above or equal to the rising threshold and the startup type is rising alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is below or equal to the falling threshold and the startup type is rising alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is between the thresholds.</td>
<td></td>
</tr>
<tr>
<td>Owner</td>
<td>Name of the entry configured by the user. If the entry was created through the CLI, the owner has monitor prepended to it.</td>
<td>detail</td>
</tr>
<tr>
<td>Creator</td>
<td>Mechanism by which the entry was configured (Health Monitor).</td>
<td>detail</td>
</tr>
<tr>
<td>Sample interval</td>
<td>Time period between samples (in seconds).</td>
<td>detail</td>
</tr>
<tr>
<td>Rising threshold</td>
<td>Upper limit threshold value as a percentage of the maximum possible value.</td>
<td>detail</td>
</tr>
</tbody>
</table>
### Table 448: show snmp health-monitor Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Falling threshold</td>
<td>Lower limit threshold value as a percentage of the maximum possible value.</td>
<td>detail</td>
</tr>
<tr>
<td>Rising event index</td>
<td>Event triggered when the rising threshold is crossed.</td>
<td>detail</td>
</tr>
<tr>
<td>Falling event index</td>
<td>Event triggered when the falling threshold is crossed.</td>
<td>detail</td>
</tr>
</tbody>
</table>

### Sample Output

```
show snmp health-monitor

user@host> show snmp health-monitor

<table>
<thead>
<tr>
<th>Alarm Index</th>
<th>Variable description</th>
<th>Value</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>32768</td>
<td>Health Monitor: root file system utilization</td>
<td>58</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>jnxHrStoragePercentUsed.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32769</td>
<td>Health Monitor: /config file system utilization</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>jnxHrStoragePercentUsed.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32770</td>
<td>Health Monitor: RE 0 CPU utilization</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>jnxOperatingCPU.9.1.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32773</td>
<td>Health Monitor: RE 0 Memory utilization</td>
<td>35</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>jnxOperatingBuffer.9.1.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32775</td>
<td>Health Monitor: jkernel daemon CPU utilization</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Init daemon</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chassis daemon</td>
<td>50</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Firewall daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Interface daemon</td>
<td>5</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>SNMP daemon</td>
<td>11</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>MIB2 daemon</td>
<td>42</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Sonet APS daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>VRRP daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Alarm daemon</td>
<td>3</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>PFE daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>CRAFT daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Traffic sampling control daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Ilmi daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Remote operations daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>CoS daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Pic Services Logging daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Internal Routing Service Daemon</td>
<td>3</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Network Access Service daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Forwarding UDP daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Routing socket proxy daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Disk Monitoring daemon</td>
<td>1</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Inet daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Syslog daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Adaptive Services PIC daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>ECC parity errors Logging Daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>Layer 2 Tunneling Protocol daemon</td>
<td>0</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>PPPoE daemon</td>
<td>3</td>
<td>active</td>
</tr>
</tbody>
</table>
```
Redundancy device daemon | 0 active
PPP daemon | 0 active
Dynamic Flow Capture Daemon | 0 active

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>32776</td>
<td>Health Monitor: jroute daemon CPU utilization</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Routing protocol daemon</td>
<td>1 active</td>
</tr>
<tr>
<td>-</td>
<td>Management daemon</td>
<td>0 active</td>
</tr>
<tr>
<td>-</td>
<td>Command line interface</td>
<td>4 active</td>
</tr>
<tr>
<td>-</td>
<td>Periodic Packet Management daemon</td>
<td>0 active</td>
</tr>
<tr>
<td>-</td>
<td>Link Management daemon</td>
<td>0 active</td>
</tr>
<tr>
<td>-</td>
<td>Pragmatic General Multicast daemon</td>
<td>0 active</td>
</tr>
<tr>
<td>-</td>
<td>Bidirectional Forwarding Detection daemon</td>
<td>0 active</td>
</tr>
<tr>
<td>-</td>
<td>SRC daemon</td>
<td>0 active</td>
</tr>
<tr>
<td>-</td>
<td>audit daemon</td>
<td>0 active</td>
</tr>
<tr>
<td>-</td>
<td>Event daemon</td>
<td>0 active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>32777</td>
<td>Health Monitor: jcrypto daemon CPU utilization</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>IPSec Key Management daemon</td>
<td>0 active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>32779</td>
<td>Health Monitor: jkernel daemon Memory utilization</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Init daemon</td>
<td>47384 active</td>
</tr>
<tr>
<td>-</td>
<td>Chassis daemon</td>
<td>20204 active</td>
</tr>
<tr>
<td>-</td>
<td>Firewall daemon</td>
<td>1956 active</td>
</tr>
<tr>
<td>-</td>
<td>Interface daemon</td>
<td>3340 active</td>
</tr>
<tr>
<td>-</td>
<td>SNMP daemon</td>
<td>4540 active</td>
</tr>
<tr>
<td>-</td>
<td>MIB2 daemon</td>
<td>3880 active</td>
</tr>
<tr>
<td>-</td>
<td>Sonet APS daemon</td>
<td>2632 active</td>
</tr>
<tr>
<td>-</td>
<td>VRRP daemon</td>
<td>2672 active</td>
</tr>
<tr>
<td>-</td>
<td>Alarm daemon</td>
<td>1856 active</td>
</tr>
<tr>
<td>-</td>
<td>PFE daemon</td>
<td>2600 active</td>
</tr>
<tr>
<td>-</td>
<td>CRAFT daemon</td>
<td>2000 active</td>
</tr>
<tr>
<td>-</td>
<td>Traffic sampling control daemon</td>
<td>3164 active</td>
</tr>
<tr>
<td>-</td>
<td>Ilmi daemon</td>
<td>2132 active</td>
</tr>
<tr>
<td>-</td>
<td>Remote operations daemon</td>
<td>2964 active</td>
</tr>
<tr>
<td>-</td>
<td>CoS daemon</td>
<td>3044 active</td>
</tr>
<tr>
<td>-</td>
<td>Pic Services Logging daemon</td>
<td>1944 active</td>
</tr>
<tr>
<td>-</td>
<td>Internal Routing Service Daemon</td>
<td>1392 active</td>
</tr>
<tr>
<td>-</td>
<td>Network Access Service daemon</td>
<td>1992 active</td>
</tr>
<tr>
<td>-</td>
<td>Forwarding UDP daemon</td>
<td>1876 active</td>
</tr>
<tr>
<td>-</td>
<td>Routing socket proxy daemon</td>
<td>1296 active</td>
</tr>
<tr>
<td>-</td>
<td>Disk Monitoring daemon</td>
<td>1180 active</td>
</tr>
<tr>
<td>-</td>
<td>Inet daemon</td>
<td>1180 active</td>
</tr>
<tr>
<td>-</td>
<td>Syslog daemon</td>
<td>1296 active</td>
</tr>
<tr>
<td>-</td>
<td>Adaptive Services PIC daemon</td>
<td>3220 active</td>
</tr>
<tr>
<td>-</td>
<td>ECC parity errors logging Daemon</td>
<td>1100 active</td>
</tr>
<tr>
<td>-</td>
<td>Layer 2 Tunneling Protocol daemon</td>
<td>3372 active</td>
</tr>
<tr>
<td>-</td>
<td>PPPoE daemon</td>
<td>1424 active</td>
</tr>
<tr>
<td>-</td>
<td>Redundancy device daemon</td>
<td>1772 active</td>
</tr>
<tr>
<td>-</td>
<td>Dynamic Flow Capture Daemon</td>
<td>10740 active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>32780</td>
<td>Health Monitor: jroute daemon Memory utilization</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Routing protocol daemon</td>
<td>8104 active</td>
</tr>
<tr>
<td>-</td>
<td>Management daemon</td>
<td>13360 active</td>
</tr>
<tr>
<td>-</td>
<td>Command line interface</td>
<td>9912 active</td>
</tr>
<tr>
<td>-</td>
<td>Periodic Packet Management daemon</td>
<td>1484 active</td>
</tr>
<tr>
<td>-</td>
<td>Link Management daemon</td>
<td>2016 active</td>
</tr>
<tr>
<td>-</td>
<td>Pragmatic General Multicast daemon</td>
<td>1956 active</td>
</tr>
<tr>
<td>-</td>
<td>Bidirectional Forwarding Detection daemon</td>
<td>1956 active</td>
</tr>
<tr>
<td>-</td>
<td>SRC daemon</td>
<td>1772 active</td>
</tr>
</tbody>
</table>
audit daemon                                    1772 active
Event daemon                                    1808 active
32781 Health Monitor: jcrypto daemon Memory utilization 
IPSec Key Management daemon                     5600 active

user@host> show snmp health-monitor alarms detail

Alarm Index 32768:
Variable name                        jnxHrStoragePercentUsed.1
Variable OID                         1.3.6.1.4.1.2636.3.31.1.1.1.1.1
Sample type                          absolute value
Startup alarm                        rising alarm
Owner                                Health Monitor: root file system utilization
Creator                              Health Monitor
State                                active
Sample interval                  300 seconds
Rising threshold                  80
Falling threshold                 70
Rising event index             32768
Falling event index            32768
Instance Value: 58
Instance State: active

Alarm Index 32769:
Variable name                        jnxHrStoragePercentUsed.2
Variable OID                         1.3.6.1.4.1.2636.3.31.1.1.1.1.2
Sample type                          absolute value
Startup alarm                        rising alarm
Owner                                Health Monitor: /config file system utilization
Creator                              Health Monitor
State                                active
Sample interval                  300 seconds
Rising threshold                  80
Falling threshold                 70
Rising event index             32768
Falling event index            32768
Instance Value: 0
Instance State: active

Alarm Index 32770:
Variable name                        jnxOperatingCPU.9.1.0.0
Variable OID                         1.3.6.1.4.1.2636.3.1.13.1.8.9.1.0.0
Sample type                          absolute value
Startup alarm                        rising alarm
Owner                                Health Monitor: RE 0 CPU utilization
Creator                              Health Monitor
State                                active
Sample interval                  300 seconds
Rising threshold                  80
Falling threshold                 70
Rising event index             32768
Falling event index            32768
Instance Value: 0
Instance State: active
Alarm Index 32773:
Variable name: jnxOperatingBuffer.9.1.0.0
Variable OID: 1.3.6.1.4.1.2636.3.1.13.1.11.9.1.0.0
Sample type: absolute value
Startup alarm: rising alarm
Owner: Health Monitor: RE 0 Memory utilization

Creator: Health Monitor
State: active
Sample interval: 300 seconds
Rising threshold: 80
Falling threshold: 70
Rising event index: 32768
Falling event index: 32768
Instance Value: 35
Instance State: active

Alarm Index 32775:
Variable name: sysApplElmtRunCPU.3
Variable OID: 1.3.6.1.2.1.54.1.2.3.1.9.3
Sample type: delta value
Startup alarm: rising alarm
Owner: Health Monitor: jkernel daemon CPU utilization
Creator: Health Monitor
State: active
Sample interval: 300 seconds
Rising threshold: 24000
Falling threshold: 21000
Rising event index: 32768
Falling event index: 32768
Instance Name: sysApplElmtRunCPU.3.1.1
Instance Description: Init daemon
Instance Value: 0
Instance State: active

Instance Name: sysApplElmtRunCPU.3.2.7266
Instance Description: Chassis daemon
Instance Value: 50
Instance State: active

Instance Name: sysApplElmtRunCPU.3.3.2938
Instance Description: Firewall daemon
Instance Value: 0
Instance State: active

Instance Name: sysApplElmtRunCPU.3.4.2942
Instance Description: Interface daemon
Instance Value: 5
Instance State: active

Instance Name: sysApplElmtRunCPU.3.7.332
Instance Description: SNMP daemon
Instance Value: 11
Instance State: active

Instance Name: sysApplElmtRunCPU.3.9.2914
Instance Description: MIB2 daemon
Instance Value: 42
Instance State: active

Instance Name: sysApplElmtRunCPU.3.12.2916
Instance Description: Sonet APS daemon
Instance Value: 0
Instance State: active

Instance Name: sysApplElmtRunCPU.3.13.2917
Instance Description: VRRP daemon
Instance Value: 0
Instance State: active

Instance Name: sysApplElmtRunCPU.3.14.2787
Instance Description: Alarm daemon
Instance Value: 3
Instance State: active

Instance Name: sysApplElmtRunCPU.3.15.2940
Instance Description: PFE daemon
Instance Value: 0
Instance State: active

Instance Name: sysApplElmtRunCPU.3.16.2788
Instance Description: CRAFT daemon
Instance Value: 0
Instance State: active

Instance Name: sysApplElmtRunCPU.3.17.2918
Instance Description: Traffic sampling control daemon
---(more 23%)---
**show snmp inform-statistics**

**Syntax**

```
show snmp inform-statistics
```

**Release Information**

- Command introduced in Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display information about Simple Network Management Protocol (SNMP) inform requests.

**Options**

This command has no options.

**Required Privilege Level**

`view`

**List of Sample Output**

`show snmp inform-statistics` on page 3839

**Output Fields**

Table 449 on page 3839 describes the output fields for the `show snmp inform-statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 449: show snmp inform-statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Name</td>
<td>Name of the device configured to receive and respond to SNMP informs.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the target device.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of informs sent to the target device and acknowledged by the target device.</td>
</tr>
<tr>
<td>Pending</td>
<td>Number of informs held in memory pending a response from the target device.</td>
</tr>
<tr>
<td>Discarded</td>
<td>Number of informs discarded after the specified number of retransmissions to the target device were attempted.</td>
</tr>
<tr>
<td>Timeouts</td>
<td>Number of informs that did not receive an acknowledgement from the target device within the timeout specified.</td>
</tr>
<tr>
<td>Probe Failures</td>
<td>Connection failures that occurred (for example, when the target server returned invalid content or you incorrectly configured the target address).</td>
</tr>
</tbody>
</table>

**Sample Output**

```
user@host> show snmp inform-statistics
Inform Request Statistics:
   Target Name: TA1_v3_md5_none Address: 172.17.20.184
   Sent: 176, Pending: 0
   Discarded: 0, Timeouts: 0, Probe Failures: 0
   Target Name: TA2_v3_sha_none Address: 192.168.110.59
```

Copyright © 2013, Juniper Networks, Inc.
Sent: 0, Pending: 4
Discarded: 84, Timeouts: 0, Probe Failures: 258
Target Name: TA5_v2_none Address: 172.17.20.184
Sent: 0, Pending: 0
Discarded: 2, Timeouts: 10, Probe Failures: 0
show snmp mib

Syntax

show snmp mib (get | get-next | walk) (ascii | decimal) object-id

Release Information


Description

Display local Simple Network Management Protocol (SNMP) Management Information Base (MIB) object values.

Options

get—Retrieve and display one or more SNMP object values.

get-next—Retrieve and display the next SNMP object values.

walk—Retrieve and display the SNMP object values that are associated with the requested object identifier (OID). When you use this option, the Junos OS displays the objects below the subtree that you specify.

ascii—Display the SNMP object’s string indices as an ASCII-key representation.

decimal—Display the SNMP object values in the decimal (default) format. The decimal option is the default option for this command. Therefore, issuing the show snmp mib (get | get-next | walk) decimal object-id and the show snmp mib (get | get-next | walk) object-id commands display the same output.

object-id—The object can be represented by a sequence of dotted integers (such as 1.3.6.1.2.1.2) or by its subtree name (such as interfaces). When entering multiple objects, enclose the objects in quotation marks.

Required Privilege Level

snmp—To view this statement in the configuration.

List of Sample Output

show snmp mib get on page 3842
show snmp mib get (Multiple Objects) on page 3842
show snmp mib get (Layer 2 Policer) on page 3842
show snmp mib get-next on page 3842
show snmp mib get-next (Specify an OID) on page 3842
show snmp mib walk on page 3842
show snmp mib walk (QFX Series) on page 3842
show snmp mib walk decimal on page 3843
show snmp mib walk (ASCII) on page 3843
show snmp mib walk (Multiple Indices) on page 3843
show snmp mib walk decimal (Multiple Indices) on page 3843

Output Fields

Table 450 on page 3842 describes the output fields for the show snmp mib command. Output fields are listed in the approximate order in which they appear.
Table 450: show snmp mib Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>Object name and numeric instance value.</td>
</tr>
<tr>
<td><strong>object value</strong></td>
<td>Object value. The Junos OS translates OIDs into the corresponding object names.</td>
</tr>
</tbody>
</table>

Sample Output

**show snmp mib get**

```
user@host> show snmp mib get sysObjectID.0
sysObjectID.0 = jnxProductNameM20
```

**show snmp mib get (Multiple Objects)**

```
user@host> show snmp mib get ?sysObjectID.0 sysUpTime.0?
sysObjectID.0 = jnxProductNameM20
sysUpTime.0 = 1640992
```

**show snmp mib get (Layer 2 Policer)**

```
user@host> show snmp mib get ifInOctets.25970
ifInOctets.25970 = 7545720
```

**show snmp mib get-next**

```
user@host> show snmp mib get-next jnxMibs
jnxBoxClass.0 = jnxProductLineM20.0
```

**show snmp mib get-next (Specify an OID)**

```
user@host> show snmp mib get-next 1.3.6.1
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release: 2004-1 Build date: build date UTC Copyright (c) 1996-2004 Juniper Networks, Inc.
```

**show snmp mib walk**

```
user@host> show snmp mib walk system
sysDescr.0    = Juniper Networks, Inc. m20 internet router, kernel
Junos OS Release #0: 2004-1 Build date: build date UTC Copyright (c) 1996-2004 Juniper Networks, Inc.
sysObjectID.0 = jnxProductNameM20
sysUpTime.0   = 1640992
sysContact.0  = Your contact
sysName.0     = my router
sysLocation.0 = building 1
sysServices.0 = 4
```

**show snmp mib walk (QFX Series)**

```
user@switch> show snmp mib walk system
sysDescr.0    = Juniper Networks, Inc. qfx3500s internet router, kernel JUNOS 11.1-20100926.0 #0: 2010-09-26 06:17:38 UTC Build date: 2010-09-26 06:00:10
sysObjectID.0 = jnxProductQFX3500
sysUpTime.0   = 138980301
sysContact.0  = System Contact
```
sysName.0 = LabQFX3500
sysLocation.0 = Lab
sysServices.0 = 4

show snmp mib walk decimal

    user@host  show snmp mib walk decimal jnxUtilData
    jnxUtilCounter32Value.102.114.101.100 = 100

show snmp mib walk (ASCII)

    show snmp mib walk ascii jnxUtilData
    jnxUtilCounter32Value."fred" = 100

show snmp mib walk (Multiple Indices)

    show snmp mib walk ascii jnxFWCounterByteCount
    jnxFWCounterByteCount."fe-1/3/0.0-1"."CLASS_BE-fe-1/3/0.0-1".2 = 0
    jnxFWCounterByteCount."fe-1/3/0.0-1"."CLASS_CC-fe-1/3/0.0-1".2 = 0
    jnxFWCounterByteCount."fe-1/3/0.0-1"."CLASS_RT-fe-1/3/0.0-1".2 = 0

    .......

show snmp mib walk decimal (Multiple Indices)

    show snmp mib walk ascii jnxFWCounterByteCount
    jnxFWCounterByteCount."fe-1/3/0.0-1"."CLASS_BE-fe-1/3/0.0-1".2 = 0
    jnxFWCounterByteCount."fe-1/3/0.0-1"."CLASS_CC-fe-1/3/0.0-1".2 = 0
    jnxFWCounterByteCount."fe-1/3/0.0-1"."CLASS_RT-fe-1/3/0.0-1".2 = 0

    .......

show snmp rmon

Syntax
show snmp rmon
<alarms <brief | detail> | events <brief | detail> | logs>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display information about Simple Network Management Protocol (SNMP) Remote
Monitoring (RMON) alarms and events.

Options
none—Display information about all RMON alarms and events.
alarms—(Optional) Display information about RMON alarms.
brief | detail—(Optional) Display brief or detailed information about RMON alarms or
events.
events—(Optional) Display information about RMON events.
logs—(Optional) Display information about RMON monitoring logs.

Required Privilege
view

List of Sample Output
show snmp rmon on page 3846
show snmp rmon alarms detail on page 3846
show snmp rmon events detail on page 3847

Output Fields
Table 451 on page 3844 describes the output fields for the show snmp rmon command.
Output fields are listed in the approximate order in which they appear.

Table 451: show snmp rmon Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Index</td>
<td>Alarm identifier.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 451: show snmp rmon Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>State of the alarm or event entry:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td><strong>Alarms:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• active—Entry is fully configured and activated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• falling threshold crossed—Value of the variable has crossed the lower threshold limit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rising threshold crossed—Value of the variable has crossed the upper threshold limit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• under creation—Entry is being configured and is not yet activated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• startup—Alarm is waiting for the first sample of the monitored variable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• object not available—Monitored variable of that type is not available to the SNMP agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• instance not available—Monitored variable’s instance is not available to the SNMP agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• object type invalid—Monitored variable is not a numeric value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• object processing errored—An error occurred when the monitored variable was processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unknown—State is not one of the above.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Events:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• active—Entry has been fully configured and activated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• under creation—Entry is being configured and is not yet activated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• unknown—State is not one of the above.</td>
<td></td>
</tr>
<tr>
<td><strong>Variable name</strong></td>
<td>Name of the SNMP object instance being monitored.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Event Index</strong></td>
<td>Event identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of notification made when an event is triggered. It can be one of the following:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• log—A system log message is generated and an entry is made to the log table.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• snmptrap—An SNMP trap is sent to the configured destination.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• log and trap—A system log message is generated, an entry is made to the log table, and an SNMP trap is sent to the configured destination.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• none—Neither log nor trap will be sent.</td>
<td></td>
</tr>
<tr>
<td><strong>Last Event</strong></td>
<td>Date and time of the last event. It has the format yyyy-mm-dd hh:mm:ss timezone.</td>
<td>brief</td>
</tr>
<tr>
<td><strong>Community</strong></td>
<td>Identifies the trap group used for sending the SNMP trap.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Variable OID</strong></td>
<td>Object ID to which the variable name is resolved. The format is x.x.x.x.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Sample type</strong></td>
<td>Method of sampling the monitored variable and calculating the value to compare against the upper and lower thresholds. It can have the value of absolute value or delta value.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 451: show snmp rmon Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Startup alarm</strong></td>
<td>Alarm that might be sent when this entry is first activated, depending on the following criteria:</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>• Alarm is sent when one of the following situations exists:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is above or equal to the rising threshold and the startup type is either rising alarm or rising or falling alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is below or equal to the falling threshold and the startup type is either falling alarm or rising or falling alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Alarm is <em>not</em> sent when one of the following situations exists:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is above or equal to the rising threshold and the startup type is falling alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is below or equal to the falling threshold and the startup type is rising alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Value of the alarm is between the thresholds.</td>
<td></td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>Name of the entry configured by the user. If the entry was created through the CLI, the owner has monitor prepended to it.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Creator</strong></td>
<td>Mechanism by which the entry was configured (CLI or SNMP).</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Sample interval</strong></td>
<td>Time period between samples (in seconds).</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Rising threshold</strong></td>
<td>Upper limit threshold value configured by the user.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Falling threshold</strong></td>
<td>Lower limit threshold value configured by the user.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Rising event index</strong></td>
<td>Event triggered when the rising threshold is crossed.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Falling event index</strong></td>
<td>Event triggered when the falling threshold is crossed.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Current value</strong></td>
<td>Current value of the monitored variable in the most recent sample interval.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

```
show snmp rmon

user@host> show snmp rmon
Alarm
Index  State                        Variable name
  1  falling threshold crossed     ifInOctets.1

Event
Index  Type                        Last Event
  1  log and trap                   2002-01-30 01:13:01 PST
```

show snmp rmon alarms detail

```
user@host> show snmp rmon alarms detail
```
Alarm Index 1:
Variable name                         ifInOctets.1
Variable OID                          1.3.6.1.2.1.2.2.1.10.1
Sample type                           delta value
Startup alarm                         rising or falling alarm
Owner                                  monitor
Creator                                CLI
State                                  falling threshold crossed
Sample interval                       60 seconds
Rising threshold                      100000
Falling threshold                     80000
Rising event index                    1
Falling event index                   1
Current value                          0

show snmp rmon events detail

user@host> show snmp rmon events detail
Event Index 1:
Type                                  log and trap
Community                             boy-elroy
Last event                            2002-01-30 01:13:01 PST
Creator                               CLI
State                                  active
**show snmp rmon history**

**Syntax**

```
show snmp rmon history
  <history-index>
  <sample-index>
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display the contents of the RMON history group.

**Options**

- `none`—Display all the entries in the RMON history group.
- `history-index`—(Optional) Display the contents of the specified entry in the RMON history group.
- `sample-index`—(Optional) Display the statistics collected for the specified sample within the specified entry in the RMON history group.

**Required Privilege**

view

**Related Documentation**

- clear snmp rmon history on page 3823

**List of Sample Output**

- show snmp rmon history on page 3849
- show snmp rmon history 1 sample 15 on page 3850

**Output Fields**

Table 452 on page 3848 lists the output fields for the `show snmp rmon history` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Index</td>
<td>Identifies this RMON history entry within the RMON history group.</td>
</tr>
<tr>
<td>Owner</td>
<td>The entity that configured this entry. Range is 0 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the RMON history entry.</td>
</tr>
<tr>
<td>Interface or Data Source</td>
<td>The ifindex object that identifies the interface that is being monitored.</td>
</tr>
<tr>
<td>Interval</td>
<td>The interval (in seconds) configured for this RMON history entry.</td>
</tr>
<tr>
<td>Buckets Requested</td>
<td>The requested number of buckets (intervals) configured for this RMON history entry.</td>
</tr>
<tr>
<td>Buckets Granted</td>
<td>The number of buckets granted for this RMON history entry.</td>
</tr>
</tbody>
</table>
### Table 452: show snmp rmon history Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sample Index</strong></td>
<td>The sample statistics taken at the specified interval.</td>
</tr>
<tr>
<td><strong>Drop Events</strong></td>
<td>Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC’s RED mechanism.</td>
</tr>
<tr>
<td><strong>Octets</strong></td>
<td>Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type.</td>
</tr>
<tr>
<td><strong>Packets</strong></td>
<td>Total number of packets.</td>
</tr>
<tr>
<td><strong>Broadcast Packets</strong></td>
<td>Number of broadcast packets.</td>
</tr>
<tr>
<td><strong>Multicast Packets</strong></td>
<td>Number of multicast packets.</td>
</tr>
<tr>
<td><strong>CRC errors</strong></td>
<td>Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).</td>
</tr>
<tr>
<td><strong>Undersize Pkts</strong></td>
<td>Number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td><strong>Oversize Pkts</strong></td>
<td>Number of packets received during the sampling interval that were longer than 1518 octets (excluding framing bits, but including FCS octets) but were otherwise well formed.</td>
</tr>
<tr>
<td><strong>Fragments</strong></td>
<td>Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</td>
</tr>
<tr>
<td><strong>Jabbers</strong></td>
<td>Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms.</td>
</tr>
<tr>
<td><strong>Collisions</strong></td>
<td>Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug.</td>
</tr>
<tr>
<td><strong>Utilization(%)</strong></td>
<td>The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.</td>
</tr>
</tbody>
</table>

### Sample Output

```
show snmp rmon history 1

user@host> show snmp rmon history 1
History Index 1:
  Interface 171
  Requested Buckets 50
  Interval 10

Sample Index 1: Interval Start: Tue Feb 12 04:12:32 2008
  Drop Events 0
  Octets 486
  Packets 2
```
Broadcast Packet  0
Multicast Packets  2
CRC errors        0
Undersize Pkts    0
Oversize Pkts     0
Fragments         0
Jabbers           0
Collisions        0
Utilization(%)    0

Sample Index 2: Interval Start: Tue Feb 12 04:12:42 2008
Drop Events       0
Octets            486
Packets           2
Broadcast Packet  0
Multicast Packets 2
CRC errors        0
Undersize Pkts    0
Oversize Pkts     0
Fragments         0
Jabbers           0
Collisions        0
Utilization(%)    0

Sample Index 3: Interval Start: Tue Feb 12 04:12:52 2008
Drop Events       0
Octets            486
Packets           2
Broadcast Packet  0
Multicast Packets 2
CRC errors        0
Undersize Pkts    0
Oversize Pkts     0
Fragments         0
Jabbers           0
Collisions        0
Utilization(%)    0

show snmp rmon history 1 sample 15
user@host> show snmp rmon history 1 sample 15
Index 1
Owner    = monitor
Status    = valid
Data Source  = ifIndex.17
Interval   = 1800
Buckets Requested = 50
Buckets Granted = 50

Sample Index 44: Interval Start: Thu Jan  1 00:08:35 1970
Drop Events   = 0
Octets        = 0
Packets       = 0
Broadcast Pkts = 0
Multicast Pkts = 0
CRC Errors    = 0
Undersize Pkts = 0
Oversize Pkts = 0
Fragments     = 0
Jabbers       = 0
Collisions = 0
Utilization (%) = 0
**show snmp statistics**

**Syntax**
```
show snmp statistics
```

**Release Information**
Command introduced before Junos OS Release 7.4.  
Command introduced in Junos OS Release 9.0 for EX Series switches.  
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Display statistics about Simple Network Management Protocol (SNMP) packets sent and received by the router or switch.

**Options**
This command has no options.

**Required Privilege Level**
```
view
```

**Related Documentation**
- clear snmp statistics on page 3824

**List of Sample Output**
```
show snmp statistics on page 3855
```

**Output Fields**
Table 453 on page 3852 describes the output fields for the `show snmp statistics` command.  
Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Packets (snmpInPkts)</strong></td>
<td>Total number of messages delivered to the SNMP entity from the transport service.</td>
</tr>
<tr>
<td><strong>Bad versions</strong></td>
<td>(snmpInBadVersions) Total number of messages delivered to the SNMP entity that were for an unsupported SNMP version.</td>
</tr>
<tr>
<td><strong>Bad community names</strong></td>
<td>(snmpInBadCommunityNames) Total number of messages delivered to the SNMP entity that used an SNMP community name not known to the entity.</td>
</tr>
<tr>
<td><strong>Bad community uses</strong></td>
<td>(snmpInBadCommunityUses) Total number of messages delivered to the SNMP entity that represented an SNMP operation that was not allowed by the SNMP community named in the message.</td>
</tr>
<tr>
<td><strong>ASN parse errors</strong></td>
<td>(snmpInASNParseErrs) Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.</td>
</tr>
<tr>
<td><strong>Too big</strong></td>
<td>(snmpInTooBigs) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of tooBig.</td>
</tr>
<tr>
<td><strong>No such names</strong></td>
<td>(snmpInNoSuchNames) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of noSuchName.</td>
</tr>
<tr>
<td><strong>Bad values</strong></td>
<td>(snmpInBadValues) Total number of SNMP PDUs delivered to the SNMP entity with an error status field of badValue.</td>
</tr>
<tr>
<td><strong>Read only</strong></td>
<td>(snmpInReadOnlys) Total number of valid SNMP PDUs delivered to the SNMP entity with an error status field of readOnly. Only incorrect implementations of SNMP generate this error.</td>
</tr>
</tbody>
</table>
Table 453: show snmp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input (continued)</strong></td>
<td></td>
</tr>
<tr>
<td>General errors—(snmpInGenErrs)</td>
<td>Total number of SNMP PDUs delivered to the SNMP entity with an error status field of genErr.</td>
</tr>
<tr>
<td>Total requests varbinds—(snmpInTotalReqVars)</td>
<td>Total number of MIB objects retrieved successfully by the SNMP entity as a result of receiving valid SNMP GetRequest and GetNext PDUs.</td>
</tr>
<tr>
<td>Total set varbinds—(snmpInSetVars)</td>
<td>Total number of MIB objects modified successfully by the SNMP entity as a result of receiving valid SNMP SetRequest PDUs.</td>
</tr>
<tr>
<td>Get requests—(snmpInGetRequests)</td>
<td>Total number of SNMP GetRequest PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Get nexts—(snmpInGetNexts)</td>
<td>Total number of SNMP GetNext PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Set requests—(snmpInSetRequests)</td>
<td>Total number of SNMP SetRequest PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Get responses—(snmpInGetResponses)</td>
<td>Total number of SNMP GetResponse PDUs that have been accepted and processed by the SNMP entity.</td>
</tr>
<tr>
<td>Traps—(snmpInTraps)</td>
<td>Total number of SNMP traps generated by the SNMP entity.</td>
</tr>
<tr>
<td>Silent drops—(snmpSilentDrops)</td>
<td>Total number of GetRequest, GetNextRequest, GetBulkRequest, SetRequests, and InformRequest PDUs delivered to the SNMP entity that were silently dropped because the size of a reply containing an alternate response PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the requests.</td>
</tr>
<tr>
<td>Proxy drops—(snmpProxyDrops)</td>
<td>Total number of GetRequest, GetNextRequest, GetBulkRequest, SetRequests, and InformRequest PDUs delivered to the SNMP entity that were silently dropped because the transmission of the message to a proxy target failed in such a way (other than a timeout) that no response PDU could be returned.</td>
</tr>
<tr>
<td>Commit pending drops</td>
<td>Number of SNMP packets for Set requests dropped because of a previous pending SNMP Set request on the committed configuration.</td>
</tr>
<tr>
<td>Throttle drops</td>
<td>Number of SNMP packets for any requests dropped reaching the throttle limit.</td>
</tr>
</tbody>
</table>
Table 453: show snmp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V3 Input</td>
<td>Information about SNMP version 3 packets:</td>
</tr>
<tr>
<td></td>
<td>• Unknown security models—(snmpUnknownSecurityModels) Total number of packets received by the SNMP engine that were dropped because they referenced a security model that was not known to or supported by the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• Invalid messages—(snmpInvalidMsgs) Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message.</td>
</tr>
<tr>
<td></td>
<td>• Unknown pdu handlers—(snmpUnknownPDUHandlers) Number of packets received by the SNMP engine that were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the PDU type.</td>
</tr>
<tr>
<td></td>
<td>• Unavailable contexts—(snmpUnavailableContexts) Number of requests received for a context that is known to the SNMP engine, but is currently unavailable.</td>
</tr>
<tr>
<td></td>
<td>• Unknown contexts—(snmpUnknownContexts) Total number of requests received for a context that is unknown to the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• Unsupported security levels—(usmStatsUnsupportedSecLevels) Total number of packets received by the SNMP engine that were dropped because they requested a security level unknown to the SNMP engine (or otherwise unavailable).</td>
</tr>
<tr>
<td></td>
<td>• Not in time windows—(usmStatsNotInTimeWindows) Total number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine’s window.</td>
</tr>
<tr>
<td></td>
<td>• Unknown user names—(usmStatsUnknownUserNames) Total number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• Unknown engine ids—(usmStatsUnknownEngineIDs) Total number of packets received by the SNMP engine that were dropped because they referenced an SNMP engine ID that was not known to the SNMP engine.</td>
</tr>
<tr>
<td></td>
<td>• Wrong digests—(usmStatsWrongDigests) Total number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value.</td>
</tr>
<tr>
<td></td>
<td>• Decryption errors—(usmStatsDecryptionErrors) Total number of packets received by the SNMP engine that were dropped because they could not be decrypted.</td>
</tr>
</tbody>
</table>
Table 453: show snmp statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>Information about transmitted packets:</td>
</tr>
<tr>
<td>Packets—(snmpOutPkts)</td>
<td>Total number of messages passed from the SNMP entity to the transport service.</td>
</tr>
<tr>
<td>Too bigs—(snmpOutTooBigs)</td>
<td>Total number of SNMP PDUs generated by the SNMP entity with an error status field of tooBig.</td>
</tr>
<tr>
<td>No such names—(snmpOutNoSuchNames)</td>
<td>Total number of SNMP PDUs delivered to the SNMP entity with an error status field of noSuchName.</td>
</tr>
<tr>
<td>Bad values—(snmpOutBadValues)</td>
<td>Total number of SNMP PDUs generated by the SNMP entity with an error status field of badValue.</td>
</tr>
<tr>
<td>General errors—(snmpOutGenErrs)</td>
<td>Total number of SNMP PDUs generated by the SNMP entity with an error status field of genErr.</td>
</tr>
<tr>
<td>Get requests—(snmpOutGetRequests)</td>
<td>Total number of SNMP GetRequest PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td>Get nexts—(snmpOutGetNexts)</td>
<td>Total number of SNMP GetNext PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td>Set requests—(snmpOutSetRequests)</td>
<td>Total number of SNMP SetRequest PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td>Get responses—(snmpOutGetResponses)</td>
<td>Total number of SNMP GetResponse PDUs generated by the SNMP entity.</td>
</tr>
<tr>
<td>Traps—(snmpOutTraps)</td>
<td>Total number of SNMP traps generated by the SNMP entity.</td>
</tr>
</tbody>
</table>

Sample Output

show snmp statistics

user@host> show snmp statistics
SNMP statistics:
  Input:
    Packets: 246213, Bad versions: 12, Bad community names: 12, Bad community uses: 0, ASN parse errors: 96, Too bigs: 0, No such names: 0, Bad values: 0, Read onlys: 0, General errors: 0, Total request varbinds: 227084, Total set varbinds: 67, Get requests: 44942, Get nexts: 190371, Set requests: 10712, Get responses: 0, Traps: 0, Silent drops: 0, Proxy drops: 0, Commit pending drops: 0, Throttle drops: 0, V3 Input:
    Unknown security models: 0, Invalid messages: 0 Unknown pdu handlers: 0, Unavailable contexts: 0 Unknown contexts: 0, Unsupported security levels: 1 Not in time windows: 0, Unknown user names: 0 Unknown engine ids: 44, Wrong digests: 23, Decryption errors: 0 Output:
    Packets: 246093, Too bigs: 0, No such names: 31561, Bad values: 0, General errors: 2, Get requests: 0, Get nexts: 0, Set requests: 0, Get responses: 246025, Traps: 0
show snmp v3

Syntax

show snmp v3
  <access <brief | detail> | community | general | groups | notify <filter> | target <address | parameters> | users>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display the Simple Network Management Protocol version 3 (SNMPv3) operating configuration.

Options
none—Display all of the SNMPv3 operating configuration.

access—(Optional) Display SNMPv3 access information.

brief | detail—(Optional) Display brief or detailed information about SNMPv3 access information.

community—(Optional) Display SNMPv3 community information.

general—(Optional) Display SNMPv3 general information.

groups—(Optional) Display SNMPv3 security-to-group information.

notify <filter>—(Optional) Display SNMPv3 notify and, optionally, notify filter information.

target <address | parameters>—(Optional) Display SNMPv3 target and, optionally, either target address or target parameter information.

users—(Optional) Display SNMPv3 user information.

Additional Information
To edit the default display of the show snmp v3 command, specify options in the show statement at the [editsnmpv3] hierarchy level.

Required Privilege Level
view

List of Sample Output
show snmp v3 on page 3858

Output Fields
Table 454 on page 3857 describes the output fields for the show snmp v3 command. Output fields are listed in the approximate order in which they appear.
Table 454: show snmp v3 Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>Information about access control:</td>
</tr>
<tr>
<td>Group</td>
<td>Group name for which the configured access privileges apply. The group, together with the context prefix and the security model and security level, forms the index for this table.</td>
</tr>
<tr>
<td>Context prefix</td>
<td>SNMPv3 context for which the configured access privileges apply.</td>
</tr>
<tr>
<td>Security model/level</td>
<td>Security model and security level for which the configuration access privileges apply.</td>
</tr>
<tr>
<td>Read view</td>
<td>Identifies the MIB view applied to SNMPv3 read operations.</td>
</tr>
<tr>
<td>Write view</td>
<td>Identifies the MIB view applied to SNMPv3 write operations.</td>
</tr>
<tr>
<td>Notify view</td>
<td>Identifies the MIB view applied to outbound SNMP notifications.</td>
</tr>
<tr>
<td>Engine</td>
<td>Information about local engine configuration:</td>
</tr>
<tr>
<td>Local engine ID</td>
<td>Identifier that uniquely and unambiguously identifies the local SNMPv3 engine.</td>
</tr>
<tr>
<td>Engine boots</td>
<td>Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed.</td>
</tr>
<tr>
<td>Engine time</td>
<td>Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized.</td>
</tr>
<tr>
<td>Max msg size</td>
<td>Maximum message size the sender can accommodate.</td>
</tr>
<tr>
<td>Engine ID</td>
<td>Information about engine ID:</td>
</tr>
<tr>
<td>Local engine ID</td>
<td>Identifier that uniquely and unambiguously identifies the local SNMPv3 engine.</td>
</tr>
<tr>
<td>Engine boots</td>
<td>Number of times the local SNMPv3 engine has rebooted or reinitialized since the engine ID was last changed.</td>
</tr>
<tr>
<td>Engine time</td>
<td>Number of seconds since the local SNMPv3 engine was last rebooted or reinitialized.</td>
</tr>
<tr>
<td>Max msg size</td>
<td>Maximum message size the sender can accommodate.</td>
</tr>
<tr>
<td>User</td>
<td>SNMPv3 user.</td>
</tr>
<tr>
<td>Auth/Priv</td>
<td>Authentication and encryption algorithm available for use by each user.</td>
</tr>
<tr>
<td>Storage</td>
<td>Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the conceptual row. Only rows with an active status are used by the SNMPv3 engine.</td>
</tr>
<tr>
<td>Group name</td>
<td>Name of the group to which this entry belongs.</td>
</tr>
<tr>
<td>Security model</td>
<td>Identifies the security model context for the security name.</td>
</tr>
<tr>
<td>Security name</td>
<td>Used with the security model; identifies a specific security name instance. Each security model/security name combination can be assigned to a specific group.</td>
</tr>
<tr>
<td>Storage type</td>
<td>Indicates whether a user is saved to the configuration file (nonvolatile) or not (volatile). Applies only to users with active status.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the conceptual row. Only rows with active status are used by the SNMPv3 engine.</td>
</tr>
</tbody>
</table>
### Sample Output

**show snmp v3**

```
user@host> show snmp v3
Local engine ID: 80 00 0a 4c e04 31 32 33 34
Engine boots: 38
Engine time: 64583 seconds
Max msg size: 2048 bytes

Engine ID: local
<table>
<thead>
<tr>
<th>User</th>
<th>Auth/Priv</th>
<th>Storage</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>user1</td>
<td>md5/des</td>
<td>nonvolatile</td>
<td>active</td>
</tr>
<tr>
<td>user2</td>
<td>sha/none</td>
<td>nonvolatile</td>
<td>active</td>
</tr>
<tr>
<td>user3</td>
<td>none/none</td>
<td>nonvolatile</td>
<td>active</td>
</tr>
</tbody>
</table>

Engine ID: 81 00 0a 4c 04 64 64 64 64
<table>
<thead>
<tr>
<th>User</th>
<th>Auth/Priv</th>
<th>Storage</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNEW</td>
<td>md5/none</td>
<td>nonvolatile</td>
<td>active</td>
</tr>
</tbody>
</table>

Group name        Security model     Security name  Storage type   Status
---                ---                 ---                ---                 ---
g1                 usm                 user1             nonvolatile       active
g2                 usm                 user2             nonvolatile       active
g3                 usm                 user3             nonvolatile       active

Access control:

<table>
<thead>
<tr>
<th>Group</th>
<th>Context prefix</th>
<th>Security model/level</th>
<th>Read view</th>
<th>Write view</th>
<th>Notify view</th>
</tr>
</thead>
</table>
g1     |                | usm/privacy           | v1        | v1         | v1          |
g2     |                | usm/authent          | v1        | v1         | v1          |
g3     |                | usm/none             | v1        | v1         | v1          |
```

### Operational Commands: Analyzers and Port Mirroring
### show forwarding-options port-mirroring

#### Syntax

```
show forwarding-options port-mirroring
<terse | detail>
<instance-name>
```

#### Release Information

Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

#### Description

Display current state of port-mirroring instances.

#### Options

- `terse | detail`—(Optional) Display the specified level of output.
- `instance-name`—(Optional) Display a single port-mirroring instance.

#### Required Privilege

- Level: `view`

#### Related Documentation

- [edit forwarding-options port-mirroring] Hierarchy Level on page 3700

#### List of Sample Output

- show forwarding-options port-mirroring terse on page 3860
- show forwarding-options port-mirroring detail on page 3860

#### Output Fields

Table 455 on page 3859 lists the output fields for the `show forwarding-options port-mirroring` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Name</td>
<td>Name of port-mirroring instance.</td>
<td>All levels</td>
</tr>
<tr>
<td>Instance Id</td>
<td>Instance identification number.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>Instance state, either <code>up</code> or <code>down</code>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Rate</td>
<td>Rate (ratio of packets sampled).</td>
<td>detail</td>
</tr>
<tr>
<td>Run-length</td>
<td>Run length (number of consecutive packets sampled).</td>
<td>detail</td>
</tr>
<tr>
<td>Maximum-packet-length</td>
<td>Maximum packet length.</td>
<td>detail</td>
</tr>
<tr>
<td>Family</td>
<td>Protocol family.</td>
<td>detail</td>
</tr>
<tr>
<td>State</td>
<td>Instance state, either <code>up</code> or <code>down</code>.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 455: show forwarding-options port-mirroring Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination (next-hop group name).</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show forwarding-options port-mirroring terse

```bash
user@switch> show forwarding-options port-mirroring terse
Instance Name: &global_instance
Instance Id: 1      State: up
inst1         2      up
```

show forwarding-options port-mirroring detail

```bash
user@switch> show forwarding-options port-mirroring detail
Instance Name: &global_instance
Instance Id: 1      State: up
Input parameters:
  Rate:      1
  Run-length:     0
  Maximum-packet-length: 0
Output parameters:
  Family: ethernet-switching  State: up     Destination: ge-0/0/10.0

Instance Name: inst1
Instance Id: 2      State: up
Input parameters:
  Rate:      1
  Run-length:     0
  Maximum-packet-length: 0
Output parameters:
  Family: ethernet-switching  State: down   Destination: ge-0/0/10.0
```
**show forwarding-options analyzer**

**Syntax**

```
show forwarding-options analyzer analyzer-name
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level [edit forwarding-options] introduced in Junos OS Release T3.2X50-D10 (ELS).

**Description**

Display information about analyzers configured for mirroring.

**Options**

`analyzer-name`—(Optional) Displays the status of a specific analyzer on the switch.

**Required Privilege Level**

view

**Related Documentation**

- Understanding Port Mirroring and Analyzers on EX4300 Switches on page 3544

**List of Sample Output**

`show forwarding-options analyzer` on page 3861

**Output Fields**

Table 456 on page 3861 lists the output fields for the `show forwarding-options analyzer` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzer name</td>
<td>Displays the name of the analyzer.</td>
</tr>
<tr>
<td>Output interface</td>
<td>Specifies a local interface to which mirrored packets are sent. An analyzer can</td>
</tr>
<tr>
<td></td>
<td>have output to either an interface or a VLAN, not both.</td>
</tr>
<tr>
<td>Output VLAN</td>
<td>Specifies a VLAN to which mirrored packets are sent. An analyzer can have output</td>
</tr>
<tr>
<td></td>
<td>to either an interface or a VLAN, not both.</td>
</tr>
<tr>
<td>Mirror ratio</td>
<td>Displays the ratio of packets to be mirrored.</td>
</tr>
<tr>
<td>Egress monitored interfaces</td>
<td>Displays interfaces for which traffic exiting the interfaces is mirrored.</td>
</tr>
<tr>
<td>Ingress monitored interfaces</td>
<td>Displays interfaces for which traffic entering the interfaces is mirrored.</td>
</tr>
<tr>
<td>Ingress monitored VLANs</td>
<td>Displays VLANs for which traffic entering the VLAN is mirrored.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
user@switch> show forwarding-options analyzer
Analyzer name : employee-monitor
    Mirror rate : 1
    Maximum packet length : 0
    State : up
```
Ingress monitored interfaces : ge-0/0/0.0
Ingress monitored interfaces : ge-0/0/1.0
Output VLAN : default-switch/remote-analyzer

**Operational Commands: sFlow**
show sflow

Syntax

```
show sflow
  <collector>
  <interface>
```

Release Information
Command introduced in Junos OS Release 9.3 for EX Series switches.

Description
Display default sFlow technology configuration information.

Options

- **none**—Display default sFlow technology configuration information.
- **collector**—(Optional) Display standard status information about the specified sFlow collector.
- **interface**—(Optional) Display standard status information about the specified sFlow interface.

Required Privilege
view

Related Documentation
- show sflow interface on page 3865
- show sflow collector on page 3867
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603

List of Sample Output
show sflow on page 3864

Output Fields
Table 457 on page 3863 lists the output fields for the `show sflow` command. Output fields are listed in the approximate order in which they appear.

Table 457: show sflow Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>sFlow</td>
<td>Status of the feature: <strong>enabled</strong> or <strong>disabled</strong>.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sample rate egress</td>
<td>Rate at which egress packets are sampled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sample rate ingress</td>
<td>Rate at which ingress packets are sampled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sample limit</td>
<td>Number of packets sampled per second. The sample limit cannot be configured and is set to 300 packets/second.</td>
<td>All levels</td>
</tr>
<tr>
<td>Polling interval</td>
<td>Interval at which the sFlow agent polls the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>Agent ID</td>
<td>The IP address assigned to the sFlow agent.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Sample Output

show sflow

sFlow : Enabled
Sample rate egress : 1:1000
Sample rate ingress : 1:2048: Disabled
Sample limit : 300 packets/second
Polling interval : 20 seconds
Agent ID : 10.93.54.7
Source IP address : 10.93.54.7
show sflow interface

**Syntax**
show sflow interface

**Release Information**
Command introduced in Junos OS Release 9.3 for EX Series switches.

**Description**
Display the interfaces on which sFlow technology is enabled and the sampling parameters.

**Required Privilege Level**
view

**Related Documentation**
- show sflow on page 3863
- show sflow collector on page 3867
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603

**List of Sample Output**
show sflow interface on page 3865

**Output Fields**
Table 458 on page 3865 lists the output fields for the `show sflow interface` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interfaces on which sFlow technology is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Status Egress</td>
<td>Indicates whether egress sample rate is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Status Ingress</td>
<td>Indicates whether ingress sample rate is enabled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sample rate Egress</td>
<td>Rate at which egress packets are sampled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sample rate Ingress</td>
<td>Rate at which ingress packets are sampled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Adapted sample rate Egress</td>
<td>Adapted rate at which egress packets are sampled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Adapted sample rate Ingress</td>
<td>Adapted rate at which ingress packets are sampled.</td>
<td>All levels</td>
</tr>
<tr>
<td>Polling-interval</td>
<td>The interval at which the sFlow agent polls the interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

**Sample Output**
show sflow interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Sample rate</th>
<th>Adapted sample rate</th>
<th>Polling-interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Ingress</td>
<td>Egress Ingress</td>
<td>Egress Ingress</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>---------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ge-0/0/0.0</td>
<td>Enabled</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>2048</td>
<td>1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2048</td>
<td>1000</td>
<td>2048</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
show sflow collector

Syntax  
show sflow collector

Release Information  
Command introduced in Junos OS Release 9.3 for EX Series switches.

Description  
Displays a list of configured sFlow collectors and their properties.

Required Privilege  
view

Related Documentation  
- show sflow on page 3863
- show sflow interface on page 3865
- Example: Configuring sFlow Technology to Monitor Network Traffic on EX Series Switches on page 3559
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603

List of Sample Output  
show sflow collector on page 3867

Output Fields  
Table 459 on page 3867 lists the output fields for the show sflow collector command. Output fields are listed in the approximate order in which they appear.

Table 459: show sflow collector Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the collector.</td>
<td>All levels</td>
</tr>
<tr>
<td>UDP port</td>
<td>UDP port number.</td>
<td>All levels</td>
</tr>
<tr>
<td>No of samples</td>
<td>Packet sampling rate.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show sflow collector

<table>
<thead>
<tr>
<th>IP-address</th>
<th>UDP-Port</th>
<th>No of samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.204.32.46</td>
<td>5600</td>
<td>1000</td>
</tr>
<tr>
<td>100.204.32.76</td>
<td>3400</td>
<td>1000</td>
</tr>
</tbody>
</table>
clear sflow collectors statistics

**Syntax**

```
clear sflow collectors statistics
```

**Release Information**

Command introduced in JUNOS Release 9.5 for EX Series switches.

**Description**

Clear the sFlow collector's statistics.

**Required Privilege**

**Level**

clear

**Related Documentation**

- show sflow collector on page 3867
- Configuring sFlow Technology for Network Monitoring (CLI Procedure) on page 3603

**Sample Output**

```
clear sflow collectors statistics
```

**Operational Commands: Ethernet OAM Connectivity Fault Management**
clear oam ethernet connectivity-fault-management delay-statistics

Syntax

```
clear oam ethernet connectivity-fault-management delay-statistics
maintenance-association maintenance-association-name
maintenance-domain maintenance-domain-name
<logical-system logical-system-name>
<one-way>
<two-way>
```

Release Information

- Command introduced in Junos OS Release 11.4 for EX Series switches.

Description

On MX Series routers and EX Series switches, clear ITU-T Y.1731 Ethernet frame delay measurement (ETH-DM) delay statistics and ETH-DM frame counts.

Options

- **maintenance-association maintenance-association-name**—Clear ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance association.
- **maintenance-domain maintenance-domain-name**—Clear ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance domain.
- **logical-system logical-system-name**—(MX Series routers only) (Optional) Clear ETH-DM delay statistics and ETH-DM frame counts for the specified logical system.
- **one-way**—(Optional) Clear one-way ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance association, maintenance domain, or (on the routers only) logical system.
- **two-way**—(Optional) Clear two-way ETH-DM delay statistics and ETH-DM frame counts for the specified maintenance association, maintenance domain, or (on the routers only) logical system.

Required Privilege Level

`view`

Related Documentation

- `clear oam ethernet connectivity-fault-management statistics`
- `show oam ethernet connectivity-fault-management delay-statistics on page 3878`
- `show oam ethernet connectivity-fault-management interfaces`

List of Sample Output

`clear oam ethernet connectivity-fault-management delay-statistics on page 3869`

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear oam ethernet connectivity-fault-management delay statistics

```
user@switch> clear oam ethernet connectivity-fault-management delay-statistics maintenance-domain md1 maintenance-association ma1
```
Delay statistics entries cleared
clear oam ethernet connectivity-fault-management sla-iterator-statistics

Syntax

```
clear oam ethernet connectivity-fault-management sla-iterator-statistics
maintenance-association maintenance-association-name
maintenance-domain maintenance-domain-name
<local-mep local-mep-id>
<remote-mep remote-mep-id>
sla-iterator sla-iterator
```

Release Information

Command introduced in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 13.2 for MX Series routers.

Description

Clear Ethernet Operation, Administration, and Maintenance (OAM) service-level agreement (SLA) iterator statistics. For MX Series routers, clear the SLA iterator statistics and proactive Ethernet synthetic loss measurement (ETH-SLM) statistics.

Options

```
maintenance-association maintenance-association-name—Name of the maintenance association.
maintenance-domain maintenance-domain-name—Name of the maintenance domain.
local-mep local-mep-id—(Optional) Identifier of the local MEP.
remote-mep remote-mep-id—(Optional) Identifier of the remote MEP.
sla-iterator sla-iterator—Name of the SLA iterator profile.
```

Required Privilege

`view`

Related Documentation

- Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621
- `show oam ethernet connectivity-fault-management sla-iterator-statistics` on page 3902

List of Sample Output

```
clear oam ethernet connectivity-fault-management sla-iterator-statistics on page 3871
```

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear oam ethernet connectivity-fault-management sla-iterator-statistics
user@switch> clear oam ethernet connectivity-fault-management sla-iterator-statistics
maintenance-domain md1 maintenance-association ma1 local-mep 1 remote-mep 2 sla-iterator

Iterator statistics entries cleared
```
clear oam ethernet connectivity-fault-management statistics

Syntax

```
clear oam ethernet connectivity-fault-management statistics
   <interface ethernet-interface-name>
   <level md-level>
```

Release Information
Command introduced in Junos OS Release 10.2 for EX Series switches.

Description
Clear all statistics maintained by CFM.

Options
```
interface ethernet-interface-name — (Optional) Clear CFM statistics only for MEPs attached to the specified Ethernet physical interface.

level level — (Optional) Clear CFM statistics only for MEPs within CFM maintenance domains (MDs) of the specified level.
```

Required Privilege Level
clear

Related Documentation
- show oam ethernet connectivity-fault-management interfaces on page 3886
- show oam ethernet connectivity-fault-management path-database on page 3892
- show oam ethernet connectivity-fault-management mip on page 3901

List of Sample Output
clear oam ethernet connectivity-fault-management statistics on page 3872

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output
clear oam ethernet connectivity-fault-management statistics

```
user@host> clear oam ethernet connectivity-fault-management statistics
Cleared statistics of all CFM sessions
```
monitor ethernet delay-measurement

Syntax

monitorethernetdelay-measurement maintenance-domain md-name
maintenance-association ma-name (one-way | two-way) (remote-mac-address | mep remote-mep-id) <count count> <no-session-id-tlv> <priority 802.1p value> <size size> <wait time>

Release Information

Command introduced in Junos OS Release 11.4 for EX Series switches.

Description

Start an ITU-T Y.1731 Ethernet frame delay measurement session between the specified local connectivity fault management (CFM) maintenance association end point (MEP) and the specified remote MEP, and display a summary of the frames exchanged in the measurement session. Frame delay measurement statistics are stored at one of the MEPs for later retrieval.

NOTE: If you attempt to monitor delays to a nonexistent MAC address, you must type Ctrl +C to explicitly quit the monitorethernetdelay-measurement command and return to the CLI command prompt.

To start an Ethernet frame delay measurement session, the switch initiates an exchange of frames carrying one-way or two-way frame delay measurement protocol data units (PDUs) between the local and remote MEPs. The frame counts—the types of and number of Ethernet frame delay measurement PDU frames exchanged to measure frame delay times—are displayed as the run-time output of the monitorethernetdelay-measurement command and are also stored at both the initiator and receiver MEPs for later retrieval. Ethernet frame delay measurement statistics, described below, are measured and stored at only one of the MEPs:

- **Frame delay**—The difference, in microseconds, between the time a frame is sent and when it is received.

- **Frame delay variation**—The difference, in microseconds, between consecutive frame delay values. Frame delay variation is sometimes called “frame jitter.”

For one-way Ethernet frame delay measurement, only the receiver MEP (on the remote system) collects statistics. For two-way Ethernet frame delay measurement, only the initiator MEP (on the local system) collects statistics.

Options

- **count count**—(Optional) Number of frames to send to the specified peer MEP. The range of values is 1 through 65,535 frames. The default value is 10 frames.

- **maintenance-association ma-name**—Name of an existing CFM maintenance association.

- **maintenance-domain md-name**—Name of an existing CFM maintenance domain.

- **mep remote-mep-id**—Numeric identifier of the peer MEP with which to perform Ethernet frame delay measurement. The discovered MAC address of the peer MEP is used. The range of values is 1 through 8191.
no-session-id-tlv—(Optional) Prevent insertion of the session ID TLV in the request frame.

one-way—Measurement type is one-way Ethernet frame delay measurement, which is based on the difference between the time at which the initiator MEP sends a one-way delay measurement request (IDM) frame and the time at which the receiver MEP receives the frame.

priority 802.1p value—(Optional) Priority of the delay measurement request frame supported by both one-way delay measurement and two-way delay measurement. The range of values is from 0 through 7. The default value is zero.

remote-mac-address—Unicast MAC address of the peer MEP with which to perform Ethernet frame delay measurement. Specify the MAC address as six hexadecimal bytes in nn:nn:nn:nn:nn:nn format. Multicast MAC addresses are not supported.

size size—(Optional) Size of the data TLV to be included in the request frame. The range of values is from 1 through 1400 bytes.

two-way—Measurement type is two-way Ethernet frame delay measurement, which is based on the difference between the time at which the initiator MEP sends a two-way delay measurement message (DMM) frame and the time at which the initiator MEP receives an associated two-way delay measurement reply (DMR) frame from the responder MEP, subtracting the time elapsed at the responder MEP.

wait time—(Optional) Number of seconds to wait between sending frames. The range of values is from 1 through 255 seconds. The default value is 1 second.

Required Privilege Level

trace and maintenance

Related Documentation

• Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621
• show oam ethernet connectivity-fault-management mep-database on page 3895
• show oam ethernet connectivity-fault-management mep-statistics
• show oam ethernet connectivity-fault-management delay-statistics on page 3878
• clear oam ethernet connectivity-fault-management statistics on page 3872

List of Sample Output

monitor ethernet delay-measurement one-way on page 3876
monitor ethernet delay-measurement two-way on page 3876
monitor ethernet delay-measurement two-way (Invalid DMR Frames Received) on page 3876

Output Fields

The monitor ethernet delay-measurement command displays different output at the CLI, depending on whether you start a one-way or two-way frame delay measurement:

• Table 460 on page 3875 lists the run-time output fields for the monitor ethernet delay-measurement one-way command.
• Table 461 on page 3875 lists the run-time output fields for the monitor ethernet delay-measurement two-way command.
Output fields are listed in the approximate order in which they appear.

### Table 460: monitor ethernet delay-measurement one-way Output Fields

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Output Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-way ETH-DM request to</td>
<td>Unicast MAC address of the remote peer MEP.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.</td>
</tr>
<tr>
<td>1DM Frames sent</td>
<td>PDU frames sent to the remote MEP in this ETH-DM session.</td>
</tr>
<tr>
<td>Packets transmitted</td>
<td>Total number of 1DM PDU frames sent to the remote MEP during this measurement session.</td>
</tr>
<tr>
<td>Average delay</td>
<td>Average two-way frame delay measured in this session.</td>
</tr>
<tr>
<td>Average delay variation</td>
<td>Average frame jitter measured in this session.</td>
</tr>
<tr>
<td>Best case delay</td>
<td>Lowest two-way frame delay measured in this session.</td>
</tr>
<tr>
<td>Worst case delay</td>
<td>Highest two-way frame delay measured in this session.</td>
</tr>
</tbody>
</table>

**NOTE:** For one-way delay measurement, these CLI output fields display NA (“not applicable”) at the initiator MEP because one-way frame delay measurements occur at the receiver MEP.

### Table 461: monitor ethernet delay-measurement two-way Output Fields

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Output Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two-way Ethernet frame delay measurement request to</td>
<td>Unicast MAC address of the remote peer MEP.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the Ethernet physical, logical, or trunk interface to which the local MEP is attached.</td>
</tr>
<tr>
<td>DMR received from</td>
<td>Unicast MAC address of the remote MEP that transmitted this DMR frame in response to a DMM frame.</td>
</tr>
<tr>
<td>Delay</td>
<td>Two-way delay, in microseconds, for the initiator-transmitted DMM frame.</td>
</tr>
<tr>
<td>Delay variation</td>
<td>Difference, in microseconds, between the current and previous delay values. This is also known as jitter.</td>
</tr>
<tr>
<td>Packets transmitted</td>
<td>Total number of DMM PDU frames sent to the remote MEP in this measurement session.</td>
</tr>
<tr>
<td>Valid packets received</td>
<td>Total number of DMR PDU frames received from the remote MEP in this measurement session.</td>
</tr>
<tr>
<td>Average delay</td>
<td>Average two-way frame delay measured in this session.</td>
</tr>
<tr>
<td>Average delay variation</td>
<td>Average frame jitter measured in this session.</td>
</tr>
</tbody>
</table>
Table 461: monitor ethernet delay-measurement two-way Output Fields (continued)

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Output Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best case delay</td>
<td>Lowest two-way frame delay measured in this session.</td>
</tr>
<tr>
<td>Worst case delay</td>
<td>Highest two-way frame delay measured in this session.</td>
</tr>
</tbody>
</table>

Sample Output

monitor ethernet delay-measurement one-way

```
user@switch> monitor ethernet delay-measurement one-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10
One-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR Frames sent: 10
--- Delay measurement statistics ---
Packets transmitted: 10
Average delay: NA, Average delay variation: NA
Best case delay: NA, Worst case delay: NA
```

monitor ethernet delay-measurement two-way

```
user@switch> monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a Delay: 100 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 111 usec Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a Delay: 112 usec Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a Delay: 112 usec Delay variation: 30 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 0 usec
--- Delay measurement statistics ---
Packets transmitted: 10, Valid packets received: 10
Average delay: 103 usec, Average delay variation: 8 usec
Best case delay: 92 usec, Worst case delay: 122 usec
```

monitor ethernet delay-measurement two-way (Invalid DMR Frames Received)

```
user@switch> monitor ethernet delay-measurement two-way 00:05:85:73:39:4a maintenance-domain md6 maintenance-association ma6 count 10
Two-way ETH-DM request to 00:05:85:73:39:4a, Interface xe-5/0/0.0
DMR received from 00:05:85:73:39:4a Delay: 100 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 8 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a Delay: 111 usec Delay variation: 19 usec
DMR received from 00:05:85:73:39:4a Delay: 112 usec Delay variation: 3 usec
DMR received from 00:05:85:73:39:4a Delay: 92 usec Delay variation: 0 usec
DMR received from 00:05:85:73:39:4a with invalid timestamp(s).
--- Delay measurement statistics ---
```
Packets transmitted: 10, Valid packets received: 9, Invalid packets received: 1
Average delay: 105 usec, Average delay variation: 9 usec
Best case delay: 92 usec, Worst case delay: 122 usec
show oam ethernet connectivity-fault-management delay-statistics

**Syntax**
show oam ethernet connectivity-fault-management delay-statistics
  <count entry-count>
  <local-mep local-mep-id>
  maintenance-association ma-name
  maintenance-domain md-name
  <remote-mep remote-mep-id>

**Release Information**
Command introduced in Junos OS Release 9.5.
Command introduced in Junos OS Release 11.4 for EX Series switches.

**Description**
On MX Series routers with Ethernet interfaces on Dense Port Concentrators (DPCs), display ETH-DM delay statistics.

On EX Series switches, display delay measurement results.

**Options**
- **count entry-count**—(Optional) Number of entries to display from the statistics table. The range of values is 1 through 100. The default value is 100 entries.
- **local-mep local-mep-id**—(Optional) Numeric identifier of the local MEP. On MX Series routers, the range of values is 1 through 8192. On EX Series switches, the range of values is 1 through 8191.
- **maintenance-association ma-name**—Name of an existing CFM maintenance association.
- **maintenance-domain md-name**—Name of an existing connectivity fault management (CFM) maintenance domain.
- **remote-mep remote-mep-id**—(Optional) Numeric identifier of the remote MEP. On MX Series routers, the range of values is 1 through 8192. On EX Series switches, the range of values is 1 through 8191.

**Required Privilege Level**
view

**Related Documentation**
- clear oam ethernet connectivity-fault-management statistics
- clear oam ethernet connectivity-fault-management delay-statistics on page 3869
- show oam ethernet connectivity-fault-management interfaces
- show oam ethernet connectivity-fault-management mep-database
- show oam ethernet connectivity-fault-management mep-statistics

**List of Sample Output**
show oam ethernet connectivity-fault-management delay-statistics on page 3880
show oam ethernet connectivity-fault-management delay-statistics remote-mep on page 3880

**Output Fields**
Table 462 on page 3879 lists the output fields for the show oam ethernet connectivity-fault-management delay-statistics command and the show oam ethernet
**connectivity-fault-management mep-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 462: show oam ethernet connectivity-fault-management delay-statistics and mep-statistics Output Fields

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEP Identifier</td>
<td>Maintenance association end point (MEP) numeric identifier.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Unicast MAC address configured for the MEP.</td>
</tr>
<tr>
<td>Remote MEP count</td>
<td>Number of remote MEPs (unless you specify the remote-mep option).</td>
</tr>
<tr>
<td>Remote MEP identifier</td>
<td>Numeric identifier of the remote MEP.</td>
</tr>
<tr>
<td>Remote MAC address</td>
<td>Unicast MAC address of the remote MEP.</td>
</tr>
<tr>
<td>Index</td>
<td>Index number that corresponds to the ETH-DM entry in the CFM database.</td>
</tr>
<tr>
<td>One-way delay (usec)</td>
<td>For a one-way ETH-DM session, the frame delay time, in microseconds, measured at the receiver MEP.</td>
</tr>
<tr>
<td></td>
<td>For a detailed description of one-way Ethernet frame delay measurement, see the ITU-T Y.1731 Ethernet Service OAM topics in the Junos OS Network Interfaces Library for Routing Devices.</td>
</tr>
<tr>
<td>Two-way delay (usec)</td>
<td>For a two-way ETH-DM session, the frame delay time, in microseconds, measured at the initiator MEP.</td>
</tr>
<tr>
<td></td>
<td>For a detailed description of two-way Ethernet frame delay measurement, see the ITU-T Y.1731 Ethernet Service OAM topics in the Junos OS Network Interfaces Library for Routing Devices.</td>
</tr>
<tr>
<td>Average one-way delay</td>
<td>Average one-way frame delay for the statistics displayed.</td>
</tr>
<tr>
<td>Average one-way delay variation</td>
<td>Average one-way “frame jitter” for the statistics displayed.</td>
</tr>
<tr>
<td>Best-case one-way delay</td>
<td>Lowest one-way frame delay for the statistics displayed.</td>
</tr>
<tr>
<td>Worst-case one-way delay</td>
<td>Highest one-way frame delay for the statistics displayed.</td>
</tr>
<tr>
<td>Average two-way delay</td>
<td>Average two-way frame delay for the statistics displayed.</td>
</tr>
<tr>
<td>Average two-way delay variation</td>
<td>Average two-way “frame jitter” for the statistics displayed.</td>
</tr>
<tr>
<td>Best-case two-way delay</td>
<td>Lowest two-way frame delay for the statistics displayed.</td>
</tr>
<tr>
<td>Worst-case two-way delay</td>
<td>Highest two-way frame delay calculated in this session.</td>
</tr>
</tbody>
</table>
Sample Output

```
show oam ethernet connectivity-fault-management delay-statistics

user@switch> show oam ethernet connectivity-fault-management delay-statistics
maintenance-domain md6 maintenance-association ma6
MEP identifier: 100, MAC address: 00:05:85:73:7b:39
Remote MEP count: 2
  Remote MEP identifier: 101
  Remote MAC address: 00:05:85:73:39:4a
  Delay measurement statistics:
  Index  One-way delay  Two-way delay
      (usec)         (usec)
    1   259            519
    2   273            550
    3   287            571
    4   299            610
    5   313            650
  Average one-way delay   : 286 usec
  Average one-way delay variation: 62 usec
  Best case one-way delay : 259 usec
  Worst case one-way delay : 313 usec
  Average two-way delay   : 580 usec
  Average two-way delay variation: 26 usec
  Best case two-way delay : 519 usec
  Worst case two-way delay : 650 usec

Remote MEP identifier: 102
Remote MAC address: 00:04:55:63:39:5a
  Delay measurement statistics:
  Index  One-way delay  Two-way delay
      (usec)         (usec)
    1    29             58
    2    23             59
    3    27             56
    4    29             62
    5    33             68
  Average one-way delay   : 28 usec
  Average one-way delay variation: 3 usec
  Best case one-way delay : 23 usec
  Worst case one-way delay : 33 usec
  Average two-way delay   : 60 usec
  Average two-way delay variation: 3 usec
  Best case two-way delay : 56 usec
  Worst case two-way delay : 68 usec
```

show oam ethernet connectivity-fault-management delay-statistics remote-mep
Average one-way delay : 286 usec
Average one-way delay variation: 62 usec
Best case one-way delay : 259 usec
Worst case one-way delay : 313 usec
Average two-way delay : 580 usec
Average two-way delay variation: 26 usec
Best case two-way delay : 519 usec
Worst case two-way delay : 650 usec
show oam ethernet connectivity-fault-management forwarding-state

Syntax
`show oam ethernet connectivity-fault-management forwarding-state`  
`interface interface-name`  
`<brief | detail | extensive>`

Release Information
Command introduced in Junos OS Release 10.2 for EX Series switches.

Description
Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management forwarding state information for Ethernet interfaces.

Options
-  `interface interface-name`—Display forwarding state information for the specified Ethernet interface only.
-  `brief | detail | extensive`—(Optional) Display the specified level of output.

Required Privilege
-  view

Related Documentation
-  clear oam ethernet connectivity-fault-management statistics on page 3872
-  show oam ethernet connectivity-fault-management path-database on page 3892
-  show oam ethernet connectivity-fault-management mip on page 3901

List of Sample Output
-  show oam ethernet connectivity-fault-management forwarding-state on page 3883
-  show oam ethernet connectivity-fault-management forwarding-state interface on page 3883
-  show oam ethernet connectivity-fault-management forwarding-state interface detail on page 3884
-  show oam ethernet connectivity-fault-management forwarding-state interface interface-name on page 3885

Output Fields
Table 463 on page 3882 lists the output fields for the `show oam ethernet connectivity-fault-management forwarding-state` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Interface identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Filter action</td>
<td>Filter action for messages at the level.</td>
<td>All levels</td>
</tr>
<tr>
<td>Nexthop type</td>
<td>Next-hop type.</td>
<td>All levels</td>
</tr>
<tr>
<td>Nexthop index</td>
<td>Next-hop index number.</td>
<td>brief</td>
</tr>
<tr>
<td>Level</td>
<td>Maintenance domain (MD) level.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 463: show oam ethernet connectivity-fault-management forwarding-state Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>MEP direction configured.</td>
<td>none</td>
</tr>
<tr>
<td>CEs</td>
<td>Number of customer edge (CE) interfaces.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show oam ethernet connectivity-fault-management forwarding-state

```
user@host> show oam ethernet connectivity–fault-management forwarding-state
CEs: 3
Maintenance domain forwarding state:

Level  Direction      Filter action     Nexthop     Nexthop
       type         index        type
0       Drop              none
1       Drop              none
2       Drop              none
3       Drop              none
4       Drop              none
5       Drop              none
6       Drop              none
7       Drop              none
```

show oam ethernet connectivity-fault-management forwarding-state interface

```
user@host> show oam ethernet connectivity-fault-management forwarding-state interface
Interface name: ge-3/0/0.0
Maintenance domain forwarding state:

Level  Direction      Filter action     Nexthop     Nexthop
       type         index        type
0       Drop              none
1       Drop              none
2       Drop              none
3       Drop              none
4       Drop              none
5       Drop              none
6       Drop              none
7        down             Receive             none
```

Interface name: xe-0/0/0.0
Instance name: __+bd1__
Maintenance domain forwarding state:

```
Level  Direction      Filter action     Nexthop     Nexthop
       type         index        type
0       Drop              none
```
1 Drop none
2 Drop none
3 Drop none
4 Drop none
5 Drop none
6 Drop none
7 down Receive none

```
show oam ethernet connectivity-fault-management forwarding-state interface detail

user@host> show oam ethernet connectivity-fault-management forwarding-state interface detail
Interface name: ge-3/0/0.0

  Level: 0
  Filter action: Drop
  Nexthop type: none

  Level: 1
  Filter action: Drop
  Nexthop type: none

  Level: 2
  Filter action: Drop
  Nexthop type: none

  Level: 3
  Filter action: Drop
  Nexthop type: none

  Level: 4
  Filter action: Drop
  Nexthop type: none

  Level: 5
  Filter action: Drop
  Nexthop type: none

  Level: 6
  Filter action: Drop
  Nexthop type: none

  Level: 7
  Direction: down
  Filter action: Receive
  Nexthop type: none

Interface name: xe-0/0/0.0

  Level: 0
  Filter action: Drop
  Nexthop type: none

  Level: 1
  Filter action: Drop
  Nexthop type: none
```
show oam ethernet connectivity-fault-management forwarding-state interface interface-name

```
user@host> show oam ethernet connectivity-fault-management forwarding-state interface interface-name ge-3/0/0.0
Interface name: ge-3/0/0.0

Maintenance domain forwarding state:

<table>
<thead>
<tr>
<th>Level</th>
<th>Direction</th>
<th>Filter action</th>
<th>Nexthop type</th>
<th>Nexthop index</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Drop</td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Drop</td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Drop</td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Drop</td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Drop</td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Drop</td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Drop</td>
<td>none</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>down</td>
<td>Receive</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>
```
show oam ethernet connectivity-fault-management interfaces

Syntax

```
show oam ethernet connectivity-fault-management interfaces
<ethernet-interface-name>
<level md-level>
<brief | detail | extensive>
```

Release Information

Command introduced in Junos OS Release 10.2 for EX Series switches.

Description

Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for Ethernet interfaces.

Options

- **brief | detail | extensive**—(Optional) Display the specified level of output.
- **ethernet-interface-name**—(Optional) Display CFM information only for CFM entities attached to the specified Ethernet interface.
- **level md-level**—(Optional) Display CFM information for CFM identities enclosed within a maintenance domain of the specified level.

Required Privilege

- **view**

Related Documentation

- clear oam ethernet connectivity-fault-management statistics on page 3872
- show oam ethernet connectivity-fault-management path-database on page 3892
- show oam ethernet connectivity-fault-management mip on page 3901

List of Sample Output

show oam ethernet connectivity-fault-management interfaces on page 3889
show oam ethernet connectivity-fault-management interfaces detail on page 3889
show oam ethernet connectivity-fault-management interfacesextensive on page 3890
show oam ethernet connectivity-fault-management interfaces level on page 3891
show oam ethernet connectivity-fault-management interfaces (Trunk Interfaces) on page 3891

Output Fields

Table 464 on page 3886 lists the output fields for the show oam ethernet connectivity-fault-management interfaces command. Output fields are listed in the approximate order in which they appear.

Table 464: show oam ethernet connectivity-fault-management interfaces Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Interface status</td>
<td>Local interface status.</td>
<td>All levels</td>
</tr>
<tr>
<td>Link status</td>
<td>Local link status. Up, down, or oam-down.</td>
<td>All levels</td>
</tr>
<tr>
<td>Maintenance domain name</td>
<td>Maintenance domain name.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
## Table 464: show oam ethernet connectivity-fault-management interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format (Maintenance domain)</td>
<td>Maintenance domain name format configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Level</td>
<td>Maintenance domain level configured.</td>
<td>All levels</td>
</tr>
<tr>
<td>Maintenance association name</td>
<td>Maintenance association name.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Format (Maintenance association)</td>
<td>Maintenance association name format configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Continuity-check status</td>
<td>Continuity-check status.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Interval</td>
<td>Continuity-check message interval.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Loss-threshold</td>
<td>Lost continuity-check message threshold.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MEP identifier</td>
<td>Maintenance association end point (MEP) identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbours</td>
<td>Number of MEP neighbors.</td>
<td>All levels</td>
</tr>
<tr>
<td>Direction</td>
<td>MEP direction configured.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address configured for the MEP.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>MEP status</td>
<td>Indicates the status of the Connectivity Fault Management (CFM) protocol running on the MEP: Running, inactive, disabled, or unsupported.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Remote MEP not receiving CCM</td>
<td>Whether the remote MEP is not receiving connectivity check messages (CCMs).</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Erroneous CCM received</td>
<td>Whether erroneous CCMs have been received.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Cross-connect CCM received</td>
<td>Whether cross-connect CCMs have been received.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>RDI sent by some MEP</td>
<td>Whether the remote defect indication (RDI) bit is set in messages that have been received. The absence of the RDI bit in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>CCMs sent</td>
<td>Number of CCMs transmitted.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>CCMs received out of sequence</td>
<td>Number of CCMs received out of sequence.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 464: show oam ethernet connectivity-fault-management interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBMs sent</td>
<td>Number of loopback request messages (LBMs) sent.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Valid in-order LBRs received</td>
<td>Number of loopback response messages (LBRs) received that were valid messages and in sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Valid out-of-order LBRs received</td>
<td>Number of LBRs received that were valid messages and not in sequence.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LBRs received with corrupted data</td>
<td>Number of LBRs received that were corrupted.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LBRs sent</td>
<td>Number of LBRs transmitted.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LTM s sent</td>
<td>Linktrace messages (LTMs) transmitted.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LTM s received</td>
<td>Linktrace messages received.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LTRs sent</td>
<td>Linktrace responses (LTRs) transmitted.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>LTR s received</td>
<td>Linktrace responses received.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Sequence number of next LTM request</td>
<td>Sequence number of next LTM request to be transmitted.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>1DMs sent</td>
<td>If the interface is attached to an initiator MEP for a one-way ETH-DM session: Number of one-way delay measurement (1DM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays 0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Valid 1DMs received</td>
<td>If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of valid 1DM frames received. For all other cases, this field displays 0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Invalid 1DMs received</td>
<td>If the interface is attached to a receiver MEP for a one-way ETH-DM session: Number of invalid 1DM frames received. For all other cases, this field displays 0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DMMs sent</td>
<td>If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays 0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>DMRs sent</td>
<td>If the interface is attached to a responder MEP for a two-way ETH-DM session: Number of Delay Measurement Reply (DMR) frames sent. For all other cases, this field displays 0.</td>
<td>detail extensive</td>
</tr>
</tbody>
</table>
Table 464: show oam ethernet connectivity-fault-management interfaces Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid DMRs received</td>
<td>If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of valid DMRs received. For all other cases, this field displays 0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Invalid DMRs received</td>
<td>If the interface is attached to an initiator MEP for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays 0.</td>
<td>detail extensive</td>
</tr>
<tr>
<td>Remote MEP count</td>
<td>Number of remote MEPs.</td>
<td>extensive</td>
</tr>
<tr>
<td>Identifier (remote MEP)</td>
<td>MEP identifier of the remote MEP.</td>
<td>extensive</td>
</tr>
<tr>
<td>MAC address (remote MEP)</td>
<td>MAC address of the remote MEP.</td>
<td>extensive</td>
</tr>
<tr>
<td>State (remote MEP)</td>
<td>State of the remote MEP.</td>
<td>extensive</td>
</tr>
<tr>
<td>Interface (remote MEP)</td>
<td>Interface of the remote MEP.</td>
<td>extensive</td>
</tr>
</tbody>
</table>

Sample Output

show oam ethernet connectivity-fault-management interfaces

```
user@host> show oam ethernet connectivity-fault-management interfaces
Interface       Link       Status           Level       MEP          Neighbours
ge-1/1/0.0      Up         Active           0           2            1
ge-1/1/0.1      Up         Active           0           2            1
ge-1/1/0.10     Up         Active           0           2            1
ge-1/1/0.100    Up         Active           0           2            1
ge-1/1/0.101    Up         Active           0           2            1
ge-1/1/0.102    Up         Active           0           2            1
ge-1/1/0.103    Up         Active           0           2            1
ge-1/1/0.104    Up         Active           0           2            1
ge-1/1/0.105    Up         Active           0           2            1
ge-1/1/0.106    Up         Active           0           2            1
...```

show oam ethernet connectivity-fault-management interfaces detail

```
user@host> show oam ethernet connectivity-fault-management interfaces detail
Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
Maintenance domain name: md0, Format: string, Level: 5
Maintenance association name: ma1, Format: string
```
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 1, Direction: down, MAC address: 00:90:69:0b:4b:94
MEP status: running
Defects:
  Remote MEP not receiving CCM : no
  Erroneous CCM received : yes
  Cross-connect CCM received : no
  RDI sent by some MEP : yes
Statistics:
  CCMs sent : 76
  CCMs received out of sequence : 0
  LBMs sent : 0
  Valid in-order LBRs received : 0
  Valid out-of-order LBRs received : 0
  LBRs received with corrupted data : 0
  LBRs sent : 0
  LTMs sent : 0
  LTMs received : 0
  LTRs sent : 0
  LTRs received : 0
  Sequence number of next LTM request : 0
  1DMs sent : 0
  Valid 1DMs received : 0
  Invalid 1DMs received : 0
  DMMs sent : 0
  Valid DMRs received : 0
  Invalid DMRs received : 0
Remote MEP count: 2

<table>
<thead>
<tr>
<th>Identifier</th>
<th>MAC address</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>00:90:69:0b:7f:71</td>
<td>ok</td>
<td>ge-5/2/9.0</td>
</tr>
<tr>
<td>4001</td>
<td>00:90:69:0b:09:c5</td>
<td>ok</td>
<td>ge-5/2/9.0</td>
</tr>
</tbody>
</table>

show oam ethernet connectivity-fault-management interfaces extensive

user@host> show oam ethernet connectivity-fault-management interfaces extensive
Interface name: ge-5/2/9.0, Interface status: Active, Link status: Up
Maintenance domain name: md0, Format: string, Level: 5
Maintenance association name: ma1, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 1, Direction: down, MAC address: 00:90:69:0b:4b:94
MEP status: running
Defects:
  Remote MEP not receiving CCM : no
  Erroneous CCM received : yes
  Cross-connect CCM received : no
  RDI sent by some MEP : yes
Statistics:
  CCMs sent : 76
  CCMs received out of sequence : 0
  LBMs sent : 0
  Valid in-order LBRs received : 0
  Valid out-of-order LBRs received : 0
  LBRs received with corrupted data : 0
  LBRs sent : 0
  LTMs sent : 0
  LTMs received : 0
  LTRs sent : 0
  LTRs received : 0
show oam ethernet connectivity-fault-management interfaces level

```
user@host> show oam ethernet connectivity-fault-management interfaces level 7
Interface   Link      Status       Level  MEP         Neighbours
ge-3/0/0.0  Up        Active       7      201          0
xe-0/0/0.0  Up        Active       7      203          1
```

show oam ethernet connectivity-fault-management interfaces (Trunk Interfaces)

```
user@host> show oam ethernet connectivity-fault-management interfaces
Interface   Link      Status       Level  MEP         Neighbours
ge-4/0/1.0  Up        Active       5      100          0
ge-10/3/10.4091, vlan 4091  Down      Inactive     4      400         0
ge-4/0/0.0   Up        Active       6      200         0

user@host> show oam ethernet connectivity-fault-management interfaces ge-4/0/0.0
Interface   Link      Status       Level  MEP         Neighbours
ge-4/0/0.0  Up        Active       6      200         0

user@host> show oam ethernet connectivity-fault-management interfaces ge-4/0/1.0 vlan 100
Interface   Link      Status       Level  MEP         Neighbours
ge-4/0/1.0  Up        Active       5      100          0

user@host> show oam ethernet connectivity-fault-management interfaces ge-10/3/10.4091 vlan 4091
Interface   Link      Status       Level  MEP         Neighbours
ge-10/3/10.4091, vlan 4091  Down      Inactive     4      400         0
```
**show oam ethernet connectivity-fault-management path-database**

**Syntax**  
```
show oam ethernet connectivity-fault-management path-database host
maintenance-association ma-name maintenance-domain md-name mac-address
```

**Release Information**  
Command introduced in Junos OS Release 10.2 for EX Series switches.

**Description**  
Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management maintenance linktrace database information.

**Options**  
- `mac-address`—Display connectivity fault management path database information for the specified MAC address of the remote host.
- `maintenance-association ma-name`—Display connectivity fault management path database information for the specified maintenance association.
- `maintenance-domain md-name`—Display connectivity fault management path database information for the specified maintenance domain.

**Required Privilege**  
`view`

**Related Documentation**  
- clear oam ethernet connectivity-fault-management statistics on page 3872
- show oam ethernet connectivity-fault-management interfaces on page 3886
- show oam ethernet connectivity-fault-management mip on page 3901

**List of Sample Output**  
- show oam ethernet connectivity-fault-management path-database on page 3893
- show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands) on page 3893

**Output Fields**  
Table 465 on page 3892 lists the output fields for the `show oam ethernet connectivity-fault-management path-database` command. Output fields are listed in the approximate order in which they appear.

**Table 465: show oam ethernet connectivity-fault-management linktrace path-database Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linktrace to</td>
<td>MAC address of the 802.1ag node to which the linktrace message is targeted.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface used by the local MEP to send the linktrace message (LTM).</td>
</tr>
<tr>
<td>Maintenance Domain</td>
<td>Maintenance domain identifier specified in the traceroute command.</td>
</tr>
<tr>
<td>Maintenance Association</td>
<td>Maintenance association identifier specified in the traceroute command.</td>
</tr>
<tr>
<td>Level</td>
<td>Maintenance domain level configured for the maintenance domain.</td>
</tr>
</tbody>
</table>
Table 465: show oam ethernet connectivity-fault-management linktrace path-database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Mep</strong></td>
<td>MEP identifier of the local MEP originating the linktrace.</td>
</tr>
<tr>
<td><strong>Hop</strong></td>
<td>Sequential hop count of the linktrace path.</td>
</tr>
<tr>
<td><strong>TTL</strong></td>
<td>Number of hops remaining in the linktrace message (LTM). The time to live (TTL) is decremented at each hop.</td>
</tr>
<tr>
<td><strong>Source MAC address</strong></td>
<td>MAC address of the 802.1ag maintenance intermediate point (MIP) that is forwarding the LTM.</td>
</tr>
<tr>
<td><strong>Next hop MAC address</strong></td>
<td>MAC address of the 802.1ag node that is the next hop in the LTM path.</td>
</tr>
<tr>
<td><strong>Transaction Identifier</strong></td>
<td>4-byte identifier maintained by the MEP. Each LTM uses a transaction identifier. The transaction identifier is maintained globally across all maintenance domains. Use the transaction identifier to match an incoming linktrace responses (LTR), with a previously sent LTM.</td>
</tr>
</tbody>
</table>

Sample Output

show oam ethernet connectivity-fault-management path-database

user@host> show oam ethernet connectivity-fault-management path-database maintenance-domain MD1 maintenance-association MA1 00:01:02:03:04:05 Linktrace to 00:01:02:03:04:05, Interface : ge-5/0/0.0 Maintenance Domain: MD1, Level: 7 Maintenance Association: MA1, Local Mep: 1

<table>
<thead>
<tr>
<th>Hop</th>
<th>TTL</th>
<th>Source MAC address</th>
<th>Next hop MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>63</td>
<td>00:00:aa:aa:aa:aa</td>
<td>00:00:bb:bb:bb:bb</td>
</tr>
<tr>
<td>2</td>
<td>62</td>
<td>00:00:bb:bb:bb:bb</td>
<td>00:00:cc:cc:cc:cc</td>
</tr>
<tr>
<td>3</td>
<td>61</td>
<td>00:00:cc:cc:cc:cc</td>
<td>00:01:02:03:04:05</td>
</tr>
<tr>
<td>4</td>
<td>60</td>
<td>00:01:02:03:04:05</td>
<td>00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

Transaction Identifier:100001

show oam ethernet connectivity-fault-management linktrace path-database (Two traceroute Commands)

user@host> show oam ethernet connectivity-fault-management path-database maintenance-domain MD2 maintenance-association MA2 00:06:07:08:09:0A Linktrace to 00:06:07:08:09:0A, Interface : ge-5/0/1.0 Maintenance Domain: MD2, Level: 6 Maintenance Association: MA2, Local Mep: 10

<table>
<thead>
<tr>
<th>Hop</th>
<th>TTL</th>
<th>Source MAC address</th>
<th>Next hop MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>63</td>
<td>00:00:aa:aa:aa:aa</td>
<td>00:00:bb:bb:bb:bb</td>
</tr>
<tr>
<td>2</td>
<td>62</td>
<td>00:00:bb:bb:bb:bb</td>
<td>00:00:cc:cc:cc:cc</td>
</tr>
<tr>
<td>3</td>
<td>61</td>
<td>00:00:cc:cc:cc:cc</td>
<td>00:06:07:08:09:0A</td>
</tr>
<tr>
<td>4</td>
<td>60</td>
<td>00:06:07:08:09:0A</td>
<td>00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

Transaction Identifier:100002

Transaction Identifier:100003

Transaction Identifier:1000003

Copyright © 2013, Juniper Networks, Inc.
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>61</td>
<td>00:00:cc:cc:cc:cc</td>
<td>00:06:07:08:09:0A</td>
</tr>
<tr>
<td>4</td>
<td>60</td>
<td>00:06:07:08:09:0A</td>
<td>00:00:00:00:00:00</td>
</tr>
</tbody>
</table>
**show oam ethernet connectivity-fault-management mep-database**

**Syntax**

```
show oam ethernet connectivity-fault-management mep-database
maintenance-domain domain-name
maintenance-association ma-name
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

**Release Information**

Command introduced in Junos OS Release 10.2 for EX Series switches.

**Description**

Display IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.

**Options**

- `maintenance-association ma-name`—Display connectivity fault management information for the specified maintenance association.
- `maintenance-domain domain-name`—Display connectivity fault management information for the specified maintenance domain.
- `local-mep local-mep-id`—(Optional) Display connectivity fault management information for the specified local MEP only.
- `remote-mep remote-mep-id`—(Optional) Display connectivity fault management information for the specified remote MEP only.

**Required Privilege**

view

**Related Documentation**

- clear oam ethernet connectivity-fault-management statistics on page 3872
- show oam ethernet connectivity-fault-management interfaces on page 3886
- show oam ethernet connectivity-fault-management mip on page 3901

**List of Sample Output**

show oam ethernet connectivity-fault-management mep-database on page 3899
show oam ethernet connectivity-fault-management mep-database local-mep remote-mep on page 3899
show oam ethernet connectivity-fault-management mep-database remote-mep (Action Profile Event) on page 3899

**Output Fields**

Table 466 on page 3895 lists the output fields for the `show oam ethernet connectivity-fault-management mep-database` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance domain name</td>
<td>Maintenance domain name.</td>
</tr>
</tbody>
</table>
### Table 466: show oam ethernet connectivity-fault-management mep-database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format (Maintenance domain)</td>
<td>Maintenance domain name format configured.</td>
</tr>
<tr>
<td>Level</td>
<td>Maintenance domain level configured.</td>
</tr>
<tr>
<td>Maintenance association name</td>
<td>Maintenance association name.</td>
</tr>
<tr>
<td>Format (Maintenance association)</td>
<td>Maintenance association name format configured.</td>
</tr>
<tr>
<td>Continuity-check status</td>
<td>Continuity-check status.</td>
</tr>
<tr>
<td>Interval</td>
<td>Continuity-check message interval.</td>
</tr>
<tr>
<td>MEP Identifier</td>
<td>Maintenance association end point (MEP) identifier.</td>
</tr>
<tr>
<td>Direction</td>
<td>MEP direction configured.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address configured for the MEP.</td>
</tr>
<tr>
<td>Auto-discovery</td>
<td>Whether automatic discovery is enabled or disabled.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority used for CCMs and linktrace messages transmitted by the MEP.</td>
</tr>
<tr>
<td>Interface name</td>
<td>Interface identifier.</td>
</tr>
<tr>
<td>Interface status</td>
<td>Local interface status.</td>
</tr>
<tr>
<td>Link status</td>
<td>Local link status.</td>
</tr>
<tr>
<td>Remote MEP not receiving CCM</td>
<td>Whether the remote MEP is not receiving CCMs.</td>
</tr>
<tr>
<td>Erroneous CCM received</td>
<td>Whether erroneous CCMs have been received.</td>
</tr>
<tr>
<td>Cross-connect CCM received</td>
<td>Whether cross-connect CCMs have been received.</td>
</tr>
<tr>
<td>RDI sent by some MEP</td>
<td>Whether the remote defect indication (RDI) bit is set in messages that have been received. The absence of the RDI bit in a CCM indicates that the transmitting MEP is receiving CCMs from all configured MEPs.</td>
</tr>
<tr>
<td>CCMs sent</td>
<td>Number of CCMs transmitted.</td>
</tr>
<tr>
<td>CCMs received out of sequence</td>
<td>Number of CCMs received out of sequence.</td>
</tr>
</tbody>
</table>
Table 466: show oam ethernet connectivity-fault-management mep-database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBMs sent</td>
<td>Number of loopback messages (LBMs) sent.</td>
</tr>
<tr>
<td>Valid in-order LBRs received</td>
<td>Number of loopback response messages (LBRs) received that were valid messages and in sequence.</td>
</tr>
<tr>
<td>Valid out-of-order LBRs received</td>
<td>Number of LBRs received that were valid messages and not in sequence.</td>
</tr>
<tr>
<td>LBRs received with corrupted data</td>
<td>Number of LBRs received that were corrupted.</td>
</tr>
<tr>
<td>LBRs sent</td>
<td>Number of LBRs transmitted.</td>
</tr>
<tr>
<td>LTMssent</td>
<td>Linktrace messages (LTMs) transmitted.</td>
</tr>
<tr>
<td>LTMs received</td>
<td>Linktrace messages received.</td>
</tr>
<tr>
<td>LTRs sent</td>
<td>Linktrace responses (LTRs) transmitted.</td>
</tr>
<tr>
<td>LTRs received</td>
<td>Linktrace responses received.</td>
</tr>
<tr>
<td>Sequence number of next LTM request</td>
<td>Sequence number of the next linktrace message request to be transmitted.</td>
</tr>
<tr>
<td>1DMs sent</td>
<td>If the MEP is an initiator for a one-way ETH-DM session: Number of one-way delay measurement (IDM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays 0.</td>
</tr>
<tr>
<td>Valid 1DMs received</td>
<td>If the MEP is a receiver for a one-way ETH-DM session: Number of valid 1DM frames received.                                                          For all other cases, this field displays 0.</td>
</tr>
<tr>
<td>Invalid 1DMs received</td>
<td>If the MEP is a receiver for a one-way ETH-DM session: Number of invalid 1DM frames received.                                                        For all other cases, this field displays 0.</td>
</tr>
<tr>
<td>DMMs sent</td>
<td>If the MEP is an initiator for a two-way ETH-DM session: Number of Delay Measurement Message (DMM) PDU frames sent to the peer MEP in this session. For all other cases, this field displays 0.</td>
</tr>
<tr>
<td>DMRs sent</td>
<td>If the MEP is a responder for an ETH-DM session: Number of Delay Measurement Reply (DMR) frames sent.                                               For all other cases, this field displays 0.</td>
</tr>
</tbody>
</table>
Table 466: show oam ethernet connectivity-fault-management mep-database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid DMRs received</td>
<td>If the MEP is an initiator for a two-way ETH-DM session: Number of valid DMRs received. For all other cases, this field displays 0.</td>
</tr>
<tr>
<td>Invalid DMRs received</td>
<td>If the MEP is an initiator for a two-way ETH-DM session: Number of invalid DMRs received. For all other cases, this field displays 0.</td>
</tr>
<tr>
<td>Remote MEP identifier</td>
<td>MEP identifier of the remote MEP.</td>
</tr>
<tr>
<td>State (remote MEP)</td>
<td>State of the remote MEP: idle, start, ok, or failed.</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address of the remote MEP.</td>
</tr>
<tr>
<td>Type</td>
<td>Whether the remote MEP MAC address was learned using automatic discovery or configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface of the remote MEP. A seven-digit number is appended if CFM is configured to run on a routing instance of type VPLS.</td>
</tr>
<tr>
<td>Last flapped</td>
<td>Date, time, and how long ago the remote MEP interface went from down to up. The format is Last flapped: year-month-day hours:minutes:seconds timezone (hours:minutes:seconds ago). For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago).</td>
</tr>
<tr>
<td>Remote defect indication</td>
<td>Whether the remote defect indication (RDI) bit is set in messages that have been received or transmitted.</td>
</tr>
<tr>
<td>Port status TLV</td>
<td>• In the Maintenance domain section, displays the last transmitted port status TLV value.</td>
</tr>
<tr>
<td></td>
<td>• In the Remote MEP section, displays the last value of port status TLV received from the remote MEP.</td>
</tr>
<tr>
<td></td>
<td>In the Action profile section, displays the last occurred event port-status-tlv blocked event. This event occurred due to the reception of blocked value in the port status TLV from remote MEP.</td>
</tr>
<tr>
<td>Interface status TLV</td>
<td>• In the Maintenance domain section, displays the last transmitted interface status TLV value.</td>
</tr>
<tr>
<td></td>
<td>• In the Remote MEP section, displays the last value of Interface status TLV received from the remote MEP.</td>
</tr>
<tr>
<td></td>
<td>In the Action profile section, if displays, the last occurred event interface-status-tlv event (either lower-layer-down or down). This event occurred due to the reception of either lower or down value in the interface status TLV from remote MEP.</td>
</tr>
<tr>
<td>Action profile</td>
<td>Name of the action profile occurrence associated with a remote MEP.</td>
</tr>
<tr>
<td>Last event</td>
<td>When an action profile occurs, displays the last event that triggered it.</td>
</tr>
<tr>
<td>Last event cleared</td>
<td>When all the configured and occurred events (under action profile) are cleared, then the action taken gets reverted (such as down interface is made up) and the corresponding time is noted and displayed.</td>
</tr>
<tr>
<td>Action</td>
<td>Action taken and the corresponding time of the action occurrence.</td>
</tr>
</tbody>
</table>
Sample Output

show oam ethernet connectivity-fault-management mep-database

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain vpls-vlan2000 maintenance-association vpls-vlan200
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
Maintenance association name: vpls-vlan200, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
Auto-discovery: enabled, Priority: 0
Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up
Defects:
  Remote MEP not receiving CCM                  : no
  Erroneous CCM received                        : no
  Cross-connect CCM received                    : no
  RDI sent by some MEP                          : no
Statistics:
  CCMs sent                                     : 1476
  CCMs received out of sequence                 : 0
  LBMs sent                                     : 85
  Remote MEP count: 1
  Identifier    MAC address    State    Interface
  100     00:19:e2:b2:81:4b       ok  vt-0/1/10.1049088
```

show oam ethernet connectivity-fault-management mep-database local-mep remote-mep

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain vpls-vlan2000 maintenance-association vpls-vlan200 local-mep 200
remote-mep 100
Maintenance domain name: vpls-vlan2000, Format: string, Level: 5
Maintenance association name: vpls-vlan200, Format: string
Continuity-check status: enabled, Interval: 100ms, Loss-threshold: 3 frames
MEP identifier: 200, Direction: up, MAC address: 00:19:e2:b0:74:01
Auto-discovery: enabled, Priority: 0
Interface name: ge-0/0/1.0, Interface status: Active, Link status: Up
Remote MEP identifier: 100, State: ok
  MAC address: 00:19:e2:b2:81:4b, Type: Learned
  Interface: vt-0/1/10.1049088
  Last flapped: Never
  Remote defect indication: false
  Port status TLV: none
  Interface status TLV: none
```

show oam ethernet connectivity-fault-management mep-database remote-mep (Action Profile Event)

```
user@host> show oam ethernet connectivity-fault-management mep-database
maintenance-domain md5 maintenance-association ma5 remote-mep 200
Maintenance domain name: md5, Format: string, Level: 5
Maintenance association name: ma5, Format: string
Continuity-check status: enabled, Interval: 1s, Loss-threshold: 3 frames
MEP identifier: 100, Direction: down, MAC address: 00:05:85:73:e8:ad
Auto-discovery: enabled, Priority: 0
Interface status TLV: none, Port status TLV: none
Interface name: ge-1/0/8.0, Interface status: Active, Link status: Up
```
Remote MEP identifier: 200, State: ok
MAC address: 00:05:85:73:96:1f, Type: Configured
Interface: ge-1/0/8.0
Last flapped: Never
Remote defect indication: false
Port status TLV: none
Interface status TLV: lower-layer-down
Action profile: juniper
  Last event: Interface-status-tlv lower-layer-down
  Action: Interface-down, Time: 2009-03-27 14:25:10 PDT (00:00:02 ago)
**show oam ethernet connectivity-fault-management mip**

**Syntax**

```
show oam ethernet connectivity-fault-management mip <qualifier>
```

**Release Information**
Command introduced in Junos OS Release 10.2 for EX Series switches.

**Description**
Display all the maintenance association intermediate points (MIPs) created in the system. Specify qualifiers to display specific MIPs.

**Options**
- `qualifier` - (Optional) Display the specified MIP.

**Required Privilege**
- View

**Related Documentation**
- `show oam ethernet connectivity-fault-management interfaces` on page 3886
- `show oam ethernet connectivity-fault-management path-database` on page 3892

**List of Sample Output**
- `show oam ethernet connectivity-fault-management mip` on page 3901

**Output Fields**
Table 467 on page 3901 lists the output fields for the `show oam ethernet connectivity-fault-management mip` command. Output fields are listed in the approximate order in which they appear.

**Table 467: show oam ethernet connectivity-fault-management mip Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIP information for instance</td>
<td>Header for the MIP information showing the MIP name.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface type-dpc/pic/port.unit-number.</td>
</tr>
<tr>
<td>Level</td>
<td>MIP level configured.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
user@host> show oam ethernet connectivity-fault-management mip
MIP information for __mip_name__

MIP information for default-switch bd1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-3/0/0.0</td>
<td>7</td>
</tr>
<tr>
<td>ge-3/0/1.0</td>
<td>6</td>
</tr>
<tr>
<td>ge-3/0/3.0</td>
<td>6</td>
</tr>
</tbody>
</table>
```
show oam ethernet connectivity-fault-management sla-iterator-statistics

Syntax

```
show oam ethernet connectivity-fault-management sla-iterator-statistics
maintenance-domain md-name
maintenance-association ma-name
sla-iterator sla-iterator
<local-mep local-mep-id>
<remote-mep remote-mep-id>
```

Release Information

Command introduced in Junos OS Release 11.4 for EX Series switches.
Command introduced in Junos OS Release 12.2 for ACX Series routers.
Command introduced in Junos OS Release 13.2 for MX Series routers (not on MPC3E Hyperion cards).

Description

Display the Ethernet Operation, Administration, and Maintenance (OAM) service-level agreement (SLA) iterator statistics.

Options

- `maintenance-domain md-name`—Name of an existing connectivity fault management (CFM) maintenance domain.
- `maintenance-association ma-name`—Name of an existing CFM maintenance association.
- `sla-iterator sla-iterator`—Name of the iterator profile.
- `local-mep local-mep-id`—(Optional) Numeric identifier of the local MEP. The range of values is 1 through 8191.
- `remote-mep remote-mep-id`—(Optional) Numeric identifier of the remote MEP. The range of values is 1 through 8192.

Required Privilege Level

view

Related Documentation

- Configuring an Iterator Profile on a Switch (CLI Procedure) on page 3621
- clear oam ethernet connectivity-fault-management sla-iterator-statistics on page 3871

List of Sample Output

- show oam ethernet connectivity-fault-management sla-iterator-statistics on page 3905
- show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers) on page 3905

Output Fields

Table 468 on page 3902 lists the output fields for the `show oam ethernet connectivity-fault-management sla-iterator-statistics` command. Output fields are listed in the approximate order in which they appear.

Table 468: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Output Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance domain</td>
<td>Name of the maintenance domain.</td>
</tr>
</tbody>
</table>
### Table 468: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Output Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
<td>Level of the maintenance domain level configured.</td>
</tr>
<tr>
<td><strong>Maintenance association</strong></td>
<td>Name of the maintenance association.</td>
</tr>
<tr>
<td><strong>Local MEP id</strong></td>
<td>Numeric identifier of the local MEP.</td>
</tr>
<tr>
<td><strong>Remote MEP id</strong></td>
<td>Numeric identifier of the remote MEP.</td>
</tr>
<tr>
<td><strong>Remote MAC address</strong></td>
<td>Unicast MAC address of the remote MEP.</td>
</tr>
<tr>
<td><strong>Iterator name</strong></td>
<td>Name of iterator.</td>
</tr>
<tr>
<td><strong>Iterator Id</strong></td>
<td>Numeric identifier of the iterator.</td>
</tr>
<tr>
<td><strong>Iterator cycle time</strong></td>
<td>Number of cycles (in milliseconds) taken between back-to-back transmission of SLA frames for this connection</td>
</tr>
<tr>
<td><strong>Iteration period</strong></td>
<td>Maximum number of cycles per iteration</td>
</tr>
<tr>
<td><strong>Iterator status</strong></td>
<td>Current status of iterator whether running or stopped.</td>
</tr>
<tr>
<td><strong>Infinite iterations</strong></td>
<td>Status of iteration as infinite or finite.</td>
</tr>
<tr>
<td><strong>Counter reset time</strong></td>
<td>Date and time when the counter was reset.</td>
</tr>
<tr>
<td><strong>Reset reason</strong></td>
<td>Reason to reset counter.</td>
</tr>
<tr>
<td><strong>Delay weight</strong></td>
<td>Calculation weight of delay.</td>
</tr>
<tr>
<td><strong>Delay variation weight</strong></td>
<td>Calculation weight of delay variation.</td>
</tr>
<tr>
<td><strong>DMM sent</strong></td>
<td>Delay measurement message (DMM) PDU frames sent to the peer MEP in this session.</td>
</tr>
<tr>
<td><strong>DMM skipped for threshold hit</strong></td>
<td>Number of DMM frames sent to the peer MEP in this session skipped during threshold hit.</td>
</tr>
<tr>
<td><strong>DMM skipped for threshold hit window</strong></td>
<td>Number of DMM frames sent to the peer MEP in this session skipped during the last threshold hit window.</td>
</tr>
<tr>
<td><strong>DMR received</strong></td>
<td>Number of delay measurement reply (DMR) frames received.</td>
</tr>
<tr>
<td><strong>DMR out of sequence</strong></td>
<td>Total number of DMR out of sequence packets received.</td>
</tr>
<tr>
<td><strong>DMR received with invalid time stamps</strong></td>
<td>Total number of DMR frames received with invalid timestamps.</td>
</tr>
</tbody>
</table>
Table 468: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Output Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average two-way delay</td>
<td>Average two-way frame delay for the statistics displayed.</td>
</tr>
<tr>
<td>Average two-way delay variation</td>
<td>Average two-way “frame jitter” for the statistics displayed.</td>
</tr>
<tr>
<td>Average one-way forward delay variation</td>
<td>Average one-way forward delay variation for the statistics displayed in microseconds.</td>
</tr>
<tr>
<td>Average one-way backward delay variation</td>
<td>Average one-way backward delay variation for the statistics displayed in microseconds.</td>
</tr>
<tr>
<td>Weighted average two-way delay</td>
<td>Weighted average two-way delay for the statistics displayed in microseconds.</td>
</tr>
<tr>
<td>Weighted average two-way delay variation</td>
<td>Weighted average two-way delay variation for the statistics displayed in microseconds.</td>
</tr>
<tr>
<td>Weighted average one-way backward delay variation</td>
<td>Weighted average one-way backward delay variation for the statistics displayed in microseconds.</td>
</tr>
<tr>
<td>Weighted average one-way forward delay variation</td>
<td>Weighted average one-way forward delay variation for the statistics displayed in microseconds.</td>
</tr>
<tr>
<td>SLM packets sent</td>
<td>Total number of synthetic loss message (SLM) PDU frames sent from the source MEP to the remote MEP during this ETH-SLM session.</td>
</tr>
<tr>
<td>SLM packets received</td>
<td>Total number of synthetic loss message (SLM) PDU frames that the remote MEP received from the source MEP during this ETH-SLM session.</td>
</tr>
<tr>
<td>SLR packets sent</td>
<td>Total number of synthetic loss reply (SLR) PDU frames that the remote MEP sent to the source MEP during this measurement session.</td>
</tr>
<tr>
<td>SLR packets received</td>
<td>Total number of synthetic loss reply (SLR) PDU frames that the source MEP received from the remote MEP during this measurement session.</td>
</tr>
<tr>
<td>Local TXFC1 value</td>
<td>Number of synthetic frames transmitted to the peer MEP for a test ID. A test ID is used to distinguish each synthetic loss measurement because multiple measurements can be simultaneously activated also on a given CoS and MEP pair. It must be unique at least within the context of any SLM for the MEG and initiating MEP.</td>
</tr>
<tr>
<td>Local RXFC1 value</td>
<td>Number of synthetic frames received from the peer MEP for a test ID. The MEP generates a unique Test ID for the session, adds the source MEP ID, and initializes the local counters for the session before SLM initiation. For each SLM PDU transmitted for the session (test ID), the local counter TXFC1 is sent in the packet.</td>
</tr>
</tbody>
</table>
| Last Received SLR frame TXFC1(tc)       | Value of the local counter TxFC1 at the time of SLM frame transmission. }
Table 468: show oam ethernet connectivity-fault-management sla-iterator-statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Output Field Name</th>
<th>Output Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value of the local counter RxFCI at the time of SLR frame transmission.</td>
<td><strong>Output Field Description</strong>: Value of the local counter RxFCI at the time of SLR frame transmission.</td>
</tr>
<tr>
<td>Count of frame loss associated with ingress data frames.</td>
<td><strong>Output Field Description</strong>: Count of frame loss associated with ingress data frames.</td>
</tr>
<tr>
<td>Count of frame loss associated with egress data frames.</td>
<td><strong>Output Field Description</strong>: Count of frame loss associated with egress data frames.</td>
</tr>
</tbody>
</table>

Sample Output

```
user@switch> show oam ethernet connectivity-fault-management sla-iterator-statistics
maintenance-domain default-1 maintenance-association ma1 local-mep 1 remote-mep 2
Iterator statistics:
Maintenance domain: md6, Level: 6
Maintenance association: ma6, Local MEP id: 1000
Remote MEP id: 103, Remote MAC address: 00:90:69:0a:43:92
Iterator name: i1, Iterator Id: 1
Iterator cycle time: 10ms, Iteration period: 1 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2010-03-19 20:42:39 PDT (2d 18:24 ago)
Reset reason: Adjacency flap

Iterator delay measurement statistics:
Delay weight: 1, Delay variation weight: 1
DMM sent : 23898520
DMM skipped for threshold hit : 11000
DMM skipped for threshold hit window : 0
DMR received : 23851165
DMR out of sequence : 1142
DMR received with invalid time stamps : 36540
Average two-way delay : 129 usec
Average two-way delay variation : 15 usec
Average one-way forward delay variation : 22 usec
Average one-way backward delay variation : 22 usec
Weighted average two-way delay : 134 usec
Weighted average two-way delay variation : 8 usec
Weighted average one-way forward delay variation : 6 usec
Weighted average one-way backward delay variation : 2 usec
```

Sample Output

```
user@switch> show oam ethernet connectivity-fault-management sla-iterator-statistics (MX Series routers)
maintenance-domain mdu maintenance-association mau local-mep 4 remote-mep 3 sla-iterator lm
Iterator statistics:
Maintenance domain: 2, Level: 2
Maintenance association: W-160432000-001, Local MEP id: 2
Remote MEP id: 1, Remote MAC address: 00:90:69:0a:43:39
```
Iterator name: iter1, Iterator Id: 1
Iterator cycle time: 100ms, Iteration period: 10 cycles
Iterator status: running, Infinite iterations: true
Counter reset time: 2012-09-25 02:15:31 PDT (00:00:45 ago)
Reset reason: Adjacency flap
Iterator loss measurement statistics:
  LMM sent: 444
  LMM skipped for threshold hit: 0
  LMM skipped for threshold hit window: 0
  LMR received: 444
  LMR out of sequence: 0
  LMR forwarding-class mismatch: 0
Accumulated transmit statistics:
  Near-end (CIR): 0
  Far-end (CIR): 0
  Near-end (EIR): 0
  Far-end (EIR): 0
Accumulated receive statistics:
  Near-end (CIR): 0
  Far-end (CIR): 0
  Near-end (EIR): 0
  Far-end (EIR): 0
Accumulated loss statistics:
  Near-end loss (CIR): 0 (0.00000%)
  Near-end loss-ratio (CIR): 0 (0.00000%)
  Far-end loss (CIR): 0
  Far-end loss-ratio (CIR): 0 (0.00000%)
  Near-end loss (EIR): 0
  Near-end loss-ratio (EIR): 0 (0.00000%)
  Far-end loss (EIR): 0
  Far-end loss-ratio (EIR): 0 (0.00000%)
Last loss measurement statistics:
  Near-end (CIR): 0
  Far-end (CIR): 0
  Near-end (EIR): 0
  Far-end (EIR): 0

Operational Commands: Ethernet OAM Link Fault Management
**show oam ethernet link-fault-management**

**Syntax**

```
show oam ethernet link-fault-management
  <brief | detail>
  <interface-name>
```

**Release Information**

Command introduced in Junos OS Release 9.4 for EX Series switches.

**Description**

Displays Operation, Administration, and Maintenance (OAM) link fault management (LFM) information for Ethernet interfaces.

**Options**

- `brief | detail`—(Optional) Display the specified level of output.
- `interface-name`—(Optional) Display link fault management information for the specified Ethernet interface only.

**Required Privilege**

View

**Related Documentation**

- Example: Configuring Ethernet OAM Link Fault Management on EX Series Switches on page 3591
- Configuring Ethernet OAM Link Fault Management (CLI Procedure) on page 3616

**List of Sample Output**

- show oam ethernet link-fault-management brief on page 3911
- show oam ethernet link-fault-management detail on page 3911

**Output Fields**

Table 469 on page 3907 lists the output fields for the `show oam ethernet link-fault-management` command. Output fields are listed in the approximate order in which they appear.

**Table 469: show oam ethernet link-fault-management Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates the status of the established link.</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- Fail—A link fault condition exists.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Running—A link fault condition does not exist.</td>
<td></td>
</tr>
<tr>
<td>Discovery state</td>
<td>State of the discovery mechanism:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- Passive Wait</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Send Any</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Send Local Remote</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Send Local Remote Ok</td>
<td></td>
</tr>
<tr>
<td>Peer address</td>
<td>Address of the OAM peer.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 469: show oam ethernet link-fault-management Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flags</strong></td>
<td>Information about the interface.</td>
<td>All levels</td>
</tr>
<tr>
<td>• Remote-Stable</td>
<td>Indicates remote OAM client acknowledgment of, and satisfaction with local OAM state information. <strong>False</strong> indicates that remote DTE has either not seen or is unsatisfied with local state information. <strong>True</strong> indicates that remote DTE has seen and is satisfied with local state information.</td>
<td></td>
</tr>
<tr>
<td>• Local-Stable</td>
<td>Indicates local OAM client acknowledgment of, and satisfaction with remote OAM state information. <strong>False</strong> indicates that local DTE either has not seen or is unsatisfied with remote state information. <strong>True</strong> indicates that local DTE has seen and is satisfied with remote state information.</td>
<td></td>
</tr>
<tr>
<td>• Remote-State-Valid</td>
<td>Indicates the OAM client has received remote state information found within Local Information TLVs of received Information OAM PDUs. <strong>False</strong> indicates that OAM client has not seen remote state information. <strong>True</strong> indicates that the OAM client has seen remote state information.</td>
<td></td>
</tr>
<tr>
<td><strong>Remote loopback status</strong></td>
<td>Indicates the remote loopback status. An OAM entity can put its remote peer into loopback mode using the Loopback control OAM PDU. In loopback mode, every frame received is transmitted back on the same port (except for OAM PDUs, which are needed to maintain the OAM session).</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Remote entity information</strong></td>
<td>Remote entity information.</td>
<td>All levels</td>
</tr>
<tr>
<td>• Remote MUX action</td>
<td>Indicates the state of the multiplexer functions of the OAM sublayer. Device is forwarding non-OAM PDUs to the lower sublayer or discarding non-OAM PDUs.</td>
<td></td>
</tr>
<tr>
<td>• Remote parser action</td>
<td>Indicates the state of the parser function of the OAM sublayer. Device is forwarding non-OAM PDUs to higher sublayer, looping back non-OAM PDUs to the lower sublayer, or discarding non-OAM PDUs.</td>
<td></td>
</tr>
<tr>
<td>• Discovery mode</td>
<td>Indicates whether discovery mode is active or inactive.</td>
<td></td>
</tr>
<tr>
<td>• Unidirectional mode</td>
<td>Indicates the ability to operate a link in a unidirectional mode for diagnostic purposes.</td>
<td></td>
</tr>
<tr>
<td>• Remote loopback mode</td>
<td>Indicates whether remote loopback is supported or not supported.</td>
<td></td>
</tr>
<tr>
<td>• Link events</td>
<td>Indicates whether interpreting link events is supported or not supported on the remote peer.</td>
<td></td>
</tr>
<tr>
<td>• Variable requests</td>
<td>Indicates whether variable requests are supported or not supported. The Variable Request OAM PDU, is used to request one or more MIB variables from the remote peer.</td>
<td></td>
</tr>
</tbody>
</table>

**OAM Receive Statistics**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>The number of information PDUs received.</td>
<td>detail</td>
</tr>
<tr>
<td>Event</td>
<td>The number of loopback control PDUs received.</td>
<td>detail</td>
</tr>
<tr>
<td>Variable request</td>
<td>The number of variable request PDUs received.</td>
<td>detail</td>
</tr>
<tr>
<td>Variable response</td>
<td>The number of variable response PDUs received.</td>
<td>detail</td>
</tr>
<tr>
<td>Loopback control</td>
<td>The number of loopback control PDUs received.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Table 469: show oam ethernet link-fault-management Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization specific</strong></td>
<td>The number of vendor organization specific PDUs received.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td><strong>OAM Transmit Statistics</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information</td>
<td>The number of information PDUs transmitted.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Event</td>
<td>The number of event notification PDUs transmitted.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Variable request</td>
<td>The number of variable request PDUs transmitted.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Variable response</td>
<td>The number of variable response PDUs transmitted.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Loopback control</td>
<td>The number of loopback control PDUs transmitted.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Organization specific</td>
<td>The number of vendor organization specific PDUs transmitted.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td><strong>OAM Received Symbol Error Event information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>The number of symbol error event TLVs that have been received after the OAM sublayer was reset.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Window</td>
<td>The symbol error event window in the received PDU.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td></td>
<td>The protocol default value is the number of symbols that can be received in one second on the underlying physical layer.</td>
<td></td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of errored symbols in the period required for the event to be generated.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Errors in period</td>
<td>The number of symbol errors in the period reported in the received event PDU.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Total errors</td>
<td>The number of errored symbols that have been reported in received event TLVs after the OAM sublayer was reset. Symbol errors are coding symbol errors.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td><strong>OAM Received Frame Error Event Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>The number of errored frame event TLVs that have been received after the OAM sublayer was reset.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Window</td>
<td>The duration of the window in terms of the number of 100 ms period intervals.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of detected errored frames required for the event to be generated.</td>
<td><strong>detail</strong></td>
</tr>
<tr>
<td>Errors in period</td>
<td>The number of detected errored frames in the period.</td>
<td><strong>detail</strong></td>
</tr>
</tbody>
</table>
### Table 469: show oam ethernet link-fault-management Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total errors</strong></td>
<td>The number of errored frames that have been reported in received event TLVs after the OAM sublayer was reset.</td>
<td>detail</td>
</tr>
<tr>
<td></td>
<td>A frame error is any frame error on the underlying physical layer.</td>
<td></td>
</tr>
<tr>
<td><strong>OAM Received Frame Period Error Event Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>The number of frame seconds errors event TLVs that have been received after the OAM sublayer was reset.</td>
<td>detail</td>
</tr>
<tr>
<td>Window</td>
<td>The duration of the frame seconds window.</td>
<td>detail</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of frame seconds errors in the period.</td>
<td>detail</td>
</tr>
<tr>
<td>Errors in period</td>
<td>The number of frame seconds errors in the period.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Total errors</strong></td>
<td>The number of frame seconds errors that have been reported in received event TLVs after the OAM sublayer was reset.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>OAM Transmitted Symbol Error Event Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>The number of symbol error event TLVs that have been transmitted after the OAM sublayer was reset.</td>
<td>detail</td>
</tr>
<tr>
<td>Window</td>
<td>The symbol error event window in the transmitted PDU.</td>
<td>detail</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of errored symbols in the period required for the event to be generated.</td>
<td>detail</td>
</tr>
<tr>
<td>Errors in period</td>
<td>The number of symbol errors in the period reported in the transmitted event PDU.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Total errors</strong></td>
<td>The number of errored symbols reported in event TLVs that have been transmitted after the OAM sublayer was reset.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>OAM Transmitted Frame Error Event Information</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events</td>
<td>The number of errored frame event TLVs that have been transmitted after the OAM sublayer was reset.</td>
<td>detail</td>
</tr>
<tr>
<td>Window</td>
<td>The duration of the window in terms of the number of 100 ms period intervals.</td>
<td>detail</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of detected errored frames required for the event to be generated.</td>
<td>detail</td>
</tr>
<tr>
<td>Errors in period</td>
<td>The number of detected errored frames in the period.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Total errors</strong></td>
<td>The number of errored frames that have been detected after the OAM sublayer was reset.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Sample Output

```
show oam ethernet link-fault-management brief

user@host> show oam ethernet link-fault-management brief
Interface: ge-0/0/1
  Status: Running, Discovery state: Send Any
  Peer address: 00:90:69:72:2c:83
  Flags: Remote-Stable Remote-State-Valid Local-Stable 0x50
  Remote loopback status: Disabled on local port, Enabled on peer port
  Remote entity information:
    Remote MUX action: discarding, Remote parser action: loopback
    Discovery mode: active, Unidirectional mode: unsupported
    Remote loopback mode: supported, Link events: supported
    Variable requests: unsupported

show oam ethernet link-fault-management detail

user@host> show oam ethernet link-fault-management detail
Interface: ge-0/0/1
  Status: Running, Discovery state: Send Any
  Peer address: 00:90:69:0a:07:14
  Flags: Remote-Stable Remote-State-Valid Local-Stable 0x50
  OAM receive statistics:
    Information: 186365, Event: 0, Variable request: 0, Variable response: 0
    Loopback control: 0, Organization specific: 0
  OAM transmit statistics:
    Information: 186347, Event: 0, Variable request: 0, Variable response: 0
    Loopback control: 0, Organization specific: 0
  OAM received symbol error event information:
    Events: 0, Window: 0, Threshold: 0
    Errors in period: 0, Total errors: 0
  OAM received frame error event information:
    Events: 0, Window: 0, Threshold: 0
    Errors in period: 0, Total errors: 0
  OAM received frame period error event information:
    Events: 0, Window: 0, Threshold: 0
    Errors in period: 0, Total errors: 0
  OAM transmitted symbol error event information:
    Events: 0, Window: 0, Threshold: 1
    Errors in period: 0, Total errors: 0
  OAM transmitted frame error event information:
    Events: 0, Window: 0, Threshold: 1
    Errors in period: 0, Total errors: 0
  Remote entity information:
    Remote MUX action: forwarding, Remote parser action: forwarding
    Discovery mode: active, Unidirectional mode: unsupported
    Remote loopback mode: supported, Link events: supported
    Variable requests: unsupported
```

Operational Commands: Uplink Failure Detection
**show uplink-failure-detection**

**Syntax**

```
show uplink-failure-detection
<group group-name>
```

**Release Information**

Command introduced in Junos OS Release 11.1 for EX Series switches.

**Description**

Display information about the uplink-failure-detection group, the member interfaces, and their status.

**Options**

- `none`—Display information about all groups configured for uplink failure detection.
- `group group-name`—(Optional) Display information about the specified group only.

**Required Privilege**

```
view
```

**Related Documentation**

- Configuring Interfaces for Uplink Failure Detection (CLI Procedure) on page 3618

**List of Sample Output**

```
show uplink-failure-detection
```

```
Group             : group1
Uplink            :  ge-0/0/0*
Downlink          :  ge-0/0/1*
Failure Action    :  Inactive
```

**Output Fields**

Table 470 on page 3912 lists the output fields for the `show uplink-failure-detection` command. Output fields are listed in the approximate order in which they appear.

**Table 470: show uplink-failure-detection Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Uplink</td>
<td>The uplink interface or interfaces configured as link-to-monitor.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The asterisk (*) indicates that the link is up.</td>
</tr>
<tr>
<td>Downlink</td>
<td>The downlink interface or interfaces configured as link-to-disable.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The asterisk (*) indicates that the link is up.</td>
</tr>
<tr>
<td>Failure Action</td>
<td>Status of uplink failure detection:</td>
</tr>
<tr>
<td></td>
<td>• Active—The switch has detected an uplink failure and has brought the downlink down.</td>
</tr>
<tr>
<td></td>
<td>• Inactive—The uplink or uplinks are up.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
show uplink-failure-detection
```

```
user@switch> show uplink-failure-detection
Group            : group1
Uplink           : ge-0/0/0*
Downlink         : ge-0/0/1*
Failure Action   : Inactive
```
Group : group2
Uplink : ge-0/0/3.0
Downlink : ge-0/0/4.0
Failure Action : Active
Troubleshooting Port Mirroring Configuration Error Messages

Problem
In an analyzer configuration, if the VLAN to which mirrored traffic is sent contains more than one member interface, the following error message is displayed in the CLI when you commit the analyzer configuration and the commit fails:

```
Multiple interfaces cannot be configured as a member of Analyzer output VLAN <vlan name>
```

Solution
You must direct the mirrored traffic to a VLAN that has a single member interface. You can do this by completing either of these tasks:

- Reconfigure the existing VLAN to contain a single member interface. You can choose this method if you want to use the existing VLAN.
- Create a new VLAN with a single member interface and associate the VLAN with the analyzer.

To reconfigure the existing VLAN to contain only one member interface:

1. Remove member interfaces from the VLAN repeatedly by using either the `delete vlan` command or the `delete interface` command until the VLAN contains a single member interface:
   ```
   [edit]
   user@switch# delete vlan vlan-id interface interface-name
   ```
• [edit]
  user@switch# delete interface interface-name unit 0 family family-name vlan member vlan-id

2. (Optional) Confirm that the VLAN contains only one interface:

[edit]
user@switch# show vlans vlan-name
The output for this command must display only one interface.

To create a new VLAN with a single member interface:

1. Configure a VLAN to carry the mirrored traffic:

[edit]
user@switch# set vlans vlan-name

2. Associate an interface with the VLAN:

[edit]
user@switch# set interfaces interface-name unit logical-unit-number family family-name vlan members vlan-name

3. Associate the VLAN with the analyzer:

[edit ethernet-switching-options]
user@switch# set analyzer analyzer-name output vlan vlan-name

Related Documentation

• Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches

• Configuring Port Mirroring to Analyze Traffic (CLI Procedure)

• Configuring Port Mirroring to Analyze Traffic (J-Web Procedure) on page 3601

• Understanding Port Mirroring on EX Series Switches

Operational Commands
show pfe statistics bridge

Syntax

```
show pfe statistics bridge
<fpc slot>
```

Release Information
Command introduced in Junos OS Release 12.1 for EX Series switches.

Description
Display information about the number of packets discarded in the ingress pipeline of the Packet Forwarding Engine, packets discarded because of egress filtering or congestion filtering, number of control packets, and general counters for dropped packets. You can use this information to inform troubleshooting investigations.

Options
- **none**—Display bridge counter statistics for all Flexible PIC Concentrator (FPC) slots.
- **fpc slot**—(Optional) Display bridge counter statistics for a specific FPC slot.

Required Privilege
- **view**

Related Documentation
- Monitoring System Process Information on page 718
- Monitoring Switch Control Traffic on page 712
- List of Sample Output
  - show pfe statistics bridge (EX3200 and EX4200 Switches) on page 3918
  - show pfe statistics bridge (EX8200 Switches and EX8200 Virtual Chassis) on page 3919
  - show pfe statistics bridge fpc (EX8200 Switches and EX8200 Virtual Chassis) on page 3920
  - show pfe statistics bridge fpc (EX8200-40XS (40-port SFP+) Line Card) on page 3920

Output Fields
Table 443 on page 3804 lists the output fields for the `show pfe statistics bridge` command. Output fields are listed in the approximate order in which they appear.

Table 471: show pfe statistics bridge Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Counters</td>
<td>Information about ingress counters:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Received</strong> — Number of packets received by the bridge.</td>
</tr>
<tr>
<td></td>
<td>- <strong>VLAN Filtered</strong> — Number of packets discarded because of VLAN filtering.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Security Filtered</strong> — Number of packets discarded because of security filtering.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Other Discards</strong> — Number of packets dropped by the bridge for reasons other than VLAN or security filtering.</td>
</tr>
</tbody>
</table>
### Field Name | Field Description
--- | ---
**Egress Counters** | Information about egress counters:
- **Unicast**—Number of unicast packets transmitted.
- **Multicast**—Number of multicast packets transmitted.
- **Broadcast**—Number of broadcast packets transmitted.
- **Egress Filtered**—Number of egress-filtered packets (regardless of port, priority, or mode).
- **TailDrop**—Number of packets filtered because of egress queue congestion.
- **Forward Restrict**—Number of packets filtered because of egress forward restrictions.
- **Congestion Filtered**—Number of packets filtered because of transmit queue (TxQ) congestion.
- **Control Packets**—Number of control packets (sent to CPU, received from CPU, and sent to analyzer).

**Drop Counters** | Information about drop counters:
- **Drop Mode**—Count mode of the counter.
- **Drop Counter**—Counter value.

**General Counters** | Information about general counters:
- **Drop Mode**—Count mode of the counter.
- **Drop Counter**—Counter value.
- **Source Not Learnt**—Number of source addresses that were not learnt because of internal congestion.

**MUX PFE** | Information about multiplexer PFE for oversubscribed cards:
- **Drop Mode**—Count mode of the counter.
- **Drop Count**—Counter value.

### Sample Output

**show pfe statistics bridge (EX3200 and EX4200 Switches)**

```
user@switch> show pfe statistics bridge
Slot 0
PFE:                        0           1           2
---------------------------------------------------------------------
---- Ingress Counters ----
Received:                       0          52           0
VLAN Filtered:                  0           0           0
Security Filtered:              0           0           0
Other Discards:                 0           0           0
---- Egress Counters ----
Unicast:                        0         104          52
Multicast:                      0           0           0
Broadcast:                      0           0           0
Egress Filtered:                0           0           0
Congestion Filtered:            0           0           0
Control Packets:                5           0           0
---- General Counters ----
Drop Mode:                     0           0           0
```

---
show pfe statistics bridge (EX8200 Switches and EX8200 Virtual Chassis)

user@switch> show pfe statistics bridge
Slot 0
PFE: 0 1

--- Ingress Counters ----
Received: 946 48
VLAN Filtered: 0 0
Security Filtered: 0 0
Other Discards: 0 0

--- Egress Counters ----
Unicast: 0 0
Multicast: 0 0
Broadcast: 0 0
Egress Filtered: 0 0
TailDrop: 0 0
Forward Restrict: 0 0
Congestion Filtered: 0 0
Control Packets: 4103 896

--- Drop Counters ----
Drop Mode: 0 0
Drop Counter: 12528 2

Slot 1
PFE: 0 1

--- Ingress Counters ----
Received: 0 0
VLAN Filtered: 0 0
Security Filtered: 0 0
Other Discards: 0 0

--- Egress Counters ----
Unicast: 0 0
Multicast: 0 0
Broadcast: 0 0
Egress Filtered: 0 0
TailDrop: 0 0
Forward Restrict: 0 0
Congestion Filtered: 0 0
Control Packets: 0 0

--- Drop Counters ----
Drop Mode: 0 0
Drop Counter: 0 0

Slot 2
PFE: 0 1

--- Ingress Counters ----
Received: 0 0
VLAN Filtered: 0 0
Security Filtered: 0 0
Other Discards: 0 0

--- Egress Counters ----
Unicast: 0 0
Multicast: 0 0
<table>
<thead>
<tr>
<th>Counters</th>
<th>Slot 2</th>
<th>Slot 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Egress Filtered:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TailDrop:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Forward Restrict:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Congestion Filtered:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Control Packets:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drop Counters</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drop Mode:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Drop Counter:</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**show pfe statistics bridge fpc (EX8200 Switches and EX8200 Virtual Chassis)**

```plaintext
user@switch> show pfe statistics bridge fpc 2
Slot 2
PFE:                        0           1

----- Ingress Counters -----
Received:                0           0
VLAN Filtered:           0           0
Security Filtered:       0           0
Other Discards:          0           0

----- Egress Counters -----
Unicast:                 0           0
Multicast:               0           0
Broadcast:               0           0
Egress Filtered:         0           0
TailDrop:                0           0
Forward Restrict:        0           0
Congestion Filtered:     0           0
Control Packets:         0           0

----- Drop Counters -----
Drop Mode:               0           0
Drop Counter:            0           0
```

**show pfe statistics bridge fpc (EX8200-40XS (40-port SFP+) Line Card)**

```plaintext
user@switch> show pfe statistics bridge fpc 8
Slot 8
PFE:                        0           1           2           3

----- Ingress Counters -----
Received:                0           3           0           0
VLAN Filtered:           0           0           0           0
Security Filtered:       0           0           0           0
Other Discards:          0           1           0           0

----- Egress Counters -----
Unicast:                 0           0           0           0
Multicast:               0           0           0           0
Broadcast:               0           0           0           0
Egress Filtered:         0           0           0           0
TailDrop:                0           0           0           0
Forward Restrict:        0           0           0           0
Congestion Filtered:     0           2           0           0
Control Packets:         4           0           0           0

----- Drop Counters -----
Drop Mode:               0           0           0           0
Drop Counter:            0           1           0           0

MUX PFE:                    4           5
```
<table>
<thead>
<tr>
<th>Drop Mode:</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop Count:</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
PART 23

PoE

- Overview on page 3925
- Configuration on page 3935
- Administration on page 3967
- Troubleshooting Procedures on page 3991
CHAPTER 70

Overview

- Power over Ethernet Overview on page 3925

Power over Ethernet Overview

- Understanding PoE on EX Series Switches on page 3925

Understanding PoE on EX Series Switches

Power over Ethernet (PoE) permits electric power, along with data, to be passed over a copper Ethernet LAN cable. Powered devices—such as voice over IP (VoIP) telephones, wireless access points, video cameras, and point-of-sale devices—that support PoE can receive power safely from the same access ports that are used to connect personal computers to the network.

This topic describes PoE on Juniper Networks EX Series Ethernet Switches:

- PoE, PoE+, and Enhanced PoE on page 3925
- PoE Power Allocation on page 3927

PoE, PoE+, and Enhanced PoE

PoE was first defined in the IEEE 802.3af standard. In this standard, the amount of power that can be supplied to a powered device is limited to 15.4 W. A later standard, IEEE 802.3at, defined PoE+, which increases the amount of power to 30 W. The PoE+ standard provides support for legacy PoE devices—an IEEE 802.3af powered device can operate normally when connected to IEEE 802.3at (PoE+) power sourcing equipment.

Beginning in Juniper Networks Junos operating system (Junos OS) Release 11.1, Juniper Networks provides enhanced PoE on EX3200 and EX4200 switches. Enhanced PoE is a Juniper Networks extension to the IEEE 802.3af standard that allows power of up to 18.6 W per PoE port.

Table 472 on page 3926 lists EX Series switches and line cards and the version of PoE they support.
Table 472: PoE Version Support

<table>
<thead>
<tr>
<th>Switch or Line Card</th>
<th>PoE Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200 switch</td>
<td>PoE+ (IEEE 802.3at)</td>
</tr>
<tr>
<td>(EX2200-C-12P-2G, EX2200-24P-4G, EX2200-48P-4G models)</td>
<td></td>
</tr>
<tr>
<td>NOTE: Starting with Junos OS Release 12.2R1, PoE commands are enabled on all non-PoE-capable EX2200 switch models. The PoE commands do not provide any meaningful information on standalone non-PoE-capable switch models. However, in an EX2200 Virtual Chassis, you can execute PoE commands from a non-PoE-capable master switch to configure PoE on PoE-capable Virtual Chassis members.</td>
<td></td>
</tr>
<tr>
<td>EX3200 switch</td>
<td>Enhanced PoE</td>
</tr>
<tr>
<td>EX3300 switch</td>
<td>PoE+ (IEEE 802.3at)</td>
</tr>
<tr>
<td>(EX3300-24P, EX3300-48P models)</td>
<td></td>
</tr>
<tr>
<td>EX4200 switch—P and T models</td>
<td>Enhanced PoE</td>
</tr>
<tr>
<td>EX4200 switch—PX models</td>
<td>PoE+ (IEEE 802.3at)</td>
</tr>
<tr>
<td>(EX4200-24PX and EX4200-48PX)</td>
<td></td>
</tr>
<tr>
<td>EX4300 switch</td>
<td>PoE+ (IEEE 802.3at)</td>
</tr>
<tr>
<td>(EX4300-24P and EX4300-48P)</td>
<td></td>
</tr>
<tr>
<td>EX6200-48P (48-port PoE+) line card</td>
<td>PoE+ (IEEE 802.3at)</td>
</tr>
<tr>
<td>EX8200-2XS-40P (40-port PoE+ with 4-port SFP and 2-port SFP+) line card</td>
<td>PoE+ (IEEE 802.3at)—Ports 0 through 11, and PoE (IEEE 802.3af)—remaining PoE ports.</td>
</tr>
<tr>
<td>EX8200-48PL (2-port SFP+ and 48-port PoE+ 20 Gbps) line card</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: This topic and its related topics use the term PoE as a generic term to refer to PoE, PoE+, and enhanced PoE.
PoE Power Allocation

A switch or line card that supports PoE has a PoE controller that keeps track of the PoE power consumption on the switch or line card, and allocates power to the PoE ports. The following factors determine how the PoE controller allocates power to the PoE ports:

- PoE Power Budget on page 3927
- PoE Interface Power Allocation on page 3931
- PoE Interface Power Priority on page 3933

PoE Power Budget

The PoE power budget is the total amount of power available for the PoE controller to allocate to the PoE ports. The PoE controller cannot exceed its PoE power budget and does not allocate power to a PoE port if the allocation would exceed the PoE power budget.

How the PoE power budget is determined depends on the switch model:

- PoE Power Budget on EX2200, EX3200, EX3300, EX4200, and EX4300 Switches on page 3927
- PoE Power Budget on EX6200 and EX8200 Switches on page 3930

PoE Power Budget on EX2200, EX3200, EX3300, EX4200, and EX4300 Switches

The PoE power budget on EX2200, EX3200, EX3300, EX4200, and EX4300 switches depends on the switch model and the capacities of the power supplies installed. To find the PoE power budget for each switch model, see Table 473 on page 3928 for EX2200 switch models, Table 474 on page 3928 for EX3200 switch models, Table 475 on page 3928 for EX3300 switch models, Table 476 on page 3929 for EX4200 switch models, and Table 477 on page 3929 for EX4300 switch models.

Use the `show poe controller` command to display a switch’s PoE power budget.

If your switch supports power supplies of different capacities, keep the following points in mind:

- If you change your existing power supply to a lower-capacity power supply, the PoE power budget might no longer be sufficient to power all the PoE ports on the switch.
- If your switch supports redundant power supplies and you have installed power supplies of different capacities, the PoE power budget is based on the wattage of the lower-capacity power supply.
- You cannot increase the number of PoE-capable ports on a switch by installing a power supply that has a higher capacity.

Table 473 on page 3928 lists the EX2200 switch models, number of PoE-enabled ports, power supply ratings, and PoE power budgets.
<table>
<thead>
<tr>
<th>Switch Model Number</th>
<th>Number of PoE-Enabled Ports</th>
<th>Power Supply Rating</th>
<th>PoE Power Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200-C-12T</td>
<td>–</td>
<td>30 W</td>
<td>–</td>
</tr>
<tr>
<td>EX2200-C-12P</td>
<td>12</td>
<td>180 W</td>
<td>100 W</td>
</tr>
<tr>
<td>EX2200-24T</td>
<td>–</td>
<td>75 W</td>
<td>–</td>
</tr>
<tr>
<td>EX2200-24P</td>
<td>24</td>
<td>550 W</td>
<td>405 W</td>
</tr>
<tr>
<td>EX2200-24T-DC</td>
<td>–</td>
<td>100 W</td>
<td>–</td>
</tr>
<tr>
<td>EX2200-48T</td>
<td>–</td>
<td>75 W</td>
<td>–</td>
</tr>
<tr>
<td>EX2200-48P</td>
<td>48</td>
<td>550 W</td>
<td>405 W</td>
</tr>
</tbody>
</table>

Table 474 on page 3928 lists the EX3200 switch models, number of PoE-enabled ports, power supply ratings, and PoE power budgets.

<table>
<thead>
<tr>
<th>Switch Model Number</th>
<th>Number of PoE-Enabled Ports</th>
<th>Power Supply Rating</th>
<th>PoE Power Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3200-24T</td>
<td>8</td>
<td>320 W</td>
<td>130 W</td>
</tr>
<tr>
<td>EX3200-48T</td>
<td>8</td>
<td>320 W</td>
<td>130 W</td>
</tr>
<tr>
<td>EX3200-24P</td>
<td>24</td>
<td>600 W</td>
<td>410 W</td>
</tr>
<tr>
<td>EX3200-48P</td>
<td>48</td>
<td>930 W</td>
<td>740 W</td>
</tr>
</tbody>
</table>

Table 475 on page 3928 lists the EX3300 switch models, number of PoE-enabled ports, power supply ratings, and PoE power budgets.

<table>
<thead>
<tr>
<th>Switch Model Number</th>
<th>Number of PoE-Enabled Ports</th>
<th>Power Supply Rating</th>
<th>PoE Power Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3300-24T</td>
<td>–</td>
<td>100 W</td>
<td>–</td>
</tr>
<tr>
<td>EX3300-24P</td>
<td>24</td>
<td>550 W</td>
<td>405 W</td>
</tr>
<tr>
<td>EX3300-24T-DC</td>
<td>–</td>
<td>100 W</td>
<td>–</td>
</tr>
<tr>
<td>EX3300-48T</td>
<td>–</td>
<td>100 W</td>
<td>–</td>
</tr>
<tr>
<td>EX3300-48T-BF</td>
<td>–</td>
<td>100 W</td>
<td>–</td>
</tr>
</tbody>
</table>
Table 475: PoE Power Budget EX3300 Switch Models *(continued)*

<table>
<thead>
<tr>
<th>Switch Model Number</th>
<th>Number of PoE-Enabled Ports</th>
<th>Power Supply Rating</th>
<th>PoE Power Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3300-48P</td>
<td>48</td>
<td>900 W</td>
<td>740 W</td>
</tr>
</tbody>
</table>

Table 476 on page 3929 lists the EX4200 switch models, number of PoE-enabled ports, power supply ratings, and PoE power budgets.

Table 476: PoE Power Budget for EX4200 Switch Models

<table>
<thead>
<tr>
<th>Switch Model Number</th>
<th>Number of PoE-Enabled Ports</th>
<th>Power Supply Rating</th>
<th>PoE Power Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX4200-24T</td>
<td>8</td>
<td>320 W</td>
<td>130 W</td>
</tr>
<tr>
<td>EX4200-48T</td>
<td>8</td>
<td>320 W</td>
<td>130 W</td>
</tr>
<tr>
<td>EX4200-24P</td>
<td>24</td>
<td>600 W</td>
<td>410 W</td>
</tr>
<tr>
<td>EX4200-48P</td>
<td>48</td>
<td>930 W</td>
<td>740 W</td>
</tr>
<tr>
<td>EX4200-24PX</td>
<td>24</td>
<td>930 W</td>
<td>740 W</td>
</tr>
<tr>
<td>EX4200-48PX</td>
<td>48</td>
<td>930 W</td>
<td>740 W</td>
</tr>
</tbody>
</table>

Table 477 on page 3929 lists the EX4300 switch models, number of PoE-enabled ports, power supply ratings, and PoE power budgets.

Table 477: PoE Power Budget for EX4300 Switch Models

<table>
<thead>
<tr>
<th>Switch Model Number</th>
<th>Number of PoE-Enabled Ports</th>
<th>Power Supply Rating</th>
<th>PoE Power Budget</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX4300-48P</td>
<td>48</td>
<td>1100 W</td>
<td>900 W</td>
</tr>
<tr>
<td>EX4300-48T</td>
<td>0</td>
<td>350 W</td>
<td>-</td>
</tr>
<tr>
<td>EX4300-48T-AFI</td>
<td>0</td>
<td>350 W</td>
<td>-</td>
</tr>
<tr>
<td>EX4300-24P</td>
<td>0</td>
<td>715 W</td>
<td>550 W</td>
</tr>
<tr>
<td>EX4300-24T</td>
<td>24</td>
<td>350 W</td>
<td>-</td>
</tr>
<tr>
<td>EX4300-48T-DC</td>
<td>0</td>
<td>550 W</td>
<td>-</td>
</tr>
<tr>
<td>EX4300-48T-DC-AFI</td>
<td>0</td>
<td>550 W</td>
<td>-</td>
</tr>
</tbody>
</table>
**PoE Power Budget on EX6200 and EX8200 Switches**

For EX6200 and EX8200 switches, each line card that supports PoE has its own PoE controller and PoE power budget. The PoE power budget is allocated to the line card by the switch's power management, while PoE power is allocated to the ports on the line card by the PoE controller. Because EX6200 and EX8200 switches can differ in the number and capacity of power supplies installed and in the number and types of line cards installed, the amount of power available for PoE power can vary for different switches of the same model.

Power management allocates PoE power to line cards that support PoE only after it has allocated base power to and powered on all line cards. It then allocates the remaining power to the PoE power budgets of PoE line cards in order of line card power priority. (In a default configuration, power priority is determined by the line card slot number, with slot 0 having the highest priority.) If the remaining power is insufficient to provide PoE power to all PoE line cards, a low-priority line card might receive no PoE power or partial PoE power.

By default, power management allocates enough PoE power to a line card to power all PoE ports at their maximum supported power. If the powered devices connected to that line card require less power than that, you can configure a smaller PoE power budget for the line card. For example, power management normally allocates 915 W of PoE power to a 48-port PoE+ 20 Gbps (EX8200-48PL) line card. If the powered devices connected to that line card consume no more than a total of 250 W, you can set the PoE power budget for the line card to 250 W. Doing so frees up 665 W, which then can be used to fulfill the PoE power needs of lower-priority line cards.

You can also configure the power priority of the PoE ports on a line card. If power management is unable to allocate enough power to a line card to meet its PoE power budget, the line card PoE controller will turn off power to PoE ports in reverse priority order as required to meet the reduced power allocation.

Power management adjusts PoE power allocations as power availability and demand in a switch changes. As a general rule, power management allocates power to power on line cards before it allocates PoE power. For example, if you add a line card and there is insufficient power available to power it on, power management reduces the PoE power it provides to line cards, starting with the lowest priority line card, until it frees up enough power to power on the new line card. When power management reduces the PoE power budget for a line card because of insufficient power, it logs a message in the system log.

Note that the actual power consumed by the powered devices does not affect power management's power allocation for a line card. If you have set the PoE budget for a line card to 500 W, power management allocates 500 W even if the powered devices are consuming less power than that. Similarly, the PoE power budget is not increased if you add additional powered devices: if the powered devices require more than the 500 W PoE budget that you have configured, lower-priority devices do not receive power.

You can display the switch's power budget maintained by power management, including its PoE power allocations, by using the `show chassis power-budget-statistics` command. You can also display the PoE power budget for each line card in a switch by using the `show poe controller` command.
For more information about how power management allocates power, including PoE power, see “Understanding Power Management on EX Series Switches” on page 2213.

**PoE Interface Power Allocation**

You can configure how the switch determines the maximum power for a PoE interface and how power is allocated to the PoE interfaces. If the power consumption of a powered device exceeds the maximum power allocated to the interface, the switch turns off power to the interface.

These PoE power allocation methods are available:

- LLDP Power Negotiation on page 3931
- Class PoE Management Mode on page 3931
- Static PoE Management Mode on page 3932

**LLDP Power Negotiation**

Link Layer Discovery Protocol (LLDP) power negotiation allows the PoE controller to dynamically allocate power to LLDP-enabled powered devices based on their power needs. The PoE controller allocates to an interface only the power currently required by the connected powered device, and it can allocate the power in small increments.

When the PoE management mode is set to **class** and LLDP is enabled (both are default settings), LLDP power negotiation is enabled by default. If you disable LLDP power negotiation or the powered device does not support it, the switch uses the class of the powered device to determine the maximum power for interfaces.

**NOTE:** LLDP power negotiation is not supported on EX3200 and EX4200 (except EX4200 PX models) switches.

**Class PoE Management Mode**

In **class** PoE management mode, the maximum power for an interface is determined by the class of the connected powered device. Table 478 on page 3931 lists the classes of powered devices and associated power levels.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Class</th>
<th>Maximum Power Delivered by PoE Port</th>
<th>Power Range of Powered Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.3af (PoE) and IEEE 802.3at (PoE+)</td>
<td>0</td>
<td>15.4 W</td>
<td>0.44 through 12.95 W</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>4.0 W</td>
<td>0.44 through 3.84 W</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>7.0 W</td>
<td>3.84 through 6.49 W</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>15.4 W</td>
<td>6.49 through 12.95 W</td>
</tr>
<tr>
<td>IEEE 802.3at (PoE+)</td>
<td>4</td>
<td>30.0 W</td>
<td>12.95 through 25.5 W</td>
</tr>
</tbody>
</table>
Because of line loss, the power range of the powered device is less than the maximum power delivered at the PoE port for each class. Line loss is influenced by cable length, quality, and other factors and is typically less than 16 percent of the maximum power.

The powered device communicates to the PoE controller which class it belongs to when it is connected. The PoE controller then allocates to the interface the maximum power required by the class (see Table 478 on page 3931). It does not allocate power to an interface until a powered device is connected. Class 0 is the default class for powered devices that do not provide class information. Class 4 powered devices are supported only by PoE ports that support IEEE 802.3at (PoE+).

By default, when class PoE management mode and LLDP are enabled, LLDP power negotiation is also enabled on supported switches. See “LLDP Power Negotiation” on page 3931 for more information.

**Static PoE Management Mode**

In the static PoE management mode, you specify the maximum power for each PoE interface. The PoE controller then allocates this amount of power to the interface from its total budget. For example, if you specify a maximum value of 8.0 W for ge-0/0/3, the PoE controller allocates 8.0 W out of its total power budget for this interface. This amount is allocated to the interface whether or not a powered device is connected to the interface or whether the connected powered device uses less power than 8.0 W.

Because of line loss, the power received by the powered device can be less than the power available at the PoE port. Table 479 on page 3932 shows the maximum power available at a PoE port and the resulting power guaranteed to the powered device.

**Table 479: Maximum Power Per Port in Static Mode**

<table>
<thead>
<tr>
<th>Switch or Line Card</th>
<th>Maximum Power Delivered by PoE Port</th>
<th>Guaranteed Power to Powered Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200 switches, EX3300 switches, EX4200 PX model switches, and EX4300 switches</td>
<td>30 W</td>
<td>25.5 W</td>
</tr>
<tr>
<td>EX3200 switches and EX4200 P and T model switches running Junos OS Release 10.4 or earlier</td>
<td>15.4 W</td>
<td>12.95 W</td>
</tr>
<tr>
<td>EX3200 switches and EX4200 P and T model switches running Junos OS Release 11.1 or later</td>
<td>18.6 W</td>
<td>15.64 W</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Switches that are upgraded to Junos OS Release 11.1 from a previous release require an upgrade of the PoE controller software to obtain 18.6 W.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX6200-48P line cards</td>
<td>30 W</td>
<td>25.5 W</td>
</tr>
<tr>
<td>EX8200-2XS-40P line cards and EX8200-48PL line cards</td>
<td>30 W (ports 0 through 11)</td>
<td>25.5 W</td>
</tr>
<tr>
<td></td>
<td>15.4 W (remaining PoE ports)</td>
<td>12.95 W</td>
</tr>
</tbody>
</table>
**PoE Interface Power Priority**

You can configure a PoE interface to have either a high or a low power priority. The power priority determines which interfaces receive power if PoE power demands are greater than the PoE power budget. If the total power allocated for all interfaces exceeds the switch budget, PoE power to lower-priority interfaces is turned off and the power allocated to those interfaces drops to 0. Thus you must set interfaces that connect to critical powered devices, such as security cameras and emergency phones, to high priority.

Among PoE interfaces that have the same assigned priority, power priority is determined by the port number, with lower-numbered ports having higher priority.

For EX6200 and EX8200 switches, interface power priority determines the relative priority of the interfaces on a line card, not on the switch as a whole. The relative priority of interfaces residing on different line cards is determined by line card priority. For example, if line card 1 has a higher power priority than line card 2 and a power shortage occurs, power is removed from the PoE interfaces in this order:

- Low-priority interfaces on line card 2
- High-priority interfaces on line card 2
- Low-priority interfaces on line card 1
- High-priority interfaces on line card 1

You can manually configure PoE interface power priority, or you can enable LLDP power priority, which assigns each interface the power priority provided by the connected LLDP-enabled powered device. Table 480 on page 3933 describes how the switch converts LLDP power priorities to switch power priorities.

### Table 480: LLDP Power Priority Conversion

<table>
<thead>
<tr>
<th>LLDP Power Priority</th>
<th>Switch Power Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical, High</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

**NOTE:** LLDP power priority requires LLDP power negotiation to be enabled, which is enabled by default when the PoE management option is set to class.

**NOTE:** LLDP power priority is not supported on EX3200 and EX4200 (except EX4200 PX model) switches.

**Related Documentation**

- Example: Configuring PoE Interfaces on an EX Series Switch on page 3935
- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
• Example: Configuring PoE on an EX6200 or EX8200 Switch
• Upgrading the PoE Controller Software on page 3967
Power over Ethernet (PoE) ports supply electric power over the same ports that are used to connect network devices and allow you to plug in devices that require both network connectivity and electric power, such as voice over IP (VoIP) phones, wireless access points, and some IP cameras.

You do not need to configure PoE unless you wish to modify the default values or disable PoE on a specific interface.

This example describes a default configuration of PoE interfaces on an EX Series switch:

- Requirements on page 3935
- Overview and Topology on page 3936
- Configuration on page 3936
- Verification on page 3937

Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch that supports PoE

Before you configure PoE, be sure you have:
• Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure) or Connecting and Configuring an EX Series Switch (J-Web Procedure) for details.

Overview and Topology

The topology used in this example consists of a switch that has 24 ports. Eight of the ports support PoE (IEEE 802.3af), which means they provide both network connectivity and electric power for powered devices such as VoIP telephones, wireless access points, and IP security cameras that require 12.95 W or less. The remaining 16 ports provide only network connectivity. You use the standard ports to connect devices that have their own power sources, such as desktop and laptop computers, printers, and servers. Table 481 on page 3936 details the topology used in this configuration example.

Table 481: Components of the PoE Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>EX Series switch with 24 Gigabit Ethernet ports: 8 PoE interfaces (ge-0/0/0 through ge-0/0/7) and 16 non-PoE interfaces (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
<tr>
<td>Connection to a wireless access point (requires PoE)</td>
<td>ge-0/0/0</td>
</tr>
<tr>
<td>Connections to Avaya IP telephones with integrated hubs that allow phone and desktop PC to connect to a single port (requires PoE)</td>
<td>ge-0/0/1 through ge-0/0/7</td>
</tr>
<tr>
<td>Direct connections to desktop PCs, file servers, integrated printer/fax/copier machines (no PoE required)</td>
<td>ge-0/0/8 through ge-0/0/20</td>
</tr>
<tr>
<td>Unused ports (for future expansion)</td>
<td>ge-0/0/21 through ge-0/0/23</td>
</tr>
</tbody>
</table>

Configuration

To enable the default PoE configuration on the switch:

CLI Quick Configuration

To quickly enable the default configuration on the switch:

Simply connect the powered devices to the PoE ports.

Step-by-Step Procedure

To use the PoE interfaces with default values:

1. Make sure the switch is powered on.
2. Connect the wireless access point to interface ge-0/0/0.
3. Connect the Avaya phones to interfaces ge-0/0/1 through ge-0/0/7.
### Verification

To verify that PoE interfaces have been created and are operational, perform this task:

- **Verifying That the PoE Interfaces Have Been Created on page 3937**

### Purpose

Verify that the PoE interfaces have been created on the switch.

### Action

List all the PoE interfaces configured on the switch:

```bash
user@switch> show poe interface
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>7.9W</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
</tr>
</tbody>
</table>

### Meaning

The `show poe interface` command lists PoE interfaces configured on the switch, with their status, priority, power consumption, and class. This output shows that eight interfaces have been created with default values and are consuming power at the expected rates.

### Related Documentation

- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Configuring PoE (CLI Procedure) on page 3942
- Troubleshooting PoE Interfaces on page 3991

### Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch

Power over Ethernet (PoE) ports supply electric power over the same ports that are used to connect network devices. These ports allow you to plug in devices that need both network connectivity and electric power, such as voice over IP (VoIP) phones, wireless access points, and some IP cameras.

By default, PoE ports on EX Series switches are set to low power priority. You can configure a PoE port to have a high power priority setting. If a situation arises where there is not sufficient power for all the PoE ports, the available power is directed to the higher priority ports, while power to the lower priority ports is shut down as needed. Thus you should set ports that connect to security cameras, emergency phones, and other high priority powered devices to high priority.

This example describes how to configure a few high priority PoE interfaces.

- Requirements on page 3938
- Overview and Topology on page 3938
Requirements

This example uses the following software and hardware components:

- Junos OS Release 9.0 or later for EX Series switches
- One EX Series switch that supports PoE

Before you configure PoE, be sure you have:

- Performed the initial switch configuration. See Connecting and Configuring an EX Series Switch (CLI Procedure) or Connecting and Configuring an EX Series Switch (J-Web Procedure) for details.

Overview and Topology

The topology used in this example consists of a switch that has 24 ports. Eight of the ports support PoE (IEEE 802.3af), which means they provide both network connectivity and electric power for powered devices such as VoIP telephones, wireless access points, and IP security cameras that require 12.95 W or less. The remaining 16 ports provide only network connectivity. You use the standard ports to connect devices that have their own power sources, such as desktop and laptop computers, printers, and servers.

Table 482 on page 3938 details the topology used in this configuration example.

Table 482: Components of the PoE Configuration Topology

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>Switch with 24 Gigabit Ethernet ports: 8 PoE interfaces (ge-0/0/0 through ge-0/0/7) and 16 non-PoE interfaces (ge-0/0/8 through ge-0/0/23)</td>
</tr>
<tr>
<td>VLAN name</td>
<td>default</td>
</tr>
<tr>
<td>Connection to a wireless access point (requires PoE)</td>
<td>ge-0/0/0</td>
</tr>
<tr>
<td>Security IP Cameras (require PoE)</td>
<td>ge-0/0/1 and ge-0/0/2 high</td>
</tr>
<tr>
<td>Emergency VoIP phone (requires PoE)</td>
<td>ge-0/0/3 high</td>
</tr>
<tr>
<td>VoIP phone in Executive Office (requires PoE)</td>
<td>ge-0/0/4 high</td>
</tr>
<tr>
<td>Other VoIP phones (require PoE)</td>
<td>ge-0/0/5 through ge-0/0/7</td>
</tr>
<tr>
<td>Direct connections to desktop PCs, file servers, integrated printer/fax/copier machines (no PoE required)</td>
<td>ge-0/0/8 through ge-0/0/20</td>
</tr>
<tr>
<td>Unused ports (for future expansion)</td>
<td>ge-0/0/21 through ge-0/0/23</td>
</tr>
</tbody>
</table>
Configuration

To configure PoE interfaces:

**CLI Quick Configuration**

By default, PoE interfaces are created for all PoE ports and PoE is enabled. The default priority for PoE interfaces is low.

To quickly set some interfaces to high priority and to include descriptions of the interfaces, copy the following commands and paste them into the switch terminal window:

```bash
[edit]
set poeinterface ge-0/0/1 priority high telemetries
set poeinterface ge-0/0/2 priority high telemetries
set poeinterface ge-0/0/3 priority high telemetries
set poeinterface ge-0/0/4 priority high telemetries
set interfaces ge-0/0/0 description "wireless access point"
set interfaces ge-0/0/1 description "security camera front door"
set interfaces ge-0/0/2 description "security camera back door"
set interfaces ge-0/0/3 description "emergency phone"
set interfaces ge-0/0/4 description "Executive Office VoIP phone"
set interfaces ge-0/0/5 description "staff VoIP phone"
set interfaces ge-0/0/6 description "staff VoIP phone"
set interfaces ge-0/0/7 description "staff VoIP phone"
```

**Step-by-Step Procedure**

To configure PoE interfaces with different priorities:

1. Set the interfaces connected to high priority powered devices to high priority. Include the telemetries statement for the high priority interfaces, thus enabling the logging of power consumption on those interfaces:

   ```bash
   [edit poe]
   user@switch# set interface ge-0/0/1 priority high telemetries
   user@switch# set interface ge-0/0/2 priority high telemetries
   user@switch# set interface ge-0/0/3 priority high telemetries
   user@switch# set interface ge-0/0/4 priority high telemetries
   ```

2. Provide descriptions for the PoE interfaces:

   ```bash
   [edit interfaces]
   user@switch# set ge-0/0/0 description "wireless access point"
   user@switch# set ge-0/0/1 description "security camera front door"
   user@switch# set ge-0/0/2 description "security camera back door"
   user@switch# set ge-0/0/3 description "emergency phone"
   user@switch# set ge-0/0/4 description "Executive Office VoIP phone"
   user@switch# set ge-0/0/5 description "staff VoIP phone"
   user@switch# set ge-0/0/6 description "staff VoIP phone"
   user@switch# set ge-0/0/7 description "staff VoIP phone"
   ```

3. Connect the wireless access point to interface ge-0/0/0. This interface uses the default PoE settings.

4. Connect the two security cameras to interfaces ge-0/0/1 and ge-0/0/2. These interfaces are set to high priority with telemetries enabled.

5. Connect the emergency VoIP phone to interface ge-0/0/3. This interface is set to high priority with telemetries enabled.
6. Connect the Executive Office VoIP phone to interface **ge-0/0/4**. This interface is set to high priority with telemetries enabled.

7. Connect the staff VoIP phones to **ge-0/0/5**, **ge-0/0/6**, and **ge-0/0/7**. These interfaces use the default PoE settings.

**Results**

Check the results of the configuration:

```
[edit]
user@switch# show interfaces { 
  ge-0/0/0 { 
    description "wireless access point"; 
    unit 0 { 
      family ethernet-switching; 
    } 
  } 
  ge-0/0/1 { 
    description "security camera front door"; 
    unit 0 { 
      family ethernet-switching; 
    } 
  } 
  ge-0/0/2 { 
    description "security camera back door"; 
    unit 0 { 
      family ethernet-switching; 
    } 
  } 
  ge-0/0/3 { 
    description "emergency phone"; 
    unit 0 { 
      family ethernet-switching; 
    } 
  } 
  ge-0/0/4 { 
    description "Executive Office VoIP phone"; 
    unit 0 { 
      family ethernet-switching; 
    } 
  } 
  ge-0/0/5 { 
    description "staff VoIP phone"; 
    unit 0 { 
      family ethernet-switching; 
    } 
  } 
  ge-0/0/6 { 
    description "staff VoIP phone"; 
    unit 0 { 
      family ethernet-switching; 
    } 
  } 
```
ge-0/0/7 {
    description "staff VoIP phone";
    unit 0 {
        family ethernet-switching;
    }
}
}
poe {
    interface all;
    interface ge-0/0/1 {
        priority high;
        telemetries;
    }
    interface ge-0/0/2 {
        priority high;
        telemetries;
    }
    interface ge-0/0/3 {
        priority high;
        telemetries;
    }
    interface ge-0/0/4 {
        priority high;
        telemetries;
    }
}

Verification

To verify that PoE interfaces have been created and are operational, perform the following tasks:

- Verifying That the PoE Interfaces Have Been Created with the Correct Priorities on page 3941

Verifying That the PoE Interfaces Have Been Created with the Correct Priorities

Purpose

Verify that the PoE interfaces on the switch are now set to the correct priority settings.

Action

List all the PoE interfaces configured on the switch:

```
user@switch> show poe interface
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>7.9W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>High</td>
<td>4.8W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>High</td>
<td>4.8W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>High</td>
<td>3.3W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>High</td>
<td>4.7W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.2W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.3W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/7</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>3.3W</td>
<td>2</td>
</tr>
</tbody>
</table>

Meaning

The `show poe interface` command lists PoE interfaces configured on the switch, with their status, priority, power consumption, and class. This output shows that eight PoE interfaces
are enabled. Interfaces ge-0/0/1 through ge-0/0/4 are configured as priority high. The remaining PoE interfaces are configured with the default priority value of low.

Related Documentation
- Example: Configuring PoE Interfaces on an EX Series Switch on page 3935
- Configuring PoE (CLI Procedure) on page 3942
- Troubleshooting PoE Interfaces on page 3991

Configuration Tasks
- Configuring PoE (CLI Procedure) on page 3942
- Configuring PoE (J-Web Procedure) on page 3948

Configuring PoE (CLI Procedure)

Power over Ethernet (PoE) ports on EX Series switches supply electric power over the same ports that are used to connect network devices. These ports allow you to plug in devices that require both network connectivity and electric power, such as voice over IP (VoIP) phones, wireless access points, and some IP cameras.

This topic describes:
- PoE Configurable Options on page 3942
- Configuring the PoE Controller on EX2200, EX3200, EX3300, EX4200, and EX4300 Switches on page 3945
- Configuring the PoE Controllers on EX6200 and EX8200 Switches on page 3946
- Configuring PoE Interfaces on page 3947

PoE Configurable Options

For EX Series switches that support PoE ports, the factory default configuration enables PoE on the PoE-capable ports, with default settings in effect. You might not have to do any additional configuration if the default settings work for you. Table 483 on page 3942 shows the configurable PoE options and their default settings for the PoE controller and for the PoE interfaces.

NOTE: On EX8200 switches, the factory default configuration enables PoE on all interfaces starting at Junos OS Release 11.2. Switches that have been upgraded to Release 11.2 from a previous release might not have PoE enabled by default. To enable PoE on all PoE-capable ports on a switch, use the set poe interface all configuration command.

Table 483: Configurable PoE Options and Default Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE Controller Options</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 483: Configurable PoE Options and Default Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| guard-band      | 0 W                          | Reserves a specified amount of power from the PoE power budget to be used in the case of a spike in PoE power consumption:  
• Up to 15 W on EX6200 and EX8200 switches  
• Up to 19 W on all other switches |
| lldp-priority   | Not included in default configuration | When included in the configuration, assigns interfaces the power priority provided by the connected powered device by using Link Layer Discovery Protocol (LLDP) power negotiation rather than the power priority configured on the switch interface. Requires LLDP power negotiation to be enabled. |
| management      | **class**                    | Sets the PoE power management mode for the switch or line card. The power management mode determines how power to a PoE interface is allocated:  
• **class**—In this mode, the power allocated to a PoE interface is determined in one of two ways:  
  • If LLDP power negotiation is enabled, the PoE controller allocates PoE power by using LLDP power negotiation, which allows the PoE controller to dynamically allocate power to LLDP-enabled devices based on their power needs. LLDP power negotiation is enabled by default on supported switches when the `management` option is set to `class`. For information about configuring LLDP power negotiation, see “Configuring LLDP (CLI Procedure)” on page 1745.  
  • If LLDP power negotiation is disabled or not supported on the powered device or the switch, the maximum power delivered by an interface is determined by the class of the connected powered device. If there is no powered device connected, standard 15.4W power is allocated on the interface.  
• **static**—The maximum power delivered by an interface is statically configured and is independent of the class of the connected powered device. The maximum power is allocated to the interface even if a powered device is not connected. |
| maximum-power   | 792 W for the EX8200-2XS-40P (40-port PoE+ with 4-port SFP and 2-port SFP+) line card  
915 W for the EX8200-48PL (48-port PoE+ 20 Gbps) line card  
1440 W for the EX6200-48P (48-port PoE+) line card | (EX6200 and EX8200 switches only) Sets the PoE power budget for the line card:  
• 37 W through 792 W for the EX8200-2XS-40P line card  
• 37 W through 915 W for the EX8200-48PL line card  
• 37 W through 1440 W for the EX6200-48P line card |
| notification-control | Not included in default configuration | When included in the configuration, enables the PoE controller to send PoE SNMP traps. |

Interface Options
### Table 483: Configurable PoE Options and Default Settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>af-mode</strong></td>
<td>Not included in default</td>
<td>(EX6200 switches only) When included in the configuration, restricts a PoE interface to supporting IEEE 802.3af only. The maximum power that can be delivered by the PoE interface is 15.4 W.</td>
</tr>
<tr>
<td><strong>disable (Power over Ethernet)</strong></td>
<td>Not included in default</td>
<td>When included in the configuration, disables PoE on the interface. The interface maintains network connectivity but no longer supplies power to a connected powered device. Power is not allocated to the interface.</td>
</tr>
</tbody>
</table>
| **maximum-power (Interface)** | 30.0 W for interfaces that support PoE+ (IEEE 802.3at) and 15.4 W for interfaces that support PoE (IEEE 802.3af) | Sets the maximum power that can be delivered by a PoE interface when the power management mode is static:  
  • Up to 30 W for EX2200, EX3300, EX4200, EX4300, EX6200, and EX8200 switches  
  • Up to 18.6 W for EX3200 switches  
  This setting is ignored if the power management mode is class.  

**NOTE:** The maximum-power setting permitted by the CLI might be greater than the maximum power a given PoE port can deliver. For example, the CLI permits you to set any port on an EX8200 line card to 30 W; however, only ports 0 through 11 support 30 W. Similarly, the CLI permits you to set any port on an EX4200 switch to 30 W, but some EX4200 models support only 18.6 W per port. If you configure a maximum-power value that is greater than the maximum power supported by a port, the power allocated to the port will be the maximum supported. |
| **priority (Power over Ethernet)** | low                            | Sets an interface’s power priority to either low or high. If power is insufficient for all PoE interfaces, the PoE power to low priority interfaces is shut down before power to high priority interfaces is shut down. Among interfaces that have the same assigned priority, the power priority is determined by port number, with lower-numbered ports having higher priority.  
  If LLDP power priority is enabled, the switch assigns each interface the power priority provided by the connected LLDP-enabled powered device rather than the interface’s configured priority.  
  On EX6200 and EX8200 switches, priority determines the interface’s power priority relative to the other interfaces on the line card, not the interfaces on the switch as a whole. If power management cannot provide the line card with its full PoE power budget, PoE power to interfaces with low priority is shut down first. |
| **telemetries**            | Not included in default        | When included in the configuration, enables the logging of power consumption records on an interface. Logging occurs every 5 minutes for 1 hour unless you specify a different value for interval (Power over Ethernet) or duration. |
Configuring the PoE Controller on EX2200, EX3200, EX3300, EX4200, and EX4300 Switches

To configure the PoE controller on EX2200, EX3200, EX3300, EX4200, and EX4300 switches:

- To change the management mode or to configure a guard band setting for a standalone switch or for all members of an EX3300 Virtual Chassis, an EX4200 Virtual Chassis, an EX4300 Virtual Chassis, or a mixed EX4200 and EX4500 Virtual Chassis that supports PoE:

  [edit]
  user@switch# set poe management mode guard-band watts

  For example, to set the management mode to static and to configure a guard band of 15 W:

  [edit]
  user@switch# set poe management static guard-band 15

  **NOTE:** If the PoE power budget for the switch is insufficient to provide maximum power to all the PoE ports, we recommend that you do not change the management mode from class to static. If you change the power management mode to static and do not change the other default settings, the PoE controller allocates maximum power to the PoE ports in the order of port number, which means PoE will be disabled on higher-numbered ports when the PoE power budget runs out.

  In class mode, on the other hand, the PoE controller does not allocate power to a port until a powered device is connected. The class of the connected device determines the amount of power allocated. Thus in class mode, any PoE port can be used to power a device and all the PoE ports on the switch can be used as long as the combined power demand does not exceed the PoE power budget.

- To enable PoE SNMP traps on a standalone switch or on a specific member of a Virtual Chassis:

  [edit]
  user@switch# set poe notification-control fpc number

  For example, to enable PoE SNMP traps on a standalone switch or on member 0 of a Virtual Chassis:

  [edit]
  user@switch# set poe notification-control fpc 0

  **NOTE:** On EX3200 and EX4200 switches that support enhanced PoE, you must change the management mode from class mode to static mode to take advantage of the higher per-port power limits of enhanced PoE.
Configuring the PoE Controllers on EX6200 and EX8200 Switches

On EX6200 and EX8200 switches, each line card that supports PoE has its own PoE controller. This means that the PoE controller options are configured separately for each line card.

In addition, each line card has its own separate, configurable PoE power budget. The default power budget for a line card is the amount of power needed to supply all PoE ports on the line card with their maximum supported power. Because there might not be enough power available in a switch to supply each PoE line card with the default PoE power budget, you can configure smaller power budgets for one or more line cards, freeing up power for other line cards.

To configure the line card PoE controllers in an EX6200 or EX8200 switch:

- To configure a guard band setting, to change the management mode, or to configure the PoE power budget for a specific line card:

  ```
  [edit]
  user@switch# set poe fpc number guard-band watts management mode maximum-power watts
  ```

  For example, to configure a PoE budget of 350 W and a guard band of 15 W on line card 1:

  ```
  [edit]
  user@switch# set poe fpc 1 guard-band 15 maximum-power 350
  ```

  **NOTE:** If you configure a PoE power budget for a line card that is smaller than the default power budget, we recommend that you do not change the management mode from class to static. If you change the power management mode to static and do not change the interface default settings, the PoE controller allocates maximum power to the PoE ports in the order of port number. As a result, PoE will be disabled on higher-numbered ports when the PoE power budget runs out.

  In class mode, on the other hand, the PoE controller does not allocate power to a port until a powered device is connected. The class of the connected device determines the amount of power allocated. Thus in class mode, any PoE port can be used to power a device and all the PoE ports on the switch can be used as long as the combined power demand does not exceed the PoE power budget.

- To configure the same guard band value, management mode, or PoE power budget for all line cards in a switch:

  ```
  [edit]
  user@switch# set poe fpc all guard-band watts management mode maximum-power watts
  ```

  For example, to configure a PoE budget of 1000 W and static management mode for all line cards in a switch:
[edit]
user@switch# set poe fpc all management static maximum-power 1000

If you configure different settings for a specific line card, those settings override the settings configured with the `fpc all` statement.

- To enable PoE SNMP traps on a line card:
  
  [edit]
  user@switch# set poe notification-control fpc number

  For example, to enable PoE SNMP traps on line card 7:

  [edit]
  user@switch# set poe notification-control fpc 7

### Configuring PoE Interfaces

To configure the PoE interfaces on a switch that supports PoE:

- To configure all PoE interfaces with the same setting or settings:

  [edit]
  user@switch# set poe interface all options

  For example, to enable telemetry collection on all interfaces, using the default collection duration and interval:

  [edit]
  user@switch# set poe interface all telemetries

  **NOTE:** For PoE to be enabled on all PoE-capable interfaces, the configuration must include the `interface all` statement in the `[edit poe]` hierarchy. With the exception of EX8200 switches that were shipped from the factory with a Junos OS release earlier than Release 11.2, the factory default configurations of switches that support PoE include this statement.

  [edit]
  user@switch# set poe interface ge-0/0/0 priority high telemetries duration 24

  [edit]
  user@switch# set poe interface ge-0/0/1

  [edit]
  user@switch# set poe interface ge-0/0/5 maximum-power 18.6

  [edit]
  user@switch# set poe interface ge-5/0/7 disable
When you configure an individual interface, its configuration overrides any settings you configure with the `set poe interface all` command. For example, `ge-0/0/1` in the preceding example retains the default settings, regardless of any settings configured with the `set poe interface all` command.

**Related Documentation**
- Example: Configuring PoE Interfaces on an EX Series Switch on page 3935
- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Example: Configuring PoE on an EX6200 or EX8200 Switch
- Verifying PoE Configuration and Status (CLI Procedure) on page 3974
- Understanding PoE on EX Series Switches on page 3925

**Configuring PoE (J-Web Procedure)**

Power over Ethernet (PoE) ports supply electric power over the same ports that are used to connect network devices to EX Series switches. These ports allow you to plug in devices that require both network connectivity and electric power, such as VoIP phones, wireless access points, and some IP cameras. Using the Power over Ethernet (PoE) Configuration page in the J-Web interface, you can modify the settings of all interfaces that are PoE-enabled.

This topic includes:
- Configuring PoE on EX2200, EX2200-C, EX3200, EX3300, EX4200, and EX4300 Switches on page 3948
- Configuring PoE on EX6200 Switches on page 3949

**Configuring PoE on EX2200, EX2200-C, EX3200, EX3300, EX4200, and EX4300 Switches**

To configure PoE:

1. Select **Configure > Power over Ethernet**.

   The page displays a list of all PoE-capable interfaces except uplink ports. Specific operational details about an interface are displayed in the Details section of the page.

   The details include the PoE operational status and port class.

   **NOTE:** If you are configuring a Virtual Chassis, the PoE configuring option is displayed if any member of the Virtual Chassis supports PoE, even if the Virtual Chassis master does not support PoE.
NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Edit**—Changes PoE settings for the selected port as described in Table 484 on page 3949.
   - **System Settings**—Modifies general PoE settings as described in Table 485 on page 3949.

### Table 484: PoE Edit Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable PoE</td>
<td>Specifies that PoE is enabled on the interface.</td>
<td>Select this option to enable PoE or PoE+ on the interface.</td>
</tr>
<tr>
<td>Priority</td>
<td>Lists the power priority (low or high) configured on the interface enabled for PoE.</td>
<td>Set the priority as <strong>High</strong> or <strong>Low</strong>.</td>
</tr>
<tr>
<td>Maximum Power</td>
<td>Specifies the maximum PoE wattage available to provision the active PoE interface on the switch.</td>
<td>Select a value in watts. If no value is specified, the default is 15.4 for PoE interfaces and 30.0 for PoE+ interfaces.</td>
</tr>
</tbody>
</table>

### Table 485: System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE Management</td>
<td>Specifies the power management mode. The options are: <strong>static</strong> and <strong>class</strong>.</td>
<td>By default, the power management mode is <strong>class</strong>. Select <strong>static</strong> to change the power management mode.</td>
</tr>
</tbody>
</table>

**NOTE:** When the power management mode is set to **class**, the maximum power value is overridden by the maximum power value of the class of the powered device that is connected to the switch on the PoE port. When the power management mode is set to **static**, you can specify the maximum power for each PoE interface.

| Guard Band (watts) | Specifies the amount of power reserved for power spikes from the PoE power budget of the switch. | Enter a value to set the guard band value in watts. The default value is 0. |

---

### Configuring PoE on EX6200 Switches

To configure PoE:

1. Select **Configure > Power over Ethernet**.
The page displays a list of all PoE-capable interfaces for each FPC. Specific operational details about an interface are displayed in the Details section of the page. The details include the PoE operational status and port class.

**NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Edit**—Changes PoE settings for the selected port as described in Table 486 on page 3950.
   - **FPC Settings**—Changes PoE settings of PoE-capable FPCs.

   To configure FPC settings, click one of the following options:
   - **Add**—Adds a PoE setting for an FPC as described in Table 487 on page 3950.
   - **Edit**—Modifies a PoE setting for an FPC as described in Table 487 on page 3950.
   - **Delete**—Deletes an existing PoE settings for an FPC.

### Table 486: Edit PoE Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable PoE</td>
<td>Specifies that PoE is enabled on the interface.</td>
<td>Select this option to enable PoE or PoE+ on the interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the interface is PoE or PoE+.</td>
<td>Select an option from the list.</td>
</tr>
<tr>
<td>Priority</td>
<td>Lists the power priority (low or high) configured on the interface enabled for PoE.</td>
<td>Set the priority as High or Low.</td>
</tr>
<tr>
<td>Maximum Power</td>
<td>Specifies the maximum PoE wattage available to provision active PoE ports on the switch.</td>
<td>Select a value in watts. If no value is specified, the default is 15.4 for PoE interfaces and 30.0 for PoE+ interfaces.</td>
</tr>
</tbody>
</table>

### Table 487: FPC PoE Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC</td>
<td>Specifies the FPC number.</td>
<td>Select a value from the list.</td>
</tr>
</tbody>
</table>
Table 487: FPC PoE Settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoE Management</td>
<td>Specifies the power management mode. The options are static and class.</td>
<td>By default, the power management mode is class. Select static to change the power management mode.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When the power management mode is set to class, the maximum power value is overridden by the maximum power value for the interface that is connected to the switch on the PoE port. When the power management mode is set to static, you can specify the maximum power for each PoE interface.</td>
<td></td>
</tr>
<tr>
<td>Guard Band (watts)</td>
<td>Specifies the amount of power reserved for power spikes from the PoE power budget of the switch.</td>
<td>Enter a value to set the guard band value in watts. The default value is 0.</td>
</tr>
<tr>
<td>Maximum Power</td>
<td>Specifies the maximum PoE wattage available to provision active PoE ports on the FPC. For example, if you specify 1000 W, the PoE controller is limited to a power budget of 1000 W to distribute to the PoE ports.</td>
<td>Select a value in watts.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring PoE (CLI Procedure) on page 3942
- Example: Configuring PoE Interfaces on an EX Series Switch on page 3935
- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Example: Configuring PoE on an EX6200 or EX8200 Switch
- Monitoring PoE on page 3970
- Understanding PoE on EX Series Switches on page 3925

**Configuration Statements**
- [edit poe] Configuration Statement Hierarchy on EX Series Switches on page 3951

**[edit poe] Configuration Statement Hierarchy on EX Series Switches**

This topic lists supported and unsupported configuration statements in the [edit poe] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.
This topic lists:

- Supported Statements in the [edit poe] Hierarchy Level on page 3952
- Unsupported Statements in the [edit poe] Hierarchy Level on page 3953

**Supported Statements in the [edit poe] Hierarchy Level**

The following hierarchy shows the [edit poe] configuration statements supported on EX Series switches except for EX6200 and EX8200 switches:

```plaintext
poe {
  guard-band watts;
  interface (all | interface-name) {
    disable;
    maximum-power watts;
    priority (high | low);
    telemetries {
      disable;
      duration hours;
      interval minutes;
    }
  }
  lldp-priority;
  management (class | static);
  notification-control {
    fpc slot-number {
      disable;
    }
  }
}
```

The following hierarchy shows the [edit poe] configuration statements supported on EX Series switches for EX6200 and EX8200 switches:

```plaintext
poe {
  fpc (all | slot-number) {
    guard-band watts;
    lldp-priority;
    management (class | static);
    maximum-power watts;
  }
  interface (all | interface-name) {
    af-mode;
    disable;
    maximum-power watts;
    priority (high | low);
    telemetries {
      disable;
      duration hours;
      interval minutes;
    }
  }
  notification-control {
    fpc slot-number {
      disable;
    }
  }
}
```
Unsupported Statements in the [edit poe] Hierarchy Level

All statements in the [edit poe] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation
- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Example: Configuring PoE on an EX6200 or EX8200 Switch
- Configuring PoE (CLI Procedure) on page 3942
- Understanding PoE on EX Series Switches on page 3925

af-mode

Syntax af-mode;
Hierarchy Level [edit poe interface (Power over Ethernet) (all | interface-name)]
Release Information Statement introduced in Junos OS Release 11.3 for EX Series switches.
Description Configure a PoE port on an EX6200 switch to support IEEE 802.3af only. The maximum power the port can deliver in either class or static mode is 15.4 W.
Default PoE ports on an EX6200 switch support IEEE 802.3at (PoE+) by default.
Required Privilege Level system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.
Related Documentation • Configuring PoE (CLI Procedure) on page 3942
disable (Power over Ethernet)

Syntax

```
disable;
```

Hierarchy Level

```
[edit poe interface (all | interface-name)],
[edit poe interface (all | interface-name) telemetries],
[edit poe notification-control fpc slot-number]
```

Release Information


Description

Disable a PoE interface, disable the collection of power consumption data for a PoE interface, or disable the generation of the PoE SNMP traps. The action of the `disable` statement depends on which statement it is used with:

- When used with `interface`—Disable the PoE capability of this interface. The interface operates as a standard network access interface, and power is no longer allocated to it from the PoE power budget. Although the PoE capability is disabled, the PoE configuration for the interface is retained. To re-enable the PoE capability of this interface, delete the `disable` statement from the `interface` entry in the configuration.

- When used with `telemetries`—Disable the collection of PoE power consumption records for this interface. Any previously collected records are deleted. However, the `telemetries` configuration is retained, including the values for `interval` and `duration`. To re-enable record collection, delete the `disable` statement from the `telemetries` entry in the configuration.

- When used with `notification-control`—Disable the generation of PoE SNMP traps. To re-enable PoE traps, delete the `disable` statement from the `notification-control` entry in the configuration.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Configuring PoE (CLI Procedure) on page 3942
- Example: Disabling a PoE Interface on ACX2000 Routers
duration

Syntax  

duration hours;

Hierarchy Level  

[edit poe interface (all | interface-name) telemetries]

Release Information  

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  

Modify the duration over which data is collected when you are monitoring the power consumption of a PoE interface.

Options  

hours — Number of hours over which the data is to be collected.

Range: 1 through 24

Default: 1

Required Privilege  

Level  

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation  

• Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937

• Configuring PoE (CLI Procedure) on page 3942
**fpc (Notification Control)**

**Syntax**

```
fpc slot-number {
    disable;
}
```

**Hierarchy Level**

```
[edit poe notification-control]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Enable the specified PoE controller to generate PoE traps.

**Default**

PoE traps are disabled by default.

**Options**

`slot-number`—Indicates the PoE controller by FPC slot number, where `slot-number` is:

- 0—On an EX2200, EX3200, standalone EX3300, standalone EX4200, or standalone EX4300 switch
- Member ID—On an EX3300, EX4200, or EX4300 switch in a Virtual Chassis
- Line card slot number—On an EX6200 or EX8200 switch

The remaining statement is explained separately.

**Required Privilege**

```
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
```

**Related Documentation**

- Configuring PoE (CLI Procedure) on page 3942
guard-band

Syntax  guard-band watts;

Hierarchy Level  [edit poe],
                 [edit poe (all | fpc slot-number)]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Reserve a specified amount of power from the PoE power budget for the switch or the
              line card in case of a spike in PoE consumption.

Options  watts—Amount of power to be reserved in case of a spike in PoE consumption.
          Range: 0 through 15 for EX6200 and EX8200 switches and 0 through 19 for ACX2000
                  routers and all other switches.
          Default: 0

Required Privilege Level  system—To view this statement in the configuration.
                          system-control—To add this statement to the configuration.

Related Documentation  • Configuring PoE (CLI Procedure) on page 3942
interface (Power over Ethernet)

Syntax

```
interface (all | interface-name) {
  af-mode;
  disable;
  maximum-power watts;
  priority (high | low);
  telemetries {
    disable;
    duration hours;
    interval minutes;
  }
}
```

Hierarchy Level  [edit poe]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Specify a PoE interface to be configured.

Options  all—All PoE interfaces on the switch that have not been individually configured for PoE. If a PoE interface has been individually configured, that configuration overrides any settings specified with all.

```
interface-name—Name of the specific interface being configured.
```

If you use the interface statement without any substatements, PoE is enabled on all interfaces or the specified interface with default values for the remaining statements.

The remaining statements are explained separately.

Required Privilege Level  system—To view this statement in the configuration. system-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
  • Configuring PoE (CLI Procedure) on page 3942
interval (Power over Ethernet)

Syntax  

```
interval minutes;
```

Hierarchy Level  

```
[edit poe interface (all | interface-name) telemetries]
```

Release Information  

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  

Modify the interval at which data is collected when you are monitoring the power consumption of a PoE interface.

Options  

- **minutes**—Frequency of data collection.
  
  **Range:** 1 through 30
  
  **Default:** 5

Required Privilege Level  

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation  

- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Configuring PoE (CLI Procedure) on page 3942
- Configuring PoE (J-Web Procedure) on page 3948
management

Syntax  management (class | static | high-power);

Hierarchy Level  [edit poe],
                [edit poe (all | fpc slot-number)]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  Designate how the PoE controller allocates power to the PoE interfaces.

Default  class

Options  •  class—The amount of power allocated to the interface is determined by the class of the connected powered device. If no powered device is connected, standard 15.4 W power is allocated to the interface. See “Understanding PoE on EX Series Switches” on page 3925 for more information about classes of powered devices.

        •  static—The amount of power allocated to the interface is determined by the value of the maximum-power statement, not the class of the connected powered device. This amount is allocated even when a powered device is not connected to the interface, ensuring that power is available when needed.

        •  high-power—(ACX2000 routers only) ACX2000 PoE interfaces support power delivery of up to 65 W per port using all four pairs of Ethernet RJ45 cables. Traditional PoE ports use only two pairs of Ethernet cable for power delivery. According to the IEEE 802.3af standard, each port can deliver a maximum power of up to 32 W. With high-power mode of power delivery over all four pairs, the power sourcing equipment (PSE) has an option to deliver up to 65 W per port, provided the powered devices request this high power over all four pairs of the Ethernet cable. By default, high-power mode is not enabled and has to be explicitly enabled. When the PoE controller is configured for high-power mode, the PoE controller does not deliver power to normal powered devices that request power over two pairs.

Required Privilege Level  system—To view this statement in the configuration.
                        system-control—To add this statement to the configuration.

Related Documentation  •  Configuring PoE (CLI Procedure) on page 3942
                         •  [edit poe] Configuration Statement Hierarchy on ACX2000 Routers
                         •  Example: Configuring PoE on ACX2000 Routers
                         •  Understanding PoE on EX Series Switches on page 3925
maximum-power (Interface)

Syntax  
maximum-power watts;

Hierarchy Level  
[edit poe interface (all | interface-name)]

Release Information  

Description  
Set the maximum amount of power that the switch can supply to the PoE port.

NOTE: Although you can set this value when PoE power management is in class mode, it does not establish the maximum power for the port. Instead, the IEEE 802.3af (PoE) or IEEE 802.3at (PoE+) class of the connected device determines the maximum power for the port.

Options  
watts—The maximum number of watts that can be supplied to the port.

For EX2200 switches, EX3300 switches, EX4200 switches, EX4300 switches, EX6200 switches, and EX8200 switches:
Range: 0.0 through 30.0
Default: 15.4 W for ports that support IEEE 802.3af and 30 W for ports that support IEEE 802.3at

For EX3200 switches:
Range: 0.0 through 18.6
Default: 15.4 W

For ACX2000 routers:
Range: 1 through 65 W
Default: 32 W

NOTE: The maximum-power setting permitted by the CLI might be greater than the maximum power a given PoE port can deliver. For example, the CLI permits you to set any PoE port on an EX8200 line card to 30 W; however, only ports 0 through 11 support 30 W. Similarly, the CLI permits you to set any PoE port on an EX4200 switch to 30 W, but some models of EX4200 switch support only 18.6 W per port. If you configure a maximum-power value that is greater than the maximum power supported by a port, the power allocated to the port will be the maximum supported.

If you use the all option to set maximum-power to a value greater than 15.4 W on all interfaces on an EX8200 line card, the maximum power allocated to all ports is 15.4 W.
NOTE: Support for a maximum of 18.6 W per port instead of 15.4 W per port on EX3200 switches and P and T models of EX4200 switch requires Junos OS Release 11.1 or later. In addition to requiring an upgrade of Junos OS to Release 11.1 or later, switches that are running a previous Junos OS release require the PoE controller software be upgraded as described in “Upgrading the PoE Controller Software” on page 3967. If the controller software is not upgraded and you set maximum-power to a value greater than 15.4 W, the configuration is accepted when you commit it, but the actual power allocated to the port will be 15.4 W.

NOTE: On ACX2000 routers, the power sourcing equipment (PSE) delivers up to 65 W per port, provided the management mode is set to high-power mode, by using the high-power option at the [edit poe management] hierarchy level. By default, the management mode is set to static. In the static mode, the PSE can deliver power up to 32 W.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Configuring PoE (CLI Procedure) on page 3942
- Example: Configuring PoE on ACX2000 Routers
- management on page 3960
**notification-control**

**Syntax**

```
notification-control {
  fpc slot-number {
    disable;
  }
}
```

**Hierarchy Level**

```
[edit poe]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Enable or disable the generation of PoE SNMP traps. If PoE traps are enabled, an SNMP trap is sent whenever a PoE interface is enabled or disabled.

The remaining statements are explained separately.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Configuring PoE (CLI Procedure) on page 3942
poe

Syntax  For switches other than EX6200 and EX8200 switches:

    poe {
        guard-band watts;
        interface (all | interface-name) {
            disable;
            maximum-power watts;
            priority (high | low);
            telemetries {
                disable;
                duration hours;
                interval minutes;
            }
        }
        lldp-priority;
        management (class | static);
        notification-control {
            fpc slot-number {
                disable;
            }
        }
    }

For EX6200 and EX8200 switches:

    poe {
        fpc ( all | slot-number) {
            guard-band watts;
            lldp-priority;
            management (class | static);
            maximum-power watts;
        }
        interface (all | interface-name) {
            af-mode;
            disable;
            maximum-power watts;
            priority (high | low);
            telemetries {
                disable;
                duration hours;
                interval minutes;
            }
        }
        notification-control {
            fpc slot-number {
                disable;
            }
        }
    }

Hierarchy Level  [edit]
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Configure PoE options.

The remaining statements are explained separately.

```
priority (Power over Ethernet)
```

**Syntax**

```
priority (low | high);
```

**Hierarchy Level**

```
[edit poe interface (all | interface-name)]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Set the power priority for individual interfaces when there is insufficient power for all PoE interfaces. If the switch needs to shut down powered devices because PoE demand exceeds the PoE budget, low priority devices are shut down before high priority devices. Among interfaces that have the same assigned priority, priority is determined by port number, with lower-numbered ports having higher priority.

**Default**

```
low
```

**Options**

```
value—high or low:
```

- **high**—Specifies that this interface is to be treated as high priority in terms of power allocation. If the switch needs to shut down powered devices because PoE demand exceeds the PoE budget, power is not shut down on this interface until it has been shut down on all the low priority interfaces.

- **low**—Specifies that this interface is to be treated as low priority in terms of power allocation. If the switch needs to shut down powered devices because PoE demand exceeds the PoE budget, power is shut down on this interface before it is shut down on high priority interfaces.

**Required Privilege Level**

```
system—To view this statement in the configuration.
```

```
system-control—To add this statement to the configuration.
```

**Related Documentation**

- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Example: Configuring PoE on an EX6200 or EX8200 Switch
- Configuring PoE (CLI Procedure) on page 3942
telemetries

Syntax

telemetries {
  disable;
  duration hours;
  interval minutes;
}

Hierarchy Level
  [edit poe interface (all | interface-name)]

Release Information
  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
  Enable the logging of power consumption of a PoE interface over time.

  If you want to log the power consumption of a PoE interface, you must explicitly specify the telemetries statement. When you commit the configuration, logging begins, with data being collected at the specified intervals. Logging stops at the end of the specified duration. If you did not specify the duration and interval statements, data is collected at five minute intervals for one hour.

  The remaining statements are explained separately.

Default
  Logging of power consumption is disabled.

Required Privilege
  system—To view this statement in the configuration.

  system-control—To add this statement to the configuration.

Related Documentation

  • Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937

  • Example: Configuring PoE on ACX2000 Routers

  • Configuring PoE (CLI Procedure) on page 3942

  • show poe telemetries on page 3988
CHAPTER 72

Administration

- Upgrading on page 3967
- Routine Monitoring on page 3970
- Operational Commands on page 3976

Upgrading

- Upgrading the PoE Controller Software on page 3967

Upgrading the PoE Controller Software

Each Junos OS image for an EX Series switch that supports PoE contains the most recent version of the PoE controller software at the time the Junos OS image was built. When you upgrade Junos OS on your switch, the new image might contain a more recent version of the PoE controller software than is currently running on the PoE controller. You can upgrade your PoE controller software by requesting that the more recent version of the software contained in the Junos OS image be downloaded to the controller.

**NOTE:** Powered devices are not guaranteed to receive power while the new software is being downloaded to the PoE controller, a process that can take up to 10 minutes. In addition, during the software download, some PoE operational commands, such as `show poe interface`, might not show correct output. We recommend that you upgrade your PoE controller software during a regularly scheduled maintenance window.

**NOTE:** On an EX8200 Virtual Chassis, you cannot execute PoE commands on the XRE200 External Routing Engine. You can execute PoE commands only on the member EX8200 switches. Use the `request session member member-id` command to open a CLI session on a member switch.
This topic covers:

- Determining Whether the PoE Controller Software Needs Upgrading on page 3968
- Upgrading the PoE Controller Software on page 3968
- Monitoring the Upgrade Progress on page 3969

### Determining Whether the PoE Controller Software Needs Upgrading

To determine if the version of the PoE controller software supplied with Junos OS is more recent than the version of the software currently running on the PoE controller, enter the following command:

```
user@switch> showpoecontroller
```

<table>
<thead>
<tr>
<th>Controller</th>
<th>Maximum Power</th>
<th>Consumption Power</th>
<th>Guard Band</th>
<th>Management Class</th>
<th>Status</th>
<th>Lldp Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0**</td>
<td>130.00W</td>
<td>0.00W</td>
<td>0W</td>
<td>Class AF_MODE</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

**New PoE software upgrade available.**

Use 'request system firmware upgrade poe fpc-slot <slot>'

This procedure will take around 10 minutes (recommended to be performed during maintenance)

The **New PoE software upgrade available** text in the output indicates that the PoE controller software is out-of-date and should be upgraded.

For Virtual Chassis or switches with PoE line cards, the output of the `showpoecontroller` command indicates which members of a Virtual Chassis or which PoE line cards have PoE controllers with out-of-date software:

```
user@switch> showpoecontroller
```

<table>
<thead>
<tr>
<th>Controller</th>
<th>Maximum Power</th>
<th>Consumption Power</th>
<th>Guard Band</th>
<th>Management Class</th>
<th>Status</th>
<th>Lldp Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>130.00W</td>
<td>120.34W</td>
<td>0W</td>
<td>Class AF_ENHANCE</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>4**</td>
<td>410.00W</td>
<td>182.80W</td>
<td>0W</td>
<td>Class AF_MODE</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

**New PoE software upgrade available.**

Use 'request system firmware upgrade poe fpc-slot slot'

This procedure will take around 10 minutes (recommended to be performed during maintenance)

In the preceding example, member 4 of the Virtual Chassis has out-of-date PoE controller software.

**NOTE:** We recommend that all member switches of a Virtual Chassis or all line cards in a switch run the same version of the PoE controller software.

### Upgrading the PoE Controller Software

To upgrade the PoE controller software for a standalone switch with built-in PoE interfaces, enter:

```
user@switch> request system firmware upgrade poe fpc-slot 0
```

Firmware upgrade initiated. Poe Upgrade takes about 10 minutes

Use 'show poe controller' to get the download status
To upgrade the PoE controller software on a specific Virtual Chassis member or line card on a switch, enter:

```
user@switch> request system firmware upgrade poe fpc-slot 8
Firmware upgrade initiated. Poe Upgrade takes about 10 minutes
Use 'show poe controller' to get the download status
```

To upgrade the PoE controller software on all members of a Virtual Chassis or all line cards on a switch, enter:

```
user@switch> request system firmware upgrade poe fpc-slot all-members
Firmware upgrade initiated. Poe Upgrade takes about 10 minutes
Use 'show poe controller' to get the download status
```

**Monitoring the Upgrade Progress**

Use the `show poe controller` command to monitor the progress of the controller software upgrade:

```
user@switch> show poe controller
Controller   Maximum   Power         Guard    Management  Status            Lldp
index       power     consumption   band                                   Priority
0***       130.00W   0.00W           0W                 SW_DOWNLOAD(14%)  Disabled
**New PoE software upgrade available.
Use 'request system firmware upgrade poe fpc-slot <slot>'
This procedure will take around 10 minutes (recommended to be performed during maintenance)
```

The **Status** field is updated during the download process to show the following stages of the download:

- **DOWNLOAD_INIT**
- **SW_DOWNLOAD (n%)**

When the software upgrade is complete, the **New PoE software upgrade available** text is no longer displayed for the particular FPC.

**NOTE:** If you are upgrading the PoE controller software to enable enhanced PoE, the **Status** field for the controller shows **AF_ENHANCE** after the upgrade completes, indicating that the controller now supports enhanced PoE. The default maximum power per port is not automatically increased as a result of the upgrade—it is still 15.4 W per port. You must explicitly set the maximum power for a port to 18.6 W. Enhanced PoE is supported in Junos OS Release 11.1 or later on EX3200 switches and on EX4200 P or T model switches.

**Related Documentation**

- Verifying PoE Configuration and Status (CLI Procedure) on page 3974
- Understanding PoE on EX Series Switches on page 3925
Routine Monitoring

- Monitoring PoE on page 3970
- Monitoring PoE Power Consumption (CLI Procedure) on page 3971
- Verifying PoE Configuration and Status (CLI Procedure) on page 3974

Monitoring PoE

**Purpose**
Use the monitoring functionality to view real-time data of the power consumed by each PoE interface, and to enable and configure telemetry values. When telemetry is enabled, the software measures the power consumed by each interface and stores the data for future reference.

**NOTE:** If you are configuring a Virtual Chassis, the PoE monitoring option is displayed if any member of the Virtual Chassis supports PoE, even if the Virtual Chassis master does not support PoE.

**Action**
To monitor PoE using the J-Web interface, select **Monitor > Power over Ethernet**.

To monitor PoE power consumption with CLI commands in the CLI Terminal in the J-Web interface:

1. Select **Troubleshoot > CLI Terminal**.
2. Type a CLI command:
   - `show poe controller`
   - `show poe interface`
   - `show poe telemetry`

For detailed information about using these CLI commands to monitor PoE power consumption, see Monitoring PoE Power Consumption (CLI Procedure) in the EX Series documentation at [http://www.juniper.net/techpubs](http://www.juniper.net/techpubs).

**Meaning**
In the J-Web interface the PoE Monitoring screen is divided into two parts. The top half of the screen displays real-time data of the power consumed by each PoE-capable interface and a list of ports that utilize maximum power.

Select a particular interface to view a graph of the power consumed by the selected interface.

The bottom half of the screen displays telemetry information for interfaces. The Telemetry Status field displays whether telemetry has been enabled on the interface. Click the **Show Graph** button to view a graph of the telemetries. The graph can be based on power or voltage. To modify telemetry values, click **Edit**. Specify Interval in minutes, Duration in hours, and select **Log Telemetries** to enable telemetry on the selected interface.
You can monitor Power over Ethernet (PoE) power consumption, both for the switch as a whole and for individual PoE interfaces.

This topic describes how to monitor:

- **PoE Power Consumption on a Switch** on page 3971
- **Current Power Consumption for PoE Interfaces** on page 3971
- **Power Consumption for PoE Interfaces over Time** on page 3973

### PoE Power Consumption on a Switch

**Purpose**

Determine the current PoE power consumption on a switch.

**Action**

Enter the following command:

```
user@switch> show poe controller
```

<table>
<thead>
<tr>
<th>Controller index</th>
<th>Maximum power consumption</th>
<th>Guard band power</th>
<th>Management Class</th>
<th>Status</th>
<th>Lldp Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>405.00W</td>
<td>130.00W</td>
<td>0W</td>
<td>AT_MODE</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Meaning**

At the time the command was executed, the PoE interfaces on the switch were consuming 130 W out of the PoE power budget of 405 W.

### Current Power Consumption for PoE Interfaces

**Purpose**

Determine the current power consumption for individual PoE interfaces.

**Action**

To monitor the power consumption of all PoE interfaces on the switch, use the following command:

```
user@switch> show poe interface
```

<table>
<thead>
<tr>
<th>Interface status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Enabled</td>
<td>15.4W</td>
<td>Low</td>
<td>7.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Enabled</td>
<td>15.4W</td>
<td>High</td>
<td>12.0W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Enabled</td>
<td>15.4W</td>
<td>Low</td>
<td>12.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Enabled</td>
<td>7.0W</td>
<td>Low</td>
<td>5.3W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Enabled</td>
<td>4.0W</td>
<td>Low</td>
<td>4.0W</td>
<td>1</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Enabled</td>
<td>7.0W</td>
<td>Low</td>
<td>6.1W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Enabled</td>
<td>15.4W</td>
<td>Low</td>
<td>12.3W</td>
<td>3</td>
</tr>
</tbody>
</table>
To monitor the power consumption of the PoE interfaces on a specific EX6200 or EX8200 line card, use the following command:

```
user@switch> showpoeinterface fpc-slot 3
```

<table>
<thead>
<tr>
<th>Interface status</th>
<th>Admin status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-3/0/0</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>20.3W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/1</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>17.8W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/2</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>16.3W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/3</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>16.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/4</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>25.9W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/5</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>10.1W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/6</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>16.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/7</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>6.4W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/8</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>5.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/9</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>5.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/10</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>21.5W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/11</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>21.7W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/12</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/13</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/14</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/15</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/16</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/17</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/18</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/19</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/20</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/21</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/22</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/23</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/24</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/25</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/26</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/27</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/28</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>7.0W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/29</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/30</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/31</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/32</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.0W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/33</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.0W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/34</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/35</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/36</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/37</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/38</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/39</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
</tbody>
</table>

To monitor the power consumption of an individual PoE interface (for example, ge-0/0/3), use the following command:

```
user@switch> showpoeinterface ge-0/0/3
```

PoE interface status:
- PoE interface : ge-0/0/3
- Administrative status : Enabled
- Operational status : ON
- Power limit on the interface : 7.0W
- Priority : Low
- Power consumed : 5.3W
Class of power device : 2
PoE Mode : 802.3at

Meaning At the time the command was executed, the individual PoE ports were consuming the amount of power shown. For example, interface ge-0/0/3 was consuming 5.3 W at the time the command was executed.

Power Consumption for PoE Interfaces over Time

Purpose Monitor the power consumption of a PoE interface over a period of time. The records collected remain available for future viewing.

You can specify the intervals at which power consumption data is collected, from once every minute to once every 30 minutes. The default is once every 5 minutes. You can also specify the duration over which the records are collected, from 1 hour (default) to 24 hours.

Action To collect historical records of PoE interface power consumption and display those records:

1. Add the telemetries statement to the PoE interface configuration:

   [edit]
   user@switch# set poe interface ge-0/0/5 telemetries interval 10

   When you commit the configuration, record collection begins.

2. Display the collected records:

   user@switch> show poe telemetries interface ge-0/0/5 count all

   Sl No  Timestamp                Power    Voltage
   1     03-19-2010 13:00:07 UTC  3.9W     50.9V
   2     03-19-2010 12:50:07 UTC  3.9W     50.9V
   3     03-19-2010 12:40:07 UTC  3.9W     50.9V
   4     03-19-2010 12:30:07 UTC  3.9W     50.9V
   5     03-19-2010 12:20:07 UTC  3.9W     50.9V
   6     03-19-2010 12:10:07 UTC  3.9W     50.9V

   To start another session of record collection on the interface, you must delete the existing telemetries configuration on the interface and then reconfigure telemetries. Deleting the telemetries configuration also clears the power consumption history data.

   To clear the history of PoE power consumption without deleting the telemetries configuration, use the command clear poe telemetries interface.

Meaning Over the hour in which the PoE power consumption data on ge-0/0/5 was collected, the connected powered device consistently consumed 3.9 W.

Related Documentation

- Configuring PoE (CLI Procedure) on page 3942
- Example: Configuring PoE Interfaces on an EX Series Switch on page 3935
- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
You can verify the Power over Ethernet (PoE) configuration and status on an EX Series switch.

This topic describes how to verify:

- PoE Controller Configuration and Status on page 3974
- PoE Interface Configuration and Status on page 3975
- PoE SNMP Trap Generation Status on page 3976

### PoE Controller Configuration and Status

**Purpose**

Verify the PoE controller configuration and status, such as the PoE power budget, total PoE power consumption, power management mode, and the supported PoE standard.

**Action**

Enter the following command:

```
user@switch> show poe controller
```

Example output for an EX2200 switch:

<table>
<thead>
<tr>
<th>Controller index</th>
<th>Maximum power</th>
<th>Power consumption</th>
<th>Guard band</th>
<th>Management</th>
<th>Status</th>
<th>Lldp Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>405.00W</td>
<td>130.00W</td>
<td>19W</td>
<td>Class</td>
<td>AT_MODE</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Example output for an EX8200 switch:

<table>
<thead>
<tr>
<th>Controller index</th>
<th>Maximum power</th>
<th>Power consumption</th>
<th>Guard band</th>
<th>Management</th>
<th>Status</th>
<th>Lldp Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>540.00W</td>
<td>435.25W</td>
<td>0W</td>
<td>Static</td>
<td>AT/AF COMBO</td>
<td>Disabled</td>
</tr>
<tr>
<td>4</td>
<td>915.00W</td>
<td>627.01W</td>
<td>15W</td>
<td>Class</td>
<td>AT/AF COMBO</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Meaning**

- For the EX2200 switch—The switch has a PoE power budget of 405 W, of which 130 W were being used by the PoE ports at the time the command was executed. The **Guard band** field shows that 19 W is reserved out of the PoE power budget to protect against spikes in power demand. The power management mode is class. The PoE ports on the switch support PoE+ (IEEE 802.3at).

- For the EX8200 switch—Line card 3 has a PoE power budget of 540 W, of which 435.25 W were being used by the PoE ports on the line card at the time the command was executed. The management mode for line card 3 is static and the line card has a mix of PoE (IEEE 802.3af) and PoE+ (IEEE 802.3at) ports.

Line card 4 has a PoE power budget of 915 W, of which 627.01 W were being used by the PoE ports on the line card at the time the command was executed. The **Guard band** field shows that 15 W is reserved out of the PoE power budget to protect against spikes in power demand. The management mode for line card 4 is class and the line card has a mix of PoE (IEEE 802.3af) and PoE+ (IEEE 802.3at) ports.
PoE Interface Configuration and Status

Purpose
Verify that PoE interfaces are enabled and set to the correct maximum power and priority settings. Also verify current operational status and power consumption.

Action
To view configuration and status for all PoE interfaces, enter:

```
user@switch> show poe interface
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>7.9W</td>
<td>3</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>4.8W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>4.8W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Enabled</td>
<td>ON</td>
<td>7.0W</td>
<td>High</td>
<td>3.3W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/4</td>
<td>Enabled</td>
<td>ON</td>
<td>7.0W</td>
<td>Low</td>
<td>3.3W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/5</td>
<td>Enabled</td>
<td>ON</td>
<td>7.0W</td>
<td>Low</td>
<td>3.2W</td>
<td>2</td>
</tr>
<tr>
<td>ge-0/0/6</td>
<td>Enabled</td>
<td>ON</td>
<td>7.0W</td>
<td>Low</td>
<td>0.0W</td>
<td>not-applicable</td>
</tr>
</tbody>
</table>

To view the configuration and status for the PoE interfaces on an EX6200 or EX8200 line card:

```
user@switch> show poe interface fpc-slot 3
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-3/0/0</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>20.3W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/1</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>17.8W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/2</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>16.3W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/3</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>16.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/4</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>25.9W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/5</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>10.1W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/6</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>16.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/7</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>6.4W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/8</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>5.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/9</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>5.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/10</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>21.5W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/11</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>21.7W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/12</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/13</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/14</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/15</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/16</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/17</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/18</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/19</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/20</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/21</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/22</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/23</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/24</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/25</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/26</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/27</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/28</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>7.0W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/29</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/30</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/31</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/32</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.0W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/33</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.0W</td>
<td>1</td>
</tr>
</tbody>
</table>
To view configuration and status for a single PoE interface, enter:

```
user@switch> show poe interface ge-0/0/3
```

PoE interface status:
- **PoE interface**: ge-0/0/3
- **Administrative status**: Enabled
- **Operational status**: On
- **Power limit on the interface**: 7.0W
- **Priority**: High
- **Power consumed**: 3.3W
- **Class of power device**: 2
- **PoE Mode**: 802.3at

**Meaning**
The command output shows the status and configuration of interfaces. For example, the interface **ge-0/0/3** is administratively enabled. Its operational status is **On**; that is, the interface is currently delivering power to a connected powered device. The maximum power allocated to the interface is 7.0 W. The interface has a high power priority. At the time the command was executed, the powered device was consuming 3.3 W. The IEEE 802.3af class of the powered device is class 2. If the PoE power management mode is class, the class of the powered device determines the maximum power allocated to the interface, which is 7 W in the case of class 2 devices.

The PoE Mode field indicates that the interface supports IEEE 802.3at.

### PoE SNMP Trap Generation Status

**Purpose**: Verify the status of the `notification-control` option, which determines whether or not PoE SNMP traps are enabled.

**Action**: Enter the following command:

```
user@switch> show poe notification-control
```

**Meaning**: PoE SNMP traps are not enabled.

**Related Documentation**
- Configuring PoE (CLI Procedure) on page 3942
- Example: Configuring PoE Interfaces on an EX Series Switch on page 3935
- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Monitoring PoE Power Consumption (CLI Procedure) on page 3971

**Operational Commands**
request system firmware upgrade poe

Syntax  
request system firmware upgrade poe fpc-slot (number | all-members)

Release Information  
Command introduced in Junos OS Release 12.1 for EX Series switches.

Description  
Upgrade the PoE controller software on switches and line cards.

The Junos OS image running on the switch contains a copy of the PoE controller software. This command compares the Junos OS version with the version of the software running on the PoE controller. If the Junos OS version is a more recent version, the command downloads the more recent version to the controller.

For all Virtual Chassis except EX8200 Virtual Chassis, execute this command on the master. The master itself does not have to support PoE for this command to work—for example, you can execute this command on the master of a mixed EX4200 and EX4500 Virtual Chassis when the master is an EX4500 switch. On an EX8200 Virtual Chassis, you must execute this command on the member switch, not the master XRE200 External Routing Engine.

We recommend that all members of a Virtual Chassis run the same version of the PoE controller software.

Upgrading the controller software can take up to 10 minutes. Use the show poe controller command to monitor the progress of the software download.

You cannot downgrade the PoE controller software.

NOTE: When you enter the request system firmware upgrade poe command, a message advises you that the controller software upgrade has started and that it will take about 10 minutes to complete. This message appears even if the FPC you have specified does not have a PoE controller or if the PoE controller software is up-to-date. To determine whether or not the controller software upgrade has actually started, use the show poe controller command.

NOTE: While the upgrade is in progress, power to the powered devices is not guaranteed. We recommend that you upgrade the controller software during a regularly scheduled maintenance window.

Options  
fpc-slot (number | all-members)—Upgrade the PoE controller firmware for the Virtual Chassis member or line card specified by number, or for all Virtual Chassis members and line cards, specified by all-members.

Required Privilege Level  
maintenance
Related Documentation

- show poe controller on page 3979
- Upgrading the PoE Controller Software on page 3967

List of Sample Output
request system firmware upgrade poe fpc-slot 8 on page 3978

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system firmware upgrade poe fpc-slot 8

user@switch> request system firmware upgrade poe fpc-slot 8
Firmware upgrade initiated. Poe Upgrade takes about 10 minutes
Use 'show poe controller' to get the download status
show poe controller

Syntax
show poe controller

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.2 for ACX2000 routers.

Description
Display configuration and status of the PoE controllers.

Required Privilege
view

Related Documentation
- show poe interface on page 3982
- request system firmware upgrade poe on page 3977
- Verifying PoE Configuration and Status (CLI Procedure) on page 3974
- Monitoring PoE Power Consumption (CLI Procedure) on page 3971
- Upgrading the PoE Controller Software on page 3967

List of Sample Output
- show poe controller (EX3200 Switch) on page 3980
- show poe controller (EX8200 Switch) on page 3980
- show poe controller (Controller Software Upgrade in Progress) on page 3980
- show poe controller (ACX2000 Router) on page 3981

Output Fields
- **Controller index**: PoE controller number:
  - 0 for EX2200, EX3200, standalone EX3300, standalone EX4200 switches, standalone EX4300 switches, and ACX2000 routers.
  - Member ID for switches in an EX3300 Virtual Chassis, EX4200 Virtual Chassis, EX4300 Virtual Chassis, or a mixed EX4200 and EX4500 Virtual Chassis.
  - Slot number for line cards with a PoE controller in an EX6200 or EX8200 switch.
- **Maximum power**: The PoE power budget for the switch or line card. The PoE controller allocates power to the PoE ports from this budget.
- **Power consumption**: Total amount of power being used by the PoE ports at the time the command is executed.
- **Guard Band**: Amount of power that has been placed in reserve for power demand spikes and that cannot be allocated to a PoE interface.

Table 488 on page 3979 lists the output fields for the `show poe controller` command. Output fields are listed in the approximate order in which they appear.

Table 488: show poe controller Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller index</td>
<td>PoE controller number:</td>
</tr>
<tr>
<td></td>
<td>- 0 for EX2200, EX3200, standalone EX3300, standalone EX4200 switches, standalone</td>
</tr>
<tr>
<td></td>
<td>EX4300 switches, and ACX2000 routers.</td>
</tr>
<tr>
<td></td>
<td>- Member ID for switches in an EX3300 Virtual Chassis, EX4200 Virtual Chassis,</td>
</tr>
<tr>
<td></td>
<td>EX4300 Virtual Chassis, or a mixed EX4200 and EX4500 Virtual Chassis.</td>
</tr>
<tr>
<td></td>
<td>- Slot number for line cards with a PoE controller in an EX6200 or EX8200</td>
</tr>
<tr>
<td></td>
<td>switch.</td>
</tr>
<tr>
<td>Maximum power</td>
<td>The PoE power budget for the switch or line card. The PoE controller allocates</td>
</tr>
<tr>
<td></td>
<td>power to the PoE ports from this budget.</td>
</tr>
<tr>
<td>Power consumption</td>
<td>Total amount of power being used by the PoE ports at the time the command is</td>
</tr>
<tr>
<td></td>
<td>executed.</td>
</tr>
<tr>
<td>Guard Band</td>
<td>Amount of power that has been placed in reserve for power demand spikes and that</td>
</tr>
<tr>
<td></td>
<td>cannot be allocated to a PoE interface.</td>
</tr>
</tbody>
</table>
Table 488: show poe controller Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Power management mode: either Class or Static or high-power.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The mode high-power is available on only ACX2000 routers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• AF_ENHANCE—Controller supports enhanced PoE. The maximum power per PoE port is 18.6 W in static mode (15.4 W in class mode).</td>
<td></td>
</tr>
<tr>
<td>• DEVICE_FAIL—Software download to the controller has failed or the PoE controller is not initialized because of a hardware failure.</td>
<td></td>
</tr>
<tr>
<td>• DOWNLOAD_INIT—Software download to the controller is in the initial phase.</td>
<td></td>
</tr>
<tr>
<td>• AF_MODE—Controller supports standard IEEE 802.3af. The maximum power per PoE port is 15.4 W.</td>
<td></td>
</tr>
<tr>
<td>• AT/AF_COMBO—Controller supports a mix of standard IEEE 802.3af and IEEE 802.3at (PoE+) ports. The maximum power per port is 30 W for IEEE 802.3at (PoE+) ports and 15.4 W for the IEEE 802.3af ports.</td>
<td></td>
</tr>
<tr>
<td>• AT_MODE—Controller supports IEEE 802.3at (PoE+). The maximum power per PoE port is 30 W.</td>
<td></td>
</tr>
<tr>
<td>• SW_DOWNLOAD(n%)—Software download to the controller is in progress.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lldp Priority</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Layer Discovery Protocol (LLDP) priority operating state. The state can be Enabled or Disabled.</td>
<td></td>
</tr>
</tbody>
</table>

LLDP priority allows the PoE controller to assign interfaces the power priority provided by the connected powered device by using LLDP power negotiation rather than the power priority configured on the switch interface.

Sample Output

**show poe controller (EX3200 Switch)**

```
user@switch> show poe controller
Controller index | Maximum power | Power consumption | Guard band | Management | Status       | Lldp Priority
0                | 130.00W       | 81.20W            | 10W        | Static      | AF_ENHANCE   | Disabled
```

**show poe controller (EX8200 Switch)**

```
user@switch> show poe controller
Controller index | Maximum power | Power consumption | Guard band | Management | Status       | Lldp Priority
0                | 792.00W       | 603.50W           | 0W         | Class       | AT/AF_COMBO  | Disabled
4                | 915.00W       | 781.00W           | 0W         | Class       | AT/AF_COMBO  | Disabled
7                | 915.00W       | 0.00W             | 0W         | Class       | AT/AF_COMBO  | Disabled
```

**show poe controller (Controller Software Upgrade in Progress)**

```
user@switch> show poe controller
Controller index | Maximum power | Power consumption | Guard band | Management | Status       | Lldp Priority
0                | 130.00W       | 0.00W             | 0W         | Static      | AF_ENHANCE   | Disabled
```
**New PoE software upgrade available.**
Use 'request system firmware upgrade poe fpc-slot <slot>'
This procedure will take around 10 minutes (recommended to be performed during maintenance)

```
show poe controller (ACX2000 Router)
user@host> show poe controller

Controller index  Maximum power  Power consumption  Guard band  Management  Status  Lldp Priority

   0        130.0 W   14.2 W         0 W      high-power   UP
```
show poe interface

Syntax

```
show poe interface
  <fpc-slot number>
  <interface-name>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 12.2 for ACX2000 routers.

Description

Display the status of PoE interfaces.

Options

- **none**—Display status of all PoE interfaces on the switch or router.
  - **fpc-slot number**—(Optional) (EX6200 or EX8200 switches only) Display the status of
    the PoE interfaces on the specified line card.
  - **interface-name**—(Optional) Display the status of a specific PoE interface on the switch.

Required Privilege

- **view**

Related Documentation

- [show poe controller on page 3979](#)
- Verifying PoE Configuration and Status (CLI Procedure) on page 3974
- Monitoring PoE Power Consumption (CLI Procedure) on page 3971
- Troubleshooting PoE Interfaces on page 3991

List of Sample Output

- [show poe interface on page 3983](#)
- [show poe interface (with LLDP Negotiation) on page 3983](#)
- [show poe interface ge-0/0/3 on page 3984](#)
- [show poe interface fpc-slot 3 on page 3984](#)
- [show poe interface ge-0/1/7 (ACX2000 Universal Access Routers) on page 3985](#)

Output Fields

Table 489 on page 3982 lists the output fields for the `show poe interface` command. Output fields are listed in the approximate order in which they appear.

Table 489: show poe interface Output Fields

<table>
<thead>
<tr>
<th>Field Name (All Interfaces Output)</th>
<th>Field Name (Single Interface Output)</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>PoE Interface</td>
<td>Interface name.</td>
</tr>
<tr>
<td>Admin status</td>
<td>Administrative status</td>
<td>Administrative state of the PoE interface: Enabled or Disabled. If the PoE interface is disabled, it can provide network connectivity, but it cannot provide power to connected devices.</td>
</tr>
</tbody>
</table>
### Table 489: show poe interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name (All Interfaces Output)</th>
<th>Field Name (Single Interface Output)</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper status</td>
<td>Operational status</td>
<td>Operational state of the PoE interface:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>ON</strong>—The interface is currently supplying power to a powered device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>OFF</strong>—PoE is enabled on the interface, but the interface is not currently supplying power to a powered device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Disabled</strong>—PoE is disabled on the interface.</td>
</tr>
<tr>
<td>Max power</td>
<td>Power limit on the interface</td>
<td>Maximum power that can be provided by the interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An (L) next to the value indicates that the value on the port was negotiated by LLDP.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority</td>
<td>Interface power priority: either <strong>High</strong> or <strong>Low</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An (L) next to the value indicates that the value on the port was negotiated by LLDP.</td>
</tr>
<tr>
<td>Power consumption</td>
<td>Power consumed</td>
<td>Amount of power being used by the interface at the time the command is executed.</td>
</tr>
<tr>
<td>Class</td>
<td>Class of power device</td>
<td>IEEE 802.3af (PoE) or IEEE 802.3at (PoE+) class of the powered device. Class 0 is the default class and is used when the class of the powered device is unknown. If no powered device is connected, this field contains <strong>not applicable</strong>.</td>
</tr>
<tr>
<td>PoE Mode</td>
<td>PoE Mode</td>
<td>IEEE PoE standard supported by the interface—either <strong>802.3af</strong> or <strong>802.3at</strong>.</td>
</tr>
</tbody>
</table>

### Sample Output

**show poe interface**

```
user@switch> show poe interface

Interface   Admin status  Oper status  Max power  Priority  Power consumption  Class
ge-0/0/0     Enabled      ON      15.4W     Low      7.9W            0
ge-0/0/1     Enabled      ON      15.4W     Low      3.2W            2
ge-0/0/2     Enabled      ON      15.4W     Low      3.2W            2
ge-0/0/3     Enabled      ON      15.4W     Low      3.2W            2
ge-0/0/4     Enabled      ON      15.4W     Low      3.2W            2
ge-0/0/5     Enabled      ON      15.4W     Low      3.2W            2
ge-0/0/6     Enabled      ON      15.4W     Low      3.2W            2
ge-0/0/7     Enabled      ON      15.4W     Low      3.2W            2
```

**show poe interface (with LLDP Negotiation)**

```
user@switch> show poe interface

Interface   Admin status  Oper status  Max power  Priority  Power consumption  Class
ge-0/0/0     Enabled      ON      17.5W(L)  Low(L)    16.2W           4
ge-0/0/1     Enabled      ON      17.5W(L)  Low(L)    16.0W           4
ge-0/0/2     Enabled      ON      17.5W(L)  High(L)   16.0W           4
ge-0/0/3     Enabled      ON      17.5W(L)  Low(L)    16.0W           4
ge-0/0/4     Enabled      ON      10.1W(L)  Low(L)    10.0W           3
```
show poe interface ge-0/0/3

user@switch> show poe interface ge-0/0/3
PoE interface status:
PoE interface        :  ge-0/0/3
Administrative status :  Enabled
Operational status   :  ON
Power limit on the interface :  7.0W
Priority             :  Low
Power consumed       :  5.3W
Class of power device :  2
PoE Mode              :  802.3af

show poe interface fpc-slot 3

user@switch> show poe interface fpc-slot 3

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-3/0/0</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>20.3W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/1</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>17.8W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/2</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>16.3W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/3</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>High</td>
<td>16.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/4</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>25.9W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/5</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>10.1W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/6</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>16.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/7</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>6.4W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/8</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>5.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/9</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>5.2W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/10</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>21.5W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/11</td>
<td>Enabled</td>
<td>ON</td>
<td>30.0W</td>
<td>Low</td>
<td>21.7W</td>
<td>4</td>
</tr>
<tr>
<td>ge-3/0/12</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/13</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/14</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/15</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/16</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/17</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/18</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/19</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/20</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/21</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/22</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/23</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/24</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/25</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/26</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/27</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>9.4W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/28</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>7.0W</td>
<td>0</td>
</tr>
<tr>
<td>ge-3/0/29</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/30</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/31</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/32</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.0W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/33</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.0W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/34</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/35</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/36</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/37</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/38</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
<tr>
<td>ge-3/0/39</td>
<td>Enabled</td>
<td>ON</td>
<td>15.4W</td>
<td>Low</td>
<td>2.2W</td>
<td>1</td>
</tr>
</tbody>
</table>
show poe interface ge-0/1/7 (ACX2000 Universal Access Routers)

    user@host> show poe interface ge-0/1/7
    PoE interface status:
    PoE interface            : ge-0/1/7
    Administrative status    : Enabled
    Operational status       : Powered-up
    Power limit on the interface : 9.0 W
    Priority                 : Low
    Power consumed           : 14.2 W
    Class of power device    : 4
show poe notification-control

Syntax

```
show poe notification-control
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the state of the PoE notification-control option, which enables or disables PoE SNMP traps.

Required Privilege Level

view

Related Documentation

- show poe controller on page 3979
- show poe interface on page 3982
- Verifying PoE Configuration and Status (CLI Procedure) on page 3974

List of Sample Output

show poe notification-control on page 3987

Output Fields

Table 490 on page 3986 lists the output fields for the show poe notification-control command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC slot</td>
<td>FPC slot number:</td>
</tr>
<tr>
<td></td>
<td>• 0 for a standalone switch</td>
</tr>
<tr>
<td></td>
<td>• Member ID for a Virtual Chassis</td>
</tr>
<tr>
<td>Notification-control-status</td>
<td>Status of notification control:</td>
</tr>
<tr>
<td></td>
<td>• ON—PoE traps are enabled.</td>
</tr>
<tr>
<td></td>
<td>• OFF—PoE traps are disabled.</td>
</tr>
</tbody>
</table>
Sample Output
show poe notification-control

```
user@switch> show poe notification-control
FPC slot       Notification-control-status
  0             OFF
```

Copyright © 2013, Juniper Networks, Inc.
show poe telemetries

**Syntax**

```plaintext
show poe telemetries
  <count (all | number)>
  <interface (all | interface-name)>
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Display a history of power consumption on the specified interface or on all interfaces.

Telemetries must be enabled on the interface before you can display a history of power consumption.

**Options**

- **none**—Displays all records for all interfaces that have power consumption history data.
- **count (all | number)**—(Optional) Specify the number of power consumption records to display. The most recent records are displayed. If you do not specify the count, all available records are displayed.
- **interface (all | interface-name)**—(Optional) Display power consumption records for the specified PoE interface or for all PoE interfaces. If you do not specify interfaces, all interfaces are displayed.

**Required Privilege**

- **view**

**Related Documentation**

- show poe interface on page 3982
- show poe controller on page 3979
- Monitoring PoE Power Consumption (CLI Procedure) on page 3971
- Verifying PoE Configuration and Status (CLI Procedure) on page 3974
- Troubleshooting PoE Interfaces on page 3991

**List of Sample Output**

- show poe telemetries interface all count 2 on page 3989
- show poe telemetries interface ge-0/0/0 count all on page 3989

**Output Fields**

Table 491 on page 3988 lists the output fields for the `show poe telemetries interface` command. Output fields are listed in the approximate order in which they appear.

**Table 491: show poe telemetries interface Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the interface.</td>
</tr>
<tr>
<td>S1 No</td>
<td>Number of the record for the specified interface. Record number 1 is the most recent.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Date and time when the power-consumption data was gathered.</td>
</tr>
</tbody>
</table>
Table 491: show poe telemetries interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Amount of power provided by the specified interface at the time the data was gathered.</td>
</tr>
<tr>
<td>Voltage</td>
<td>Maximum voltage provided by the specified interface at the time the data was gathered.</td>
</tr>
</tbody>
</table>

Sample Output

**show poe telemetries interface all count 2**

```bash
user@switch> show poe telemetries interface all count 2

Interface   Sl No   Timestamp                Power    Voltage
ge-0/0/1    1       03-09-2012 11:52:03 UTC  4.2W     54.9V
            2       03-09-2012 11:47:03 UTC  4.2W     54.8V
ge-0/0/2    1       03-09-2012 11:52:03 UTC  4.2W     54.9V
            2       03-09-2012 11:47:03 UTC  4.1W     54.8V
ge-0/0/3    1       03-09-2012 11:52:03 UTC  4.2W     54.9V
            2       03-09-2012 11:47:03 UTC  4.3W     54.8V
ge-0/0/4    1       03-09-2012 11:52:03 UTC  0.0W     54.9V
            2       03-09-2012 11:47:03 UTC  0.0W     54.8V
ge-0/0/5    1       03-09-2012 11:52:03 UTC  4.2W     54.9V
            2       03-09-2012 11:47:03 UTC  4.2W     54.8V
ge-0/0/6    1       03-09-2012 11:52:03 UTC  4.2W     54.9V
            2       03-09-2012 11:47:03 UTC  4.2W     54.8V
ge-0/0/7    1       03-09-2012 11:52:03 UTC  4.2W     54.9V
```

**show poe telemetries interface ge-0/0/0 count all**

```bash
user@switch> show poe telemetries interface ge-0/0/0 count all

Sl No   Timestamp                Power    Voltage
1       01-27-2008 18:19:58 UTC  15.4W     51.6V
2       01-27-2008 18:18:58 UTC  15.4W     51.6V
3       01-27-2008 18:17:58 UTC  15.4W     51.6V
4       01-27-2008 18:16:58 UTC  15.4W     51.6V
5       01-27-2008 18:15:58 UTC  15.4W     51.6V
6       01-27-2008 18:14:58 UTC  15.4W     51.6V
7       01-27-2008 18:13:58 UTC  15.4W     51.6V
8       01-27-2008 18:12:57 UTC  15.4W     51.6V
9       01-27-2008 18:11:57 UTC  15.4W     51.6V
10      01-27-2008 18:10:57 UTC  15.4W     51.6V
11      01-27-2008 18:09:57 UTC  15.4W     51.6V
12      01-27-2008 18:08:57 UTC  15.4W     51.6V
13      01-27-2008 18:07:57 UTC  15.4W     51.6V
14      01-27-2008 18:06:57 UTC  15.4W     51.6V
15      01-27-2008 18:05:57 UTC  15.4W     51.6V
16      01-27-2008 18:04:56 UTC  15.4W     51.6V
17      01-27-2008 18:03:56 UTC  15.4W     51.6V
18      01-27-2008 18:02:56 UTC  15.4W     51.6V
19      01-27-2008 18:01:56 UTC  15.4W     51.6V
20      01-27-2008 18:00:56 UTC  15.4W     51.6V
21      01-27-2008 17:59:56 UTC  15.4W     51.6V
```
CHAPTER 73

Troubleshooting Procedures

- Troubleshooting PoE Interfaces on page 3991

Troubleshooting PoE Interfaces

<table>
<thead>
<tr>
<th>Problem</th>
<th>A Power over Ethernet (PoE) interface is not supplying power to the powered device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution</td>
<td>Check for the items shown in Table 492 on page 3991.</td>
</tr>
</tbody>
</table>

Table 492: Troubleshooting a PoE Interface

<table>
<thead>
<tr>
<th>Items to Check</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the switch a full PoE model or a partial PoE model?</td>
<td>If you are using a partial PoE model, only interfaces ge-0/0/0 through ge-0/0/7 can function as PoE ports.</td>
</tr>
<tr>
<td>Has PoE capability been disabled for that interface?</td>
<td>Use the <code>show poe interface</code> command to check PoE interface status.</td>
</tr>
<tr>
<td>Is the cable properly seated in the port socket?</td>
<td>Check the hardware.</td>
</tr>
<tr>
<td>Has the PoE power budget been exceeded for the switch?</td>
<td>Use the <code>show poe controller</code> command to check the PoE power budget and consumption for the switch.</td>
</tr>
<tr>
<td>Does the powered device require more power than is available on the interface?</td>
<td>Use the <code>show poe interface</code> command to check the maximum power provided by the interface.</td>
</tr>
<tr>
<td>If the <code>telemetries</code> option has been enabled for the interface, check the history of power consumption.</td>
<td>Use the <code>show poe telemetries</code> command to display the history of power consumption.</td>
</tr>
</tbody>
</table>

Related Documentation

- Example: Configuring PoE Interfaces with Different Priorities on an EX Series Switch on page 3937
- Example: Configuring PoE on ACX2000 Routers
- Verifying PoE Configuration and Status (CLI Procedure) on page 3974
- Monitoring PoE Power Consumption (CLI Procedure) on page 3971
- Configuring PoE (CLI Procedure) on page 3942
PART 24

Port Security

- Overview on page 3995
- Configuration on page 4017
- Administration on page 4071
Overview

Port Security Overview

- Port Security Overview on page 3995
- Understanding DAI for Port Security on page 3997
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 4000
- Understanding DHCP Snooping for Port Security on page 4004
- Understanding IP Source Guard for Port Security on EX Series Switches on page 4010
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 4013
- Understanding Persistent MAC Learning (Sticky MAC) on page 4014
- Understanding Trusted DHCP Servers for Port Security on page 4016

Port Security Overview

Ethernet LANs are vulnerable to attacks such as address spoofing (forging) and Layer 2 denial of service (DoS) on network devices. Port security features help protect the access ports on your switch against the loss of information and productivity that can result from such attacks.

Juniper Networks Junos operating system (Junos OS) provides features to help secure ports on the switch. Ports can be categorized as either trusted or untrusted. You apply policies appropriate to each category to protect ports against various types of attacks.

Basic port security features are enabled in the switch's default configuration. You can configure additional features with minimal configuration steps.

Depending on the particular feature, you can configure the feature either on VLANs or interfaces.
Port security features supported on switches are:

- **DHCP option 82**—Also known as the DHCP relay agent information option. This feature helps protect the switch against attacks such as spoofing of IP addresses and media access control (MAC) addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

- **DHCP snooping**—Filters and blocks ingress DHCP server messages on untrusted ports; builds and maintains an IP address to MAC address binding (IP-MAC binding) database, which is called the DHCP snooping database. DHCP snooping is enabled on a VLAN. The details of enabling DHCP snooping depend on the particular switch.

  **NOTE:** Most port security features depend on DHCP snooping. However, DHCP snooping is not enabled in the default switch configurations.

- **Dynamic ARP inspection (DAI)**—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made on the basis of the results of those comparisons. You enable DAI on a VLAN.

- **IP source guard**—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. With IP source guard enabled, the source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is forwarded if the source IP-MAC binding is valid; if the binding is not valid, the packet is discarded. You enable IP source guard on a VLAN.

  **NOTE:** IP source guard is not supported on the QFX Series.

- **MAC limiting**—Protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You can enable MAC limiting on an interface.

- **MAC move limiting**—(Not supported on EX9200) Tracks MAC movement and detects MAC spoofing on access ports. You enable this feature on a VLAN.

- **Persistent MAC learning**—Also known as sticky MAC. Persistent MAC learning enables interfaces to retain dynamically learned MAC addresses across switch reboots. You enable this feature on an interface.

- **Trusted DHCP server**—Configuring the DHCP server on a trusted port protects against rogue DHCP servers sending leases. You enable this feature on an interface (port). By default, access ports are untrusted, and trunk ports are trusted. (Access ports are the switch ports that connect to Ethernet endpoints such as user PCs and laptops, servers, and printers. Trunk ports are the switch ports that connect to other Ethernet switches or to routers.)

**Related Documentation**

- Security Features for EX Series Switches Overview on page 4085
- Understanding DHCP Snooping for Port Security
Understanding DAI for Port Security

Dynamic ARP inspection (DAI) protects switches against ARP spoofing.

DAI inspects Address Resolution Protocol (ARP) packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP spoofing (also known as ARP poisoning or ARP cache poisoning). ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the media access control (MAC) address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

ARP packets are sent to the Routing Engine and are rate-limited to protect the switch from CPU overload.

Address Resolution Protocol

Sending IP packets on a multi-access network requires mapping an IP address to an Ethernet MAC address.

Ethernet LANs use ARP to map MAC addresses to IP addresses.

The switch maintains this mapping in a cache that it consults when forwarding packets to network devices. If the ARP cache does not contain an entry for the destination device, the host (the DHCP client) broadcasts an ARP request for that device’s address and stores the response in the cache.

ARP Spoofing

ARP spoofing is one way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the LAN. Instead of the switch sending traffic to the proper network device, the switch sends the traffic to the device with the spoofed address that is impersonating the proper device. If the impersonating device is the attacker’s machine, the attacker receives all the traffic from the switch that must have gone to another device. The result is that traffic from the switch is misdirected and cannot reach its proper destination.
One type of ARP spoofing is gratuitous ARP, which is when a network device sends an ARP request to resolve its own IP address. In normal LAN operation, gratuitous ARP messages indicate that two devices have the same MAC address. They are also broadcast when a network interface card (NIC) in a device is changed and the device is rebooted, so that other devices on the LAN update their ARP caches. In malicious situations, an attacker can poison the ARP cache of a network device by sending an ARP response to the device that directs all packets destined for a certain IP address to go to a different MAC address instead.

To prevent MAC spoofing through gratuitous ARP and through other types of spoofing, the switches examine ARP responses through DAI.

**Dynamic ARP Inspection**

DAI examines ARP requests and responses on the LAN and validates ARP packets. The switch intercepts ARP packets from an access port and validates them against the DHCP snooping database. If no IP-MAC entry in the database corresponds to the information in the ARP packet, DAI drops the ARP packet and the local ARP cache is not updated with the information in that packet. DAI also drops ARP packets when the IP address in the packet is invalid. ARP probe packets are not subjected to dynamic ARP inspection. The switch always forwards such packets.

Junos OS for EX Series switches and the QFX Series uses DAI for ARP packets received on access ports because these ports are untrusted by default. Trunk ports are trusted by default, and therefore ARP packets bypass DAI on them.

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

If you set an interface to be a DHCP trusted port, it is also trusted for ARP packets.

---

**NOTE:**

- If your switch uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see “Enabling a Trusted DHCP Server (CLI Procedure)” on page 4036 for information about configuring an access interface to be a DHCP trusted port.

- If your switch is not using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, see Enabling a Trusted DHCP Server (CLI Procedure) for information about configuring an access interface to be a DHCP trusted port.

For packets directed to the switch to which a network device is connected, ARP queries are broadcast on the VLAN. The ARP responses to those queries are subjected to the DAI check.

For DAI, all ARP packets are trapped to the PFE. To prevent CPU overloading, ARP packets destined for the Routing Engine are rate-limited.
If the DHCP server goes down and the lease time for an IP-MAC entry for a previously valid ARP packet runs out, that packet is blocked.

**Prioritizing Inspected Packets**

**NOTE:** Prioritizing inspected packets is not supported on the QFX Series.

You can use class-of-service (CoS) forwarding classes and queues to prioritize DAI packets for a specified VLAN. This type of configuration places inspected packets for that VLAN in the egress queue, that you specify, ensuring that the security procedure does not interfere with the transmission of high-priority traffic.

**Related Documentation**

- Port Security Overview on page 3995
- Understanding DHCP Snooping for Port Security
  - Example: Configuring Basic Port Security Features
  - Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch
  - Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks
  - Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017
  - Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic
  - Enabling Dynamic ARP Inspection (CLI Procedure)
  - Enabling Dynamic ARP Inspection (CLI Procedure) on page 4035
  - Enabling Dynamic ARP Inspection (J-Web Procedure) on page 4035
Understanding DHCP Option 82 for Port Security on EX Series Switches

You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect Juniper Networks EX Series Ethernet Switches against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Hosts on untrusted access interfaces on Ethernet LAN switches send requests for IP addresses to access the Internet. The switch forwards or relays these requests to DHCP servers, and the servers send offers for IP address leases in response. Attackers can use these messages to perpetrate address spoofing and starvation.

Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client. The Juniper Networks Junos operating system (Junos OS) implementation of DHCP option 82 supports RFC 3046, DHCP Relay Agent Information Option, at http://tools.ietf.org/html/rfc3046.

This topic covers:

- DHCP Option 82 Processing on page 4000
- Suboption Components of Option 82 on page 4001
- Configurations of the EX Series Switch That Support Option 82 on page 4001

DHCP Option 82 Processing

If DHCP option 82 is enabled on a VLAN, then when a network device—a DHCP client—that is connected to the VLAN on an untrusted interface sends a DHCP request, the switch inserts information about the client’s network location into the packet header of that request. The switch then sends the request to the DHCP server. The DHCP server reads the option 82 information in the packet header and uses it to implement the IP address or another parameter for the client. See “Suboption Components of Option 82” on page 4001 for details about option 82 information.

NOTE:

- If your switch uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 only for a specific VLAN. See “Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)” on page 4039.

- If your switch is not using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, you can enable DHCP option 82 either for a specific VLAN or for all VLANs. See Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure).
When option 82 is enabled on a VLAN, the following sequence of events occurs when a DHCP client sends a DHCP request:

1. The switch receives the request and inserts the option 82 information in the packet header.
2. The switch forwards (or relays) the request to the DHCP server.
3. The server uses the DHCP option 82 information to formulate its reply and sends a response to the switch. It does not alter the option 82 information.
4. The switch strips the option 82 information from the response packet.
5. The switch forwards the response packet to the client.

NOTE: To use the DHCP option 82 feature, you must ensure that the DHCP server is configured to accept option 82. If it is not configured to accept option 82, then when it receives requests containing option 82 information, it does not use the information in setting parameters and it does not echo the information in its response message.

Suboption Components of Option 82
Option 82 as implemented on an EX Series switch comprises the suboptions circuit ID, remote ID, and vendor ID. These suboptions are fields in the packet header:

- circuit ID—Identifies the circuit (interface and/or VLAN) on the switch on which the request was received. The circuit ID contains the interface name and/or VLAN name, with the two elements separated by a colon—for example, ge-0/0/10:vlan1, where ge-0/0/10 is the interface name and vlan1 is the VLAN name. If the request packet is received on a Layer 3 interface, the circuit ID is just the interface name—for example, ge-0/0/10.
- remote ID—Identifies the host. See remote-id for details.
- vendor ID—Identifies the vendor of the host. If you specify the vendor-id option but do not enter a value, the default value Juniper is used. To specify a value, you type a character string.

Configurations of the EX Series Switch That Support Option 82
Configurations of the EX Series switch that support option 82 are:

- Switch, Clients and DHCP Server Are on Same VLAN on page 4002
- Switch Acts as a Relay Agent on page 4002
Switch, Clients and DHCP Server Are on Same VLAN

If the switch, the DHCP clients, and the DHCP server are all on the same VLAN, the switch forwards the requests from the clients on untrusted access interfaces to the server on a trusted interface. See Figure 51 on page 4002.

Figure 51: DHCP Clients, Switch, and DHCP Server Are All on Same VLAN

Switch Acts as a Relay Agent

The switch functions as a relay agent (extended relay server) when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as RVIs. Figure 52 on page 4003 illustrates a scenario for the switch acting as an extended relay server; in this instance, the switch relays requests to the server.
Figure 52: Switch Acting as an Extended Relay Server

- Port Security Overview on page 3995
- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
Understanding DHCP Snooping for Port Security

NOTE: This topic includes information about enabling DHCP snooping when using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Understanding DHCP Snooping for Port Security. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. When DHCP snooping is enabled on a VLAN, the system snoops the DHCP messages to view DHCP lease information and build and maintain a database of valid IP address to MAC address (IP-MAC) bindings called the DHCP snooping database. Only clients with valid bindings are allowed access to the network.

- DHCP Snooping Basics on page 4004
- DHCP Snooping Process on page 4005
- DHCP Server Access on page 4006
- DHCP Snooping Table on page 4009
- Static IP Address Additions to the DHCP Snooping Database on page 4009
- Snooping DHCP Packets That Have Invalid IP Addresses on page 4009

**DHCP Snooping Basics**

Dynamic Host Configuration Protocol (DHCP) allocates IP addresses dynamically, leasing addresses to devices so that the addresses can be reused when no longer needed. Hosts and end devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN.

DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

By default, all trunk ports on the switch are trusted and all access ports are untrusted for DHCP snooping.

DHCP snooping is enabled automatically by Junos OS software when you configure any port security features at the `edit vlans vlan-name forwarding-options dhcp-security` hierarchy level.

When DHCP snooping is enabled, the lease information from the switch is used to create the DHCP snooping database. See “Configuring Port Security (CLI Procedure)” on page 4023 for additional information.

NOTE: DHCP snooping is not enabled in the default switch configuration.
Entries in the DHCP database are updated in these events:

- When a DHCP client releases an IP address (sends a DHCPRELEASE message), the associated mapping entry is deleted from the database.
- If you move a network device from one VLAN to another, typically the device needs to acquire a new IP address. Therefore, its entry in the database, including the VLAN ID, is updated.
- When the lease time (timeout value) assigned by the DHCP server expires, the associated entry is deleted from the database.

**TIP:** By default, the IP-MAC bindings are lost when the switch is rebooted and DHCP clients (the network devices, or hosts) must reacquire bindings. However, you can configure the bindings to persist by setting the `dhcp-snooping-file` statement to store the database file either locally or remotely.

You can configure the switch to snoop DHCP server responses only from specific VLANs. Doing this prevents spoofing of DHCP server messages.

You configure DHCP snooping per VLAN, not per interface (port). DHCP snooping is disabled by default. The details of the enabling or configuring DHCP snooping depend on the particular switch.

**DHCP Snooping Process**

The basic process of DHCP snooping consists of the following steps:

**NOTE:** When DHCP snooping is enabled for a VLAN, all DHCP packets sent from that network devices in that VLAN are subjected to DHCP snooping. The final IP-MAC binding occurs when the DHCP server sends DHCPACK to the DHCP client.

1. The network device sends a DHCPDISCOVER packet to request an IP address.
2. The switch forwards the packet to the DHCP server.
3. The server sends a DHCPOFFER packet to offer an address. If the DHCPOFFER packet is from a trusted interface, the switch forwards the packet to the DHCP client.
4. The network device sends a DHCPREQUEST packet to accept the IP address. The switch adds an IP-MAC placeholder binding to the database. The entry is considered a placeholder until a DHCPACK packet is received from the server. Until then, the IP address could still be assigned to some other host.
5. The server sends a DHCPACK packet to assign the IP address or a DHCPNAK packet to deny the address request.
6. The switch updates the DHCP database in accordance with the type of packet received:
Upon receipt of a DHCPACK packet, the switch updates lease information for the IP-MAC binding in its database.

Upon receipt of a DHCPNACK packet, the switch deletes the placeholder.

**NOTE:** The DHCP database is updated only after the DHCPREQUEST packet has been sent.

For general information about the messages that the DHCP client and DHCP server exchange during the assignment of an IP address for the client, see the Junos OS System Basics Configuration Guide.

**DHCP Server Access**

A switch's access to the DHCP server can be configured in three ways:

- **Switch, DHCP Clients, and DHCP Server Are All on the Same VLAN on page 4006**
- **Switch Acts as DHCP Server on page 4007**
- **Switch Acts as Relay Agent on page 4008**

**Switch, DHCP Clients, and DHCP Server Are All on the Same VLAN**

When the switch, DHCP clients, and DHCP server are all members of the same VLAN, the DHCP server can be connected to the switch in one of two ways:

**NOTE:** To enable DHCP snooping on the VLAN, set [edit vlans vlan-name forwarding-options] dhcp-security.

- The server is directly connected to the same switch as the one connected to the DHCP clients (the hosts, or network devices, that are requesting IP addresses from the server). The VLAN is enabled for DHCP snooping to protect the untrusted access ports. The trunk port is configured by default as a trusted port. See Figure 53 on page 4007.
- The server is connected to an intermediary switch (Switch 2) that is connected through a trunk port to the switch (Switch 1) that the DHCP clients are connected to. Switch 2 is being used as a transit switch. The VLAN is enabled for DHCP snooping to protect the untrusted access ports of Switch 1. The trunk port is configured by default as a trusted port. See Figure 54 on page 4007—in the figure, ge-0/0/11 is a trusted trunk port.
Figure 53: DHCP Server Connected Directly to Switch

Switch Acts as DHCP Server

The switch itself is configured as a DHCP server; this is known as a "local" configuration. See Figure 55 on page 4008.
Figure 55: Switch Is the DHCP Server

Switch Acts as Relay Agent

The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. The Layer 3 interfaces on the switch are configured as routed VLAN interfaces (RVIs,) or integrated routing and bridging (IRB) interfaces. The trunk interfaces are trusted by default.

These two scenarios illustrate the switch acting as a relay agent:

- The DHCP server and clients are in different VLANs.
- The switch is connected to a router that is in turn connected to the DHCP server. See Figure 56 on page 4009.
The software creates a DHCP snooping information table that displays the content of the DHCP snooping database. The table shows current IP-MAC bindings, as well as lease time, type of binding, names of associated VLANs, and associated interface.

To display the contents of the DHCP snooping database, issue the operational mode command `show dhcp-security binding`.

Static IP Address Additions to the DHCP Snooping Database

You can add specific static IP addresses to the database as well as have the addresses dynamically assigned through DHCP snooping. To add static IP addresses, you supply the IP address, the MAC address of the device, the interface on which the device is connected, and the VLAN with which the interface is associated. No lease time is assigned to the entry. The statically configured entry never expires.

Snooping DHCP Packets That Have Invalid IP Addresses

If you enable DHCP snooping on a VLAN and then devices on that VLAN send DHCP packets that request invalid IP addresses, these invalid IP addresses will be stored in the DHCP snooping database until they are deleted when their default timeout is reached. To eliminate this unnecessary consumption of space in the DHCP snooping database, the switch drops the DHCP packets that request invalid IP addresses. The invalid IP addresses are:

- 0.0.0.0
- 128.0.x.x
- 191.255.x.x
Related Documentation

- Port Security Overview on page 3995
- Understanding Trusted DHCP Servers for Port Security on page 4016
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 4000
- Understanding DHCP Services for Switches
- DHCP/BOOTP Relay for Switches Overview
- Enabling a Trusted DHCP Server (CLI Procedure) on page 4036
- Enabling DHCP Snooping (J-Web Procedure)
- Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 4038

Understanding IP Source Guard for Port Security on EX Series Switches

Ethernet LAN switches are vulnerable to attacks that involve spoofing (forging) of source IP addresses or source MAC addresses. You can use the IP source guard access port security feature on Juniper Networks EX Series Ethernet Switches to mitigate the effects of these attacks.

- IP Address Spoofing on page 4010
- How IP Source Guard Works on page 4010
- The IP Source Guard Database on page 4011
- Typical Uses of Other Junos Operating System (Junos OS) Features with IP Source Guard on page 4011

IP Address Spoofing

Hosts on access interfaces can spoof source IP addresses and source MAC addresses by flooding the switch with packets containing invalid addresses. Such attacks combined with other techniques such as TCP SYN flood attacks can result in denial-of-service (DoS) attacks. With source IP address or source MAC address spoofing, the system administrator cannot identify the source of the attack. The attacker can spoof addresses on the same subnet or on a different subnet.

How IP Source Guard Works

IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.
NOTE:

- If your switch uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style, DHCP snooping is enabled automatically when you enable IP source guard on a VLAN. See “Configuring IP Source Guard (CLI Procedure)” on page 4029.

- If your switch is not using Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style and you enable IP source guard on a VLAN, you must also explicitly enable DHCP snooping on that VLAN. Otherwise, the default value of no DHCP snooping applies to the VLAN.

IP source guard applies its checking rules to packets sent from untrusted access interfaces on those VLANs. By default, on EX Series switches, access interfaces are untrusted and trunk interfaces are trusted. IP source guard does not check packets that have been sent to the switch by devices connected to either trunk interfaces or to trusted access interfaces so that a DHCP server can be connected to that interface to provide dynamic IP addresses.

NOTE: IP source guard is not supported on trunk interfaces regardless of whether the trunk interface is trusted or untrusted.

IP source guard obtains information about IP address to MAC address binding (IP-MAC binding) from the DHCP snooping database. It causes the switch to validate incoming IP packets against the entries in that database.

After the DHCP snooping database has been populated either through dynamic DHCP snooping or through configuration of specific static IP address/MAC address bindings, the IP source guard feature builds its database. It then checks incoming packets from access interfaces on the VLANs on which it is enabled. If the source IP addresses and source MAC addresses match the IP source guard binding entries, the switch forwards the packets to their specified destination addresses. If there are no matches, the switch discards the packets.

The IP Source Guard Database

For information about how to display the IP source guard database, issue the operational mode command that appears in the command-line interface (CLI):

- `show ip-source-guard`
- `show dhcp-security binding ip-source-guard`

Typical Uses of Other Junos Operating System (Junos OS) Features with IP Source Guard

You can configure IP source guard with various other features on the EX Series switch to provide access port security, including:
- VLAN tagging (used for voice VLANs)
- GRES (Graceful Routing Engine switchover)
- Virtual Chassis configurations (See “EX Series Switch Software Features Overview” on page 27 for list of models that support IP Source Guard.)
- Link aggregation groups (LAGs)
- 802.1X user authentication in single supplicant, single-secure supplicant, or multiple supplicant mode.

**NOTE:** If you are implementing 802.1X user authentication in single-secure supplicant or multiple supplicant mode, use the following configuration guidelines:

- If the 802.1X interface is part of an untagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has untagged membership.
- If the 802.1X interface is part of a tagged MAC-based VLAN and you want to enable IP source guard and DHCP snooping on that VLAN, you must enable IP source guard and DHCP snooping on all dynamic VLANs in which the interface has tagged membership.

**Related Documentation**

- Understanding DHCP Snooping for Port Security
- Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN
- Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017
Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches

MAC limiting for port security protects against flooding of the Ethernet switching table (also known as the MAC forwarding table or Layer 2 forwarding table). You enable this feature on interfaces (ports).

MAC move limiting detects MAC movement and MAC spoofing on access interfaces. You enable this feature on VLANs.

This topic describes the various method of MAC limiting and MAC move limiting for port security:

- MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces on page 4013
- MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed to Access Interfaces on page 4013
- MAC Move Limiting for Port Security by Monitoring MAC Address Moves within VLANs on page 4014

MAC Limiting for Port Security by Limiting the Number of MAC Addresses That Can be Learned on Interfaces

One method to enhance port security is to set the maximum number of MAC addresses that can be learned (added to the Ethernet switching table) on any of the following:

- A specific access interface (port)
- All access interfaces
- A specific access interface on the basis of its membership within a specific virtual LAN (VLAN membership MAC limit)

![NOTE: Static MAC addresses do not count toward the limit you specify for dynamic MAC addresses.]

When you are configuring the maximum MAC limit for an interface, you can choose the action that occurs on incoming packets when the MAC limit is exceeded. For additional information about configuring MAC limit for an interface, see Configuring MAC Limiting (CLI Procedure) or “Configuring MAC Limiting (CLI Procedure)” on page 2132.

MAC Limiting for Port Security by Specifying MAC Addresses That Are Allowed to Access Interfaces

Another method to enhance port security is to configure specific MAC addresses as allowed MAC addresses for specific access interfaces. Any MAC address that is not in the list of the configured addresses is not learned and the switch logs a message.

Allowed MAC binds MAC addresses to a VLAN so that the address does not get registered outside the VLAN. If an allowed MAC setting conflicts with a dynamic MAC setting, the allowed MAC setting takes precedence.
MAC Move Limiting for Port Security by Monitoring MAC Address Moves within VLANs

MAC move limiting causes the switch to limit and track the frequency with which a MAC address can move to a new interface (port). It can help prevent MAC spoofing, and it can also detect and prevent loops.

NOTE: MAC move limiting is not supported on EX9200.

If a MAC address moves more than the configured number of times within one second, the switch performs the configured action. You can configure MAC move limiting to apply to all VLANs or to a specific VLAN.

Related Documentation
- Port Security Overview on page 3995
- Configuring MAC Limiting (J-Web Procedure) on page 4031
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 2023
- Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure)
- Adding a Static MAC Address Entry to the Ethernet Switching Table (CLI Procedure) on page 2131

Understanding Persistent MAC Learning (Sticky MAC)

Persistent MAC learning, also known as sticky MAC, is a port security feature that enables an interface to retain dynamically learned MAC addresses when the switch is restarted or if the interface goes down and is brought back online.

Persistent MAC address learning is disabled by default. You can enable persistent MAC address learning in conjunction with MAC limiting to restrict the number of persistent MAC addresses. You enable this feature on interfaces.

Configure persistent MAC learning on an interface to:

- Prevent traffic losses for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic after a restart.
- Protect the switch against security attacks. Use persistent MAC learning in combination with MAC limiting to protect against attacks, such as Layer 2 denial-of-service (DoS) attacks, overflow attacks on the Ethernet switching table, and DHCP starvation attacks, by limiting the MAC addresses allowed while still allowing the interface to dynamically learn a specified number of MAC addresses. The interface is secured because after the limit has been reached, additional devices cannot connect to the port.
By configuring persistent MAC learning along with MAC limiting, you enable interfaces to learn MAC addresses of trusted workstations and servers from the time when you connect the interface to your network until the limit for MAC addresses is reached, and ensure that after this limit is reached, new devices will not be allowed to connect to the interface even if the switch restarts. As an alternative to using persistent MAC learning with MAC limiting, you can statically configure each MAC address on each port or allow the port to continuously learn new MAC addresses after restarts or interface-down events. Allowing the port to continuously learn MAC addresses represents a security risk.

**NOTE:** While a switch is restarting or an interface is coming back up, there might be a short delay before the interface can learn more MAC addresses. This delay occurs while the system re-enters previously learned persistent MAC addresses into the forwarding database for the interface.

**TIP:** If you move a device within your network that has a persistent MAC address entry on the switch, use the clear ethernet-switching table persistent-mac command to clear the persistent MAC address entry from the interface. If you move the device and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address of the device and the device will not be able to connect.

If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect. However, if you do not clear the persistent MAC address on the original port, then when the port restarts, the system reinstalls the persistent MAC address in the forwarding table for that port. If this occurs, the persistent MAC address is removed from the new port and the device loses connectivity.

Consider the following configuration guidelines when configuring persistent MAC learning:

- Interfaces must be configured in access mode (use the `port-mode` configuration statement or, for switches operating on the Enhanced Layer 2 Software (ELS) configuration style, the `interface-mode` configuration statement).
- You cannot enable persistent MAC learning on an interface on which 802.1x authentication is configured.
- You cannot enable persistent MAC learning on an interface that is part of a redundant trunk group.
- You cannot enable persistent MAC learning on an interface on which `no-mac-learning` is enabled.

**Related Documentation**
- Port Security Overview on page 3995
- Configuring Persistent MAC Learning (CLI Procedure)
- Configuring Persistent MAC Learning (CLI Procedure) on page 4032 (ELS)
Understanding Trusted DHCP Servers for Port Security

Any interface on the switch that connects to a DHCP server can be configured as a trusted port. Configuring a DHCP server on a trusted port protects against rogue DHCP servers sending leases.

Ensure that the DHCP server interface is physically secure—that is, that access to the server is monitored and controlled at the site—before you configure the port as trusted.

Related Documentation

- Understanding DHCP Snooping for Port Security
- Example: Configuring Basic Port Security Features
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from Rogue DHCP Server Attacks
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017
- Enabling a Trusted DHCP Server (CLI Procedure)
- Enabling a Trusted DHCP Server (CLI Procedure) on page 4036
- Enabling a Trusted DHCP Server (J-Web Procedure) on page 4037
CHAPTER 75

Configuration

- Configuration Examples on page 4017
- Configuration Tasks on page 4022
- Configuration Statements on page 4041

Configuration Examples

- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017

Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

This example describes how to enable IP source guard and DAI on a specified VLAN to protect the switch against spoofed IP/MAC addresses and ARP spoofing attacks. When you enable either IP source guard or DAI, the configuration automatically enables DHCP snooping for the same VLAN.

- Requirements on page 4017
- Overview and Topology on page 4018
- Configuration on page 4019
- Verification on page 4020

Requirements

This example uses the following hardware and software components:

- One EX4300 switch
- Junos OS Release 13.2X50-D10 or later for EX Series switches
• A DHCP server to provide IP addresses to network devices on the switch

Before you configure IP source guard to prevent IP/MAC spoofing or DAI to mitigate ARP spoofing attacks, be sure you have:

• Connected the DHCP server to the switch.
• Configured the VLAN to which you are adding DHCP security features. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.

Overview and Topology

Ethernet LAN switches are vulnerable to attacks on security that involve spoofing (forging) of source MAC addresses or source IP addresses. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. These spoofed packets are sent from hosts connected to untrusted access interfaces on the switch. IP source guard checks the IP source address and MAC source address in a packet sent from a host attached to an untrusted access interface on the switch against entries stored in the DHCP snooping database. If IP source guard determines that the packet header contains an invalid source IP address or source MAC address, it ensures that the switch does not forward the packet—that is, the packet is discarded.

Another type of security attack is ARP spoofing (also known as ARP poisoning or ARP cache poisoning). ARP-spoofing is a way to initiate man-in-the-middle attacks. The attacker sends an ARP packet that spoofs the MAC address of another device on the LAN. Instead of the switch sending traffic to the proper network device, it sends it to the device with the spoofed address that is impersonating the proper device. If the impersonating device is the attacker's machine, the attacker receives all the traffic from the switch that should have gone to another device. The result is that traffic from the switch is misdirected and cannot reach its proper destination.

NOTE: When dynamic ARP inspection (DAI) is enabled, the switch logs the number of invalid ARP packets that it receives on each interface, along with the sender’s IP and MAC addresses. You can use these log messages to discover ARP spoofing on the network.

This example shows how to configure these important port security features on a switch that is connected to a DHCP server. The setup for this example includes the VLAN employee-vlan on the switch. Figure 57 on page 4019 illustrates the topology for this example.

NOTE: The trunk interface connecting to the DHCP server interface is a trusted port by default.
Figure 57: Network Topology for Basic Port Security

The components of the topology for this example are shown in Table 493 on page 4019.

Table 493: Components of the Port Security Topology

<table>
<thead>
<tr>
<th>Properties</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch hardware</td>
<td>One EX4300 or EX9200 switch</td>
</tr>
<tr>
<td>VLAN name and ID</td>
<td>employee-vlan, tag 20</td>
</tr>
<tr>
<td>VLAN subnets</td>
<td>192.0.2.16/28</td>
</tr>
<tr>
<td></td>
<td>192.0.2.17 through 192.0.2.30</td>
</tr>
<tr>
<td></td>
<td>192.0.2.31 is the subnet’s broadcast address</td>
</tr>
<tr>
<td>Interfaces in employee-vlan</td>
<td>ge-0/0/1, ge-0/0/2, ge-0/0/3, ge-0/0/8</td>
</tr>
<tr>
<td>Interface connecting to DHCP server</td>
<td>ge-0/0/8</td>
</tr>
</tbody>
</table>

In this example, the switch has already been configured as follows:

- All access ports are untrusted, which is the default setting.
- The trunk port (ge-0/0/8) is trusted, which is the default setting.
- The VLAN (employee-vlan) has been configured to include the specified interfaces.

**Configuration**

To configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) to protect the switch against IP spoofing and ARP attacks:
To quickly configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping), copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set vlans employee-vlan forwarding-options dhcp-security ip-source-guard
set vlans employee-vlan forwarding-options dhcp-security arp-inspection
```

**Step-by-Step Procedure**

Configure IP source guard and DAI (and thereby, also automatically configure DHCP snooping) on the VLAN:

1. **Configure IP source guard on the VLAN:**
   ```plaintext
   [edit vlans employee-vlan forwarding-options dhcp-security]
   user@switch# set ip-source-guard
   ```

2. **Enable DAI on the VLAN:**
   ```plaintext
   [edit vlans employee-vlan forwarding-options dhcp-security]
   user@switch# set arp-inspection
   ```

**Results**

Check the results of the configuration:

```plaintext
user@switch> show vlans employee-vlan forwarding-options
employee-vlan {
    forwarding-options {
        dhcp-security {
            arp-inspection;
            ip-source-guard;
        }
    }
}
```

**Verification**

Confirm that the configuration is working properly.

- **Verifying That DHCP Snooping Is Working Correctly on the Switch** on page 4020
- **Verifying That IP Source Guard Is Working on the VLAN** on page 4021
- **Verifying That DAI Is Working Correctly on the Switch** on page 4021

**Purpose**

Verify that DHCP snooping is working on the switch.
**Action**  
Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch.

Display the DHCP snooping information when the port on which the DHCP server connects to the switch is trusted. The following output results when requests are sent from the MAC addresses and the server has provided the IP addresses and leases:

```
user@switch> show dhcp-security binding
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Vlan</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.17</td>
<td>00:05:85:3A:82:77</td>
<td>employee-vlan</td>
<td>86265</td>
<td>BOUND</td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td>192.0.2.18</td>
<td>00:05:85:3A:82:79</td>
<td>employee-vlan</td>
<td>86265</td>
<td>BOUND</td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td>192.0.2.19</td>
<td>00:05:85:3A:82:80</td>
<td>employee-vlan</td>
<td>86287</td>
<td>BOUND</td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td>192.0.2.20</td>
<td>00:05:85:3A:82:81</td>
<td>employee-vlan</td>
<td>86287</td>
<td>BOUND</td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td>192.0.2.21</td>
<td>00:05:85:3A:82:83</td>
<td>employee-vlan</td>
<td>86287</td>
<td>BOUND</td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td>192.0.2.22</td>
<td>00:05:85:27:32:88</td>
<td>employee-vlan</td>
<td>86254</td>
<td>BOUND</td>
<td>ge-0/0/3.0</td>
</tr>
</tbody>
</table>

**Meaning**  
When the interface on which the DHCP server connects to the switch has been set to trusted, the output (see preceding sample) shows, for the assigned IP address, the device’s MAC address, the VLAN name, and the time, in seconds, remaining before the lease expires.

**Verifying That IP Source Guard is Working on the VLAN**

**Purpose**  
Verify that IP source guard is enabled and working on the VLAN.

**Action**  
Send some DHCP requests from network devices (here they are DHCP clients) connected to the switch. View the IP source guard information for the data VLAN.

```
user@switch> show dhcp-security binding ip-source-guard
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Vlan</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.17</td>
<td>00:05:85:3A:82:77</td>
<td>employee-vlan</td>
<td>86265</td>
<td>BOUND</td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td>192.0.2.18</td>
<td>00:05:85:3A:82:79</td>
<td>employee-vlan</td>
<td>86265</td>
<td>BOUND</td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td>192.0.2.19</td>
<td>00:05:85:3A:82:80</td>
<td>employee-vlan</td>
<td>86287</td>
<td>BOUND</td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td>192.0.2.20</td>
<td>00:05:85:3A:82:81</td>
<td>employee-vlan</td>
<td>86287</td>
<td>BOUND</td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td>192.0.2.21</td>
<td>00:05:85:3A:82:83</td>
<td>employee-vlan</td>
<td>86287</td>
<td>BOUND</td>
<td>ge-0/0/2.0</td>
</tr>
<tr>
<td>192.0.2.22</td>
<td>00:05:85:27:32:88</td>
<td>employee-vlan</td>
<td>86254</td>
<td>BOUND</td>
<td>ge-0/0/3.0</td>
</tr>
</tbody>
</table>

**Meaning**  
The IP source guard database table contains the VLANs enabled for IP source guard.

**Verifying That DAI Is Working Correctly on the Switch**

**Purpose**  
Verify that DAI is working on the switch.
Action

Send some ARP requests from network devices connected to the switch.

Display the DAI information:

```
user@switch> show dhcp-security arp inspection statistics
ARP inspection statistics:
Interface           Packets received  ARP inspection pass  ARP inspection failed
ge-0/0/1.0                  7                       5                     2
ge-0/0/2.0                 10                      10                     0
ge-0/0/3.0                 12                      12                     0
```

Meaning

The sample output shows the number of ARP packets received and inspected per interface, with a listing of how many packets passed and how many failed the inspection on each interface. The switch compares the ARP requests and replies against the entries in the DHCP snooping database. If a MAC address or IP address in the ARP packet does not match a valid entry in the database, the packet is dropped.

Related Documentation

- Configuring IP Source Guard (CLI Procedure) on page 4029
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 4035
- Enabling Dynamic ARP Inspection (J-Web Procedure) on page 4035

Configuration Tasks

- Configuring Port Security (CLI Procedure) on page 4023
- Configuring Port Security (J-Web Procedure) on page 4024
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 4028
- Configuring IP Source Guard (CLI Procedure) on page 4029
- Configuring MAC Limiting (CLI Procedure) on page 4029
- Configuring MAC Limiting (J-Web Procedure) on page 4031
- Configuring Persistent MAC Learning (CLI Procedure) on page 4032
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 4034
- Enabling Dynamic ARP Inspection (CLI Procedure) on page 4035
- Enabling Dynamic ARP Inspection (J-Web Procedure) on page 4035
- Enabling a Trusted DHCP Server (CLI Procedure) on page 4036
- Enabling a Trusted DHCP Server (J-Web Procedure) on page 4037
- Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 4038
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
Configuring Port Security (CLI Procedure)

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Port Security (CLI Procedure). For ELS details, see "Getting Started with Enhanced Layer 2 Software" on page 3.

Ethernet LANs are vulnerable to attacks such as address spoofing and Layer 2 denial of service (DoS) on network devices. DHCP port security features such as DHCP snooping, DAI (dynamic ARP inspection), IP source guard, and DHCP option 82 help protect the access ports on the switch against the losses of information and productivity that can result from such attacks.

DAI, IP source guard, and DHCP option 82 are configured per VLAN.

The DHCP port security features that you specify for the VLAN apply to all the interfaces included within that VLAN. However, you can create a specific group of access interfaces within the VLAN to have different attributes, such as:

- Specifying a specific interface to have a static IP-MAC address (**static-ip**).
- Specifying an access interface to act as a trusted interface to a DHCP server (**trusted**)
- Specifying a specific interface not to transmit DHCP (**no-option-82**)

**NOTE:**

- If you configure any of these DHCP port security features—including configuring a group of access interfaces—for a specific VLAN, the switch software enables automatically enables DHCP snooping for that VLAN.
- If you explicitly disable DHCP snooping by setting **no-dhcp-snooping** for a specific VLAN, the switch software automatically disables any other DHCP port security features for that VLAN.

**NOTE:** Trunk interfaces are trusted by default. However, on an EX9200 switch, you can override this default behavior and set a trunk interface as untrusted.

You must configure a VLAN prior to configuring these DHCP port security features. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.
DAI, IP source guard, and DHCP option 82 are configured per VLAN. Enabling any one of these features automatically enables DHCP snooping.

For additional details, see:

- Enabling Dynamic ARP Inspection (CLI Procedure) on page 4035
- Configuring IP Source Guard (CLI Procedure) on page 4029
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039

You can override the general port security settings for the VLAN by configuring a group of access interfaces within that VLAN. For details, see:

- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 4034
- Enabling a Trusted DHCP Server (CLI Procedure) on page 4036

**Related Documentation**

- Port Security Overview on page 3995
- Understanding DHCP Snooping for Port Security

### Configuring Port Security (J-Web Procedure)

To configure port security on an EX Series switch using the J-Web interface:

1. Select **Configure > Security > Port Security**.

   The VLAN List table lists all the VLAN names, VLAN identifiers, port members, and port security VLAN features.

   The Interface List table lists all the ports and indicates whether security features have been enabled on the ports.

   **NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:

   - **Edit**—Click this option to modify the security features for the selected port or VLAN.

     Enter information as specified in Table 494 on page 4025 to modify port security settings on VLANs.

     Enter information as specified in Table 495 on page 4027 to modify port security settings on interfaces.

   - **Activate/Deactivate**—Click this option to enable or disable security on the switch.
NOTE: This option is not supported on EX4300 switches.

- **Delete**—Click this option to delete the security features of the selected port or VLAN.

NOTE: This option is supported only on EX4300 switches.

---

### Table 494: Port Security Settings on VLANs

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General tab</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable DHCP Snooping on VLAN</td>
<td>Allows the switch to monitor and control DHCP messages received from untrusted devices connected to the switch. Builds and maintains a database of valid IP addresses/MAC address bindings. (By default, access ports are untrusted and trunk ports are trusted.)</td>
<td>Select to enable DHCP snooping on a specified VLAN or all VLANs. TIP: For private VLANs (P-VLANs), enable DHCP snooping on the primary VLAN. If you enable DHCP snooping only on a community VLAN, DHCP messages coming from P-VLAN trunk ports are not snooped.</td>
</tr>
<tr>
<td>Enable ARP Inspection on VLAN</td>
<td>Uses information in the DHCP snooping database to validate ARP packets on the LAN and protect against ARP cache poisoning.</td>
<td>Select to enable ARP inspection on a specified VLAN or all VLANs. (Configure any port on which you do not want ARP inspection to occur as a trusted DHCP server port.)</td>
</tr>
<tr>
<td>MAC movement</td>
<td>Number of MAC movements allowed on the given VLAN.</td>
<td>Enter a number. The default is unlimited.</td>
</tr>
<tr>
<td>MAC movement action</td>
<td>Specifies the action to be taken if the MAC movement limit is exceeded.</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• log—Generate a system log entry, an SNMP trap, or an alarm.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm (default).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• shutdown— Shut down the VLAN and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a disable timeout value. See Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• none—Take no action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EX4300 switches have an additional option:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• drop-and-log—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.</td>
</tr>
</tbody>
</table>

**DHCP Groups**
### Table 494: Port Security Settings on VLANs (continued)

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Specifies the DHCP name of the group.</th>
<th>Enter a name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trusted</th>
<th>Specifies trusting DHCP packets on the selected interface. By default, trunk ports are dhcp-trusted.</th>
<th>To enable this option, select the check box.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No Option-82</th>
<th>Enable or disable the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.</th>
<th>To enable this option, select the check box.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>Specifies the DHCP interface.</th>
<th>Select the required interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ports</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Name of the interface.</th>
<th>Click the <strong>Edit</strong> button of the selected interface, to configure the MAC limit and the MAC limit action.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC Limit</th>
<th>Maximum number of MAC addresses learned on the interface.</th>
<th>Enter a number. The default is unlimited.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC Limit Action</th>
<th>Specifies the action to be taken if the MAC move limit is exceeded.</th>
<th>Action to be taken when MAC limit is reached. The options are:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td>• <strong>drop</strong> — Drop the packet and do not learn. Default is forward.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>drop-and-log</strong> — Drop the packet and generate an alarm, an SNMP trap, or a system log entry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>log</strong> — Do not drop the packet but generate an alarm, an SNMP trap, or a system log entry.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>none</strong> — Forward the packet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>shutdown</strong> — Disable the interface and generate an alarm, an SNMP trap, or a system log entry.</td>
</tr>
</tbody>
</table>
### Table 495: Port Security on Interfaces

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust DHCP</td>
<td>Specifies trusting DHCP packets on the selected interface. By default, trunk ports are dhcp-trusted.</td>
<td>Select to enable DHCP trust.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>MAC Limit</td>
<td>Specifies the number of MAC addresses that can be learned on a single Layer 2 access port. This option is not valid for trunk ports.</td>
<td>Enter a number.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Trunk ports are supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>MAC Limit Action</td>
<td>Specifies the action to be taken if the MAC limit is exceeded. This option is not valid for trunk ports.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- log—Generate a system log entry, an SNMP trap, or an alarm.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- drop—Drop the packets and generate a system log entry, an SNMP trap, or an alarm. (Default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- shutdown—Shut down the interface and generate an alarm. You can mitigate the effect of this option by configuring autorecovery from the disabled state and specifying a disable timeout value. See Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- none—Take no action.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300 switches have an additional option:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- drop-and-log—Drop the packet and generate an alarm, an SNMP trap, or a system log entry.</td>
<td></td>
</tr>
<tr>
<td>Allowed MAC List</td>
<td>Specifies the MAC addresses that are allowed for the interface.</td>
<td>To add a MAC address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the MAC address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click OK.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring Port Security (CLI Procedure)
- Example: Configuring Basic Port Security Features
- Monitoring Port Security
- Port Security Overview on page 3995
Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure)

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

An Ethernet switching access interface on an EX Series switch might shut down or be disabled as a result of one of the following port-security or storm control configurations:

- MAC limiting—`mac-limit` statement is configured with the action `shutdown`.
- MAC move limiting—(Not supported on EX9200) `mac-move-limit` statement is configured with the action `shutdown`.
- Storm control—`storm-control` statement is configured with the action `shutdown`.

You can configure the switch to automatically restore the disabled interfaces to service after a specified period of time. The specified `recovery-timeout` applies to all the interfaces that have been disabled due to MAC limiting, MAC move limiting, or storm control errors.

NOTE: To enable autorecovery, specify the timeout value for the interfaces to recover automatically. There is no default recovery timeout. If you do not specify a timeout value, you need to use the `clear ethernet-switching recovery-timeout` command to clear the errors and restore the interfaces to service.

Specify the recovery timeout period for the interface:

```
[edit interfaces interface-name family ethernet-switching]
user@switch# set recovery-timeout seconds
```

Related Documentation
- Configuring MAC Limiting (CLI Procedure) on page 2132
- Configuring MAC Move Limiting (CLI Procedure)
- Configuring or Disabling Storm Control (CLI Procedure) on page 2023
Configuring IP Source Guard (CLI Procedure)

**NOTE:** This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring IP Source Guard (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

You can use the IP source guard access port security feature on EX Series switches to mitigate the effects of source IP address spoofing and source MAC address spoofing. If IP source guard determines that a host connected to an access interface has sent a packet with an invalid source IP address or source MAC address in the packet header, then IP source guard ensures that the switch does not forward the packet—that is, the packet is discarded.

You enable the IP source guard feature on a specific VLAN. When you enable IP source guard on a VLAN, the switch automatically enables DHCP snooping on that VLAN.

**NOTE:** IP source guard can be applied only to untrusted interfaces.

**NOTE:** You can use IP source guard together with 802.1X user authentication in single supplicant, single-secure supplicant, or multiple supplicant mode.

Before you can enable IP source guard on a VLAN, you must configure the VLAN. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.

To enable IP source guard on a specific VLAN by using the CLI:

```
[edit vlans vlan-name forwarding-options]
user@switch# set ip-source-guard
```

**Related Documentation**
- Verifying That IP Source Guard Is Working Correctly
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017
- Understanding IP Source Guard for Port Security on EX Series Switches on page 4010

Configuring MAC Limiting (CLI Procedure)

**NOTE:** This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring MAC Limiting (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.
This topic describes various ways of configuring a limitation on MAC addresses in packets that are received and forwarded by the switch.

The different ways of setting a MAC limit are described in the following sections:

- Limiting the Number of MAC Addresses Learned by an Interface on page 4030
- Limiting the Number of MAC Addresses Learned by a VLAN on page 4030

**Limiting the Number of MAC Addresses Learned by an Interface**

To secure a port, you can set the maximum number of MAC addresses that can be learned by an interface:

- Set the MAC limit on an interface, and specify an action that the switch takes after the specified limit is exceeded:

  ```
  [edit switch-options]
  user@switch# set interface interface-name interface-mac-limit limit packet-action action
  ```

  After you set a new MAC limit for the interface, the system clears existing entries in the MAC address forwarding table associated with the interface.

**Limiting the Number of MAC Addresses Learned by a VLAN**

To limit the number of MAC addresses learned by a VLAN:

1. Set the maximum number of MAC addresses that can be learned by a VLAN, and specify an action that the switch takes after the specified limit is exceeded:

   ```
   [edit vlans]
   user@switch# set vlan-name switch-options mac-table-size limit packet-action action
   ```

2. Set the maximum number of MAC addresses that can be learned by one or all interfaces in the VLAN, and specify an action that the switch takes after the specified limit is exceeded:

   ```
   [edit vlans]
   user@switch# set vlan-name switch-options interface interface-name interface-mac-limit limit packet-action action
   ```

   ```
   [edit vlans]
   user@switch# set vlan-name switch-options interface-mac-limit limit packet-action action
   ```

**NOTE:** If you specify a MAC limit and packet action for all interfaces in the VLAN and a specific interface in the VLAN, the MAC limit and packet action specified at the specific interface level takes precedence. Also, at the VLAN interface level, only the drop and drop-and-log options are supported.

After you set new MAC limits for a VLAN by using the `mac-table-size` statement or for interfaces associated with a VLAN by using the `interface-mac-limit` statement, the system clears the corresponding existing entries in the MAC address forwarding table.
Configuring MAC Limiting (J-Web Procedure)

MAC limiting protects against flooding of the Ethernet switching table on an EX Series switch. MAC limiting sets a limit on the number of MAC addresses that can be learned on a single Layer 2 access interface (port).

Junos OS provides two MAC limiting methods:

- Maximum number of dynamic MAC addresses allowed per interface—if the limit is exceeded, incoming packets with new MAC addresses are dropped.
- Specific “allowed” MAC addresses for the access interface—Any MAC address that is not in the list of configured addresses is not learned.

You configure MAC limiting for each interface, not for each VLAN. You can specify the maximum number of dynamic MAC addresses that can be learned on a single Layer 2 access interface or on all Layer 2 access interfaces. The default action that the switch will take if that maximum number is exceeded is drop—drop the packet and generate an alarm, an SNMP trap, or a system log entry.

To enable MAC limiting on one or more interfaces using the J-Web interface:

2. Select one or more interfaces from the Interface List.
3. Click the Edit button. If a message appears asking whether you want to enable port security, click Yes.
4. To set a dynamic MAC limit:
   1. Type a limit value in the MAC Limit box.
   2. Select an action from the MAC Limit Action box (optional). The switch takes this action when the MAC limit is exceeded. If you do not select an action, the switch applies the default action, drop.
      - Log—Generate a system log entry.
      - Drop—Drop the packets and generate a system log entry. (Default)
      - Shutdown—Shut down the VLAN and generate a system log entry. You can mitigate the effect of this option by configuring the switch for autorecovery from the disabled state and specifying a disable timeout value. See Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure). If you have not configured autorecovery from the disabled state, you can bring up the interfaces by running the clear ethernet-switching port-error command.
      - None—No action to be taken.
4. To add allowed MAC addresses:
1. Click Add.

2. Type the allowed MAC address and click OK.

Repeat this step to add more allowed MAC addresses.

6. Click OK when you have finished setting MAC limits.

7. Click OK after the configuration has been successfully delivered.

NOTE: You can enable or disable port security on the switch at any time by clicking the Activate or Deactivate button on the Port Security Configuration page. If security status is shown as Disabled when you try to edit settings for any VLANs or interfaces (ports), a message asking whether you want to enable port security appears.

Related Documentation

- Configuring MAC Limiting (CLI Procedure)
- Example: Configuring Allowed MAC Addresses to Protect the Switch from DHCP Snooping Database Alteration Attacks
- Example: Configuring MAC Limiting, Including Dynamic and Allowed MAC Addresses, to Protect the Switch from Ethernet Switching Table Overflow Attacks
- Example: Configuring MAC Limiting to Protect the Switch from DHCP Starvation Attacks
- Verifying That MAC Limiting Is Working Correctly
- Setting the none Action on an Interface to Override a MAC Limit Applied to All Interfaces (CLI Procedure)
- Understanding MAC Limiting and MAC Move Limiting for Port Security on EX Series Switches on page 4013

Configuring Persistent MAC Learning (CLI Procedure)

NOTE: This topic uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Configuring Persistent MAC Learning (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Persistent MAC address learning is disabled by default. You can enable it to:

- Help prevent traffic losses for trusted workstations and servers because the interface does not have to relearn the addresses from ingress traffic after a restart.

- Protect the switch against security attacks—Use persistent MAC learning in combination with MAC limiting to protect against attacks while still avoiding the need to statically configure MAC addresses. When the initial learning of MAC addresses up to the number specified by the MAC limit is done, new addresses will not be allowed even after a
To configure persistent MAC learning on an interface and limit the number of allowed MAC addresses:

1. Enable persistent MAC learning on an interface \texttt{ge-x/y/z} where \(x, y, \) and \(z\) are variables:

   \[
   \begin{align*}
   & \text{[edit "switch-options" on page 2027]} \\
   & \text{user@switch\# set interface ge-x/y/z persistent-learning}
   \end{align*}
   \]

2. To configure a MAC move limit for MAC addresses within a specific VLAN:

   - To limit the number of MAC address movements that can be made by an individual MAC address within the specified VLAN:
     \[
     \begin{align*}
     & \text{[edit vlans vlan-name switch-options]} \\
     & \text{user@switch\# set mac-move-limit limit}
     \end{align*}
     \]
     The action is not specified, so the switch performs the default action drop if it tracks that an individual MAC address within the specified VLAN has moved more than the specified number of times within one second.

   - To limit the number of MAC address movements that can be made by an individual MAC address and to specify the action to be taken when the limit is reached:
     \[
     \begin{align*}
     & \text{[edit vlans vlan-name switch-options]} \\
     & \text{user@switch\# set mac-move-limit limit packet-action action}
     \end{align*}
     \]
     Values for \texttt{action} are:

     - \texttt{drop}—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses.

     - \texttt{drop-and-log}—(EX Series switches only) Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

     - \texttt{log}—(EX Series switches only) Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

     - \texttt{none}—(EX Series switches only) Forward packets with new source MAC addresses, and learn the new source MAC address.

     - \texttt{shutdown}—(EX Series switches only) Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.

   \[\text{TIP: If you move a device within your network that has a persistent MAC address entry on the switch, use the clear ethernet-switching table persistent-mac command to clear the persistent MAC address entry from the interface. If you move the device and do not clear the persistent MAC address from the original port it was learned on, then the new port will not learn the MAC address of the device and the device will not be able to connect.} \]

   If the original port is down when you move the device, then the new port will learn the MAC address and the device can connect. However, if you do not clear the persistent MAC address on the original port, then when the port
restarts, the system reinstall the persistent MAC address in the forwarding
table for that port. If this occurs, the persistent MAC address is removed from
the new port and the device loses connectivity.

Related
Documentation
- Configuring Persistent MAC Learning (CLI Procedure)
- Configuring MAC Move Limiting (CLI Procedure)
- Understanding Persistent MAC Learning (Sticky MAC) on page 4014

Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure)

NOTE: This example uses Junos OS for EX Series switches with support for
the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs
software that does not support ELS, see Configuring Static IP Addresses for
DHCP Bindings on Access Ports (CLI Procedure). For ELS details, see “Getting
Started with Enhanced Layer 2 Software” on page 3.

You can add static (fixed) IP addresses and bind them to fixed MAC addresses in the
DHCP snooping database. These bindings are labeled as static in the database, while
those bindings that have been added through the process of DHCP snooping are labeled
dynamic.

Before you can perform this procedure, you must configure the VLAN. See “Configuring
VLANs for EX Series Switches (CLI Procedure)” on page 2119.

To configure a static IP address/MAC address binding in the DHCP snooping database,
you must first create a group of access interfaces under [edit vlans
vlan-name
forwarding-options dhcp-security]. Creating this group automatically enables DHCP
snooping, which is a prerequisite for creating the DHCP snooping database. You can then
configure a specific interface within the group to have a static IP address that is bound
to a fixed MAC address. If you want to have multiple static IP addresses, configure
additional interfaces within the same group.

To configure a static IP address and MAC address binding in the DHCP snooping database:

[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set group group-name interface interface-name static-ip
ip-address mac
mac-address

If you want to have multiple static IP addresses within the same VLAN, configure additional
interfaces within the same group.

Related
Documentation
- show dhcp-security binding on page 4078
- Verifying That DHCP Snooping Is Working Correctly
- Understanding DHCP Snooping for Port Security
Enabling Dynamic ARP Inspection (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Enabling Dynamic ARP Inspection (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

Dynamic ARP inspection (DAI) protects switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.

Before you can enable DAI on a VLAN, you must configure the VLAN. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.

To enable DAI on a VLAN by using the CLI:

```
[edit vlans vlan-name forwarding-options dhcp-security]
user@switch# set arp-inspection
```

Enabling Dynamic ARP Inspection (J-Web Procedure)

Dynamic ARP inspection (DAI) protects EX Series switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.

You configure DAI for each VLAN, not for each interface (port). By default, DAI is disabled for all VLANs.

To enable DAI on one or more VLANs by using the J-Web interface:

2. Select one or more VLANs from the VLAN list.
3. Click the Edit button. If a message appears asking if you want to enable port security, click Yes.
4. Select the Enable ARP Inspection on VLAN check box and then click OK.
5. Click OK after the command has been successfully delivered.
NOTE: You can enable or disable port security on the switch at any time by clicking the Activate or Deactivate button on the Port Security Configuration page. If security status is shown as Disabled when you try to edit settings for any VLANs or interfaces (ports), the message asking if you want to enable port security appears.

### Related Documentation
- Enabling Dynamic ARP Inspection (CLI Procedure)
- Example: Configuring Basic Port Security Features
- Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks
- Verifying That DAI Is Working Correctly
- Monitoring Port Security
- Understanding DAI for Port Security on page 3997

## Enabling a Trusted DHCP Server (CLI Procedure)

NOTE: This example uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Enabling a Trusted DHCP Server (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

You can configure any interface on a switch that connects to a DHCP server as a trusted interface (port). Configuring a DHCP server on a trusted interface protects against rogue DHCP servers sending leases.

By default, all access interfaces are untrusted, and all trunk interfaces are trusted. However, you can override the default setting for access interfaces by configuring a group of access interfaces within a VLAN, specifying an interface to belong to that group, and then configuring the group as trusted.

Before you can configure a trusted DHCP server, you must configure a VLAN. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.

To configure an untrusted access interface as a trusted interface for a DHCP server by using the CLI:

1. Configure a group within a VLAN with a specific access interface:
   ```
   [edit vlans vlan-name forwarding-options]
   user@switch# set group group-name interface interface-name
   ```
2. Configure that group as **trusted** to make the specified interface contained within the
group a trusted interface:

   ```
   [edit vlans vlan-name forwarding-options dhcp-security group group-name]
   user@switch# set overrides trusted
   ```

**Related Documentation**

- Enabling a Trusted DHCP Server (J-Web Procedure) on page 4037
- Understanding Trusted DHCP Servers for Port Security on page 4016

### Enabling a Trusted DHCP Server (J-Web Procedure)

You can configure any interface on the EX Series switch that connects to a DHCP server
as a trusted interface (port). Configuring a DHCP server on a trusted interface protects
against rogue DHCP servers sending leases.

You configure a trusted DHCP server on an interface, not on a VLAN. By default, all access
interfaces are untrusted and all trunk interfaces are trusted.

To enable a trusted DHCP server on one or more interfaces by using the J-Web interface:

1. Select **Configure>Security>Port Security**.
2. Select one or more interfaces from the Port list.
3. Click the **Edit** button. If a message appears asking if you want to enable port security,
click **Yes**.
4. Select the **Trust DHCP** check box and then click **OK**.
5. Click **OK** after the command has been successfully delivered.

**NOTE:** You can enable or disable port security on the switch at any time by
clicking the **Activate** or **Deactivate** button on the Port Security Configuration
page. If security status is shown as **Disabled** when you try to edit settings for
any VLANs or interfaces (ports), the message asking if you want to enable
port security appears.

**Related Documentation**

- Enabling a Trusted DHCP Server (CLI Procedure)
- Example: Configuring Basic Port Security Features
- Example: Configuring a DHCP Server Interface as Untrusted to Protect the Switch from
Rogue DHCP Server Attacks
- Verifying That a Trusted DHCP Server Is Working Correctly
- Monitoring Port Security
- Understanding Trusted DHCP Servers for Port Security on page 4016
Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)

NOTE: This task uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure). For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

By default, IP-MAC bindings in the DHCP snooping database do not persist. You can configure the IP-MAC bindings in the DHCP database to persist through switch reboots by configuring a storage location for the DHCP database file. When specifying the location for the DHCP database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.

The DHCP snooping database of IP-MAC bindings is created when you enable any of the port security features for a specific VLAN in [edit vlans vlan-name forwarding-options dhcp-security]. DHCP snooping is not enabled by default.

To make the IP-MAC bindings in the DHCP snooping database persist through switch reboots:

- For local storage, specify a local pathname as the location in which to store the DHCP snooping database:

  [edit system processes]
  user@switch# set dhcp-service dhcp-snooping-file local-pathname write-interval seconds

  For example:

  [edit system processes]
  user@switch# set dhcp-service dhcp-snooping-file /var/tmp/test.log write-interval 60

- For remote storage, use ftp://ip-address or ftp://hostname/path as the location in which to store the DHCP snooping database:

  [edit system processes]
  user@switch# set dhcp-service dhcp-snooping-file remote-url write-interval seconds

  For example:

  [edit system processes]
  user@switch# set dhcp-service dhcp-snooping-file location ftp://test:Test123@14.1.2.1 write-interval 60

NOTE: Specify any requisite user credentials for the FTP server before specifying the IP address or hostname. In this example, test is the username and Test123 is the password for FTP server 14.1.2.1.

Related Documentation

• Understanding DHCP Snooping for Port Security
You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the switch against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.

You can configure the DHCP option 82 feature in two topologies:

- The switch, DHCP clients, and DHCP server are all on the same VLAN. The switch forwards the clients’ requests to the server and forwards the server’s responses to the clients. This topic describes this configuration.

- The switch functions as a relay agent when the DHCP clients or the DHCP server is connected to the switch through a Layer 3 interface. On the switch, these interfaces are configured as integrated routing and bridging (IRB) interfaces. The switch relays the clients’ requests to the server and then forwards the server’s responses to the clients. This configuration is described in Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure).

Before you configure DHCP option 82 on the switch, perform these tasks:

- Connect and configure the DHCP server.

  **NOTE:** Your DHCP server must be configured to accept DHCP option 82. If the server is not configured for DHCP option 82, the server does not use the DHCP option 82 information in the requests sent to it when it formulates its reply messages.

- Configure a VLAN on the switch and associate the interfaces on which the clients and the server connect to the switch with that VLAN. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.
To configure DHCP option 82:

1. Specify DHCP option 82 for the VLAN that you configured.
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security]
   user@switch# option-82
   ```

   **NOTE:** If you want to enable DHCP option 82 on all VLANs, you must configure it separately for each specific VLAN.

   The remaining steps are optional.

2. Configure the prefix for the circuit ID suboption to include the switch’s hostname or the routing instance name for the VLAN:
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security option-82]
   user@switch# set circuit-id prefix (host-name | routing-instance-name)
   ```

3. Specify that the circuit ID suboption value contains the interface description rather than the interface name (the default):
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security option-82]
   user@switch# set circuit-id use-interface-description
   ```

4. Specify that the circuit ID suboption value contains the VLAN ID rather than the VLAN name (the default):
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security option-82]
   user@switch# set circuit-id use-vlan-id
   ```

5. Specify that the remote ID suboption is included in the DHCP option 82 information:
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security option-82]
   user@switch# set remote-id
   ```

   **NOTE:** If you do not specify a keyword after `remote-id`, the default value for the remote-id suboption is the interface name.

6. Specify that the remote ID suboption is the hostname of the switch:
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security option-82]
   user@switch# set remote-id host-name
   ```

7. Specify that the remote ID suboption value contains the interface description:
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security option-82]
   user@switch# set remote-id use-interface-description
   ```

8. Specify that the remote ID suboption value contains a character string:
   
   ```
   [edit vlans vlan-name forwarding-options dhcp-security option-82]
   user@switch# set remote-id use-string mystring
   ```

9. Configure a vendor ID suboption:

   - To use the default value (the default value is Juniper), do not type a character string after the `vendor-id` option keyword:
     
     ```
     [edit vlans vlan-name forwarding-options dhcp-security option-82]
     user@switch# set vendor-id
     ```

   - To configure that the vendor ID suboption value contains a character string value that you specify rather than Juniper (the default):
[edit vlans vlan-name forwarding-options dhcp-security option-82]
user@switch# set vendor-id mystring

- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 4000

Configuration Statements

- [edit vlans] Configuration Statement Hierarchy on EX Series Switches on page 4041

[edit vlans] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit vlans] hierarchy level on EX Series switches.

- Supported statements are those that you can use to configure some aspect of a software feature on the switch.

- Unsupported statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

- Supported Statements in the [edit vlans] Hierarchy Level on page 4041
- Unsupported Statements in the [edit vlans] Hierarchy Level on page 4043

Supported Statements in the [edit vlans] Hierarchy Level

The following hierarchy shows the [edit vlans] configuration statements supported on one or more of the EX Series switches:

vlans {
  vlan-name {
    description text-description;
    domain-type bridge;
    forwarding-options {
      dhcp-security {
        arp-inspection;
        group group-name {
          interface interface-name {
            static-ip ip-address {
              mac mac-address;
            }
          }
        }
        overrides {
          no-option82;
          trusted;
        }
      }
    }
  }
}

Copyright © 2013, Juniper Networks, Inc.
ip-source-guard;
no-dhcp-snooping;
option-82 {
  circuit-id {
    prefix {
      host-name;
      logical-system-name;
      routing-instance-name;
    }
    use-interface-description (device | logical);
    use-vlan-id;
  }
  remote-id {
    host-name;
    use-interface-description (device | logical);
    use-string string;
  }
  vendor-id {
    use-string string;
  }
}
filter {
  input filter-name;
  output filter-name;
}
flood {
  input filter-name;
}
}
l3-interface irb.logical-unit-number;
multicast-snooping-options {
  flood-groups [group-names];
  forwarding-cache {
    threshold {
      reuse threshold;
      suppress threshold;
    }
  }
  graceful-restart {
    disable;
    restart-duration duration;
  }
  host-outbound-traffic {
    dot1p bits;
    forwarding-class forwarding-class;
  }
  multichassis-lag-replicate-state;
  nexthop-hold-time time;
  options {
    syslog {
      level level;
      mark interval;
      upto level;
    }
  }
}
traceoptions {
    file filename {
        files number;
        no-world-readable;
        size file-size;
        world-readable;
    }
    flag flag {
        disable;
    }
}
}
switch-options {
    interface interface-name {
        interface-mac-limit limit {
            packet-action action;
        }
        static-mac mac-address;
    }
    interface-mac-limit limit {
        packet-action action;
    }
    mac-move-limit limit {
        packet-action action;
    }
    mac-table-size limit {
        packet-action drop;
    }
    no-mac-learning;
}
vlan-id number;
vlan-id-list [vlan-id | vlan-id–vlan-id];
}

Unsupported Statements in the [edit vlans] Hierarchy Level

All statements in the [edit vlans] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 496: Unsupported [edit vlans] Configuration Statements on EX Series Switches

<table>
<thead>
<tr>
<th>Statement</th>
<th>Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcae-mac-synchronize</td>
<td>[edit vlans]</td>
</tr>
<tr>
<td>no-irb-layer-2-copy</td>
<td>[edit vlans]</td>
</tr>
</tbody>
</table>

NOTE: Variables, such as filename, are not shown in the statements or hierarchies.

Related Documentation

• Example: Connecting Access Switches to a Distribution Switch on page 2083
arp-inspection

Syntax
arp-inspection {
    forwarding-class class-name;
}

Hierarchy Level
- For platforms with ELS:
  [edit vlans vlan-name forwarding-options dhcp-security],
  [edit forwarding-options dhcp-relay ]
- For platforms without ELS:
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name)],
  [edit forwarding-options dhcp-relay ]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Hierarchy level [edit vlans vlan-name forwarding-options dhcp-security] introduced in
Junos OS Release 13.2X50-D10. (See "Getting Started with Enhanced Layer 2 Software"
on page 3 for information about ELS.)

Description
Perform dynamic ARP inspection (DAI) on all VLANs or on the specified VLAN.

NOTE: If you enable DAI at the [edit vlans vlan-name forwarding-options dhcp-security] hierarchy level, you can configure DAI only for a specific VLAN. You cannot configure it for a list or a range of VLAN IDs.

When DAI is enabled, the switch logs invalid ARP packets that it receives on each interface, along with the sender’s IP and MAC addresses.

NOTE: The forwarding-class statement is not available at the [edit vlans vlan-name forwarding-options dhcp-security] hierarchy level.

The remaining statement is explained separately.

NOTE: If you enable arp-inspection at the [edit vlans vlan-name forwarding-options dhcp-security] hierarchy level, DHCP snooping is automatically enabled. Conversely, if you explicitly disable DHCP snooping by specifying no-dhcp-snooping, DAI is automatically disabled.

See “Enabling Dynamic ARP Inspection (CLI Procedure)” on page 4035 for more information about this configuration.

Default
Disabled.
Required Privilege
Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Example: Configuring DHCP Snooping, DAI, and MAC Limiting on a Switch with Access to a DHCP Server Through a Second Switch
- Example: Configuring DHCP Snooping and DAI to Protect the Switch from ARP Spoofing Attacks
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017
- Example: Using CoS Forwarding Classes to Prioritize Snooped Packets in Heavy Network Traffic
- Enabling Dynamic ARP Inspection (CLI Procedure)
- Enabling Dynamic ARP Inspection (J-Web Procedure) on page 4035
**circuit-id**

**Syntax**

```plaintext
circuit-id {  
  prefix hostname;  
  use-interface-description;  
  use-vlan-id;  
}
```

**Hierarchy Level**

- For platforms with ELS:

  ```plaintext
  [edit vlans vlan-name forwarding-options dhcp-security option-82 ]
  ```

- For platforms without ELS:

  ```plaintext
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name) dhcp-option82],  
  [edit forwarding-options helpers bootp dhcp-option82],  
  [edit forwarding-options helpers bootp interface interface-name dhcp-option82]
  ```

**Release Information**


**Description**

Configure the **circuit-id** suboption (suboption 1) of DHCP option 82 (the DHCP relay agent information option) in DHCP packets destined for a DHCP server. This suboption identifies the circuit (the interface, the VLAN, or both) on which the DHCP request arrived.

The remaining statements are explained separately.

**Default**

If DHCP option 82 is enabled on the switch, the circuit ID is supplied by default in the format **interface-name:vlan-name** or, on a Layer 3 interface, just **interface-name**.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
dhcp-security

Syntax  dhcp-security {
    arp-inspection;
    group group-name {
        interface interface-name {
            static-ip ip-address {
                mac mac-address;
            }
        }
        overrides {
            no-option82;
            trusted;
            untrusted;
        }
    }
    ip-source-guard;
    no-dhcp-snooping;
    option-82 {
        circuit-id {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
            }
            use-interface-description (device | logical);
            use-vlan-id;
        }
        remote-id {
            host-name hostname;
            use-interface-description (device | logical);
            use-string string;
        }
        vendor-id {
            use-string string;
        }
    }
}

Hierarchy Level  [edit vlans vlan-name forwarding-options]

Release Information  Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description  Configure port security features on the switch. DHCP snooping is enabled automatically if you configure any of the following port security features within this hierarchy:

- Dynamic ARP inspection (DAI)
- IP source guard
- DHCP option 82
- Static IP

The remaining statements are explained separately.
**Required Privilege**

- Interface—To view this statement in the configuration.
- Interface-control—To add this statement to the configuration.

**Related Documentation**

- Enabling Dynamic ARP Inspection (CLI Procedure) on page 4035
- Configuring IP Source Guard (CLI Procedure) on page 4029
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 4034

### dhcp-service

**Syntax**

```
dhcp-service {
  dhcp-snooping-file (local_pathname | remote_URL);
  write-interval interval;
}
```

**Hierarchy Level**

[edit system processes]

**Release Information**

- Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
- Statement introduced in Junos OS Release 13.2 for the QFX Series.

**Description**

Enable DHCP services on the switch. DHCP services automate network-parameter assignment to network devices. The DHCP service process is enabled by default on your switch. However, by default, IP-MAC bindings in the DHCP snooping database do not persist. You can configure the IP-MAC bindings in the DHCP database to persist through switch reboots by configuring a storage location for the DHCP database file. When specifying the location for the DHCP database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.

The remaining statements are explained separately.

**Required Privilege**

- Admin—To view this statement in the configuration.
- Admin-control—To add this statement to the configuration.

**Related Documentation**

- Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 4038
dhcp-snooping-file

Syntax

dhcp-snooping-file (local_pathname | remote_URL);

write-interval seconds;

}

Hierarchy Level

[edit system processes dhcp-service]

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Ensure that IP-MAC bindings persist through switch reboots by specifying a local pathname or a remote URL for the storage location of the DHCP snooping database file.

The remaining statement is explained separately.

Default

The IP-MAC bindings in the DHCP snooping database file are not persistent. If the switch is rebooted, the bindings are lost.

Required Privilege

Level system—to view this statement in the configuration.

system-control—to add this statement to the configuration.

Related Documentation

• Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure) on page 4038

• Understanding DHCP Snooping for Port Security
group (DHCP Security)

Syntax

```plaintext
group group-name {
  interface interface-name;
  static-ip
}
overrides {
  no-option-82;
  trusted;
  untrusted;
}
}
```

Hierarchy Level

```
[edit vlans vlan-name forwarding-options dhcp-security]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description

Specify the name of a group of access interfaces that you want to configure for DHCP security attributes that are different from the attributes set for other interfaces in the VLAN. A group must contain at least one interface.

The remaining statements are explained separately.

Required Privilege

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

Related Documentation

- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 4034
- Enabling a Trusted DHCP Server (CLI Procedure) on page 4036
- Understanding DHCP Snooping for Port Security
**host-name**

**Syntax**

host-name *host-name*

**Hierarchy Level**

[edit vlans vlan-name forwarding-options dhcp-security option-82 remote-id]

**Release Information**

Statement introduced in Junos OS Release 13.2X50-D10.

**Description**

Use the hostname of the switch as the remote-id suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.

**Required Privilege Level**

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

**Related Documentation**

- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039

**interface (DHCP Security)**

**Syntax**

interface interface-name;
    static-ip;
}

**Hierarchy Level**

[edit vlans vlan-name forwarding-options dhcp-security group group-name]

**Release Information**

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Statement introduced in Junos OS Release 13.2 for the QFX Series.

**Description**

Configure an interface for a static IP address to MAC address binding (IP-MAC binding) or configure an interface to belong to a group within the VLAN that has DHCP security attributes that are different from the attributes of other interfaces in the VLAN.

The remaining statement is explained separately.

**Required Privilege Level**

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 4034
- Enabling a Trusted DHCP Server (CLI Procedure) on page 4036
- Configuring Port Security (CLI Procedure) on page 4023

Copyright © 2013, Juniper Networks, Inc.
**interface-mac-limit**

**Syntax**

```plaintext
interface-mac-limit limit {
    packet-action action;
}
```

**Hierarchy Level**

- [edit bridge-domains bridge-domain-name bridge-options]
- [edit bridge-domains bridge-domain-name bridge-options interface interface-name]
- [edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options]
- [edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options]
- [edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name]
- [edit logical-systems logical-system-name routing-instances routing-instance-name switch-options]
- [edit logical-systems logical-system-name routing-instances routing-instance-name switch-options interface interface-name]
- [edit logical-systems logical-system-name switch-options]
- [edit logical-systems logical-system-name switch-options interface interface-name]
- [edit logical-systems logical-system-name switch-options interface interface-name]
- [edit switch-options on page 2027 interface interface-name]
- [edit vlans on page 2136 vlan-name switch-options]
- [edit vlans on page 2136 vlan-name switch-options interface interface-name]

**Release Information**

Statement introduced in Junos OS Release 8.4.
Support for the `switch-options` statement added in Junos OS Release 9.2.
Support for top-level configuration for the `virtual-switch` type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.
Support for logical systems added in Junos OS Release 9.6.
Support at [edit switch-options], [edit switch-options interface interface-name], [edit vlans vlan-name switch-options], and [edit vlans vlan-name switch-options interface interface-name] hierarchy levels introduced in Junos OS Release 12.3R2 for EX Series switches.
Support at hierarchy levels under [edit vlans vlan-name] introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.
Description: (MX Series routers and EX Series switches) Configure a limit to the number of MAC addresses that can be learned from a bridge domain or VLAN, virtual switch, or set of bridge domains or VLANs.

Default: All devices except the EX Series switches: 1024 MAC addresses for each logical interface; EX Series switches: 65,536 MAC addresses for each interface and VLAN.

Options:

- **limit**—Maximum number of MAC addresses learned from an interface.

  Range: 1 through 131,071 MAC addresses per interface, or 1 through 65,535 MAC addresses per interface

  The remaining statement is explained separately.

Required Privilege Level:

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

Related Documentation:

- Layer 2 Learning and Forwarding for Bridge Domains Overview
- Layer 2 Learning and Forwarding for VLANs Overview
- Layer 2 Learning and Forwarding for Bridge Domains Functioning as Switches with Layer 2 Trunk Ports
- Configuring MAC Limiting (CLI Procedure) on page 2132
ip-source-guard

Syntax  ip-source-guard;

Hierarchy Level  • For platforms with ELS:
  [edit vlans vlan-name forwarding-options dhcp-security]
  • For platforms without ELS:
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name)]

  Hierarchy level [edit vlans vlan-name forwarding-options dhcp-security] introduced in
  Junos OS Release 13.2X50-D10. (See “Getting Started with Enhanced Layer 2 Software”
  on page 3 for information about ELS.)

Description  Perform IP source guard checking on packets sent from access interfaces. Validate source
  IP addresses and source MAC addresses on all VLANs or on the specified VLAN or VLAN
  range. Forward packets with valid addresses and drop those with invalid addresses.

**NOTE:** If you enable IP source guard at the [edit vlans vlan-name
  forwarding-options dhcp-security] hierarchy level, it can be configured only
  for a specific VLAN. You cannot configure it for a list or range of VLAN IDs.

  • ip-source-guard—Enable IP source guard checking.
  • no-ip-source-guard—(Not available in [edit vlans vlan-name forwarding-options
dhcp-security]) Disable IP source guard checking.

**NOTE:** If you enable ip-source-guard at the [edit ethernet-switching-options
secure-access-port vlan (all | vlan-name)] hierarchy level, use the following
guidelines:

Before you configure IP source guard, be sure that you have:

  • Explicitly enabled DHCP snooping on the specific VLAN or specific VLANs
    on which you will configure IP source guard. See Enabling DHCP Snooping
    (CLI Procedure).
  • If you configure IP source guard on specific VLANs rather than on all VLANs,
    you must also enable DHCP snooping explicitly on those VLANs. Otherwise,
    the default behavior of no DHCP snooping applies to that VLAN.

**NOTE:** If you enable ip-source-guard at the [edit vlans vlan-name
forwarding-options dhcp-security] hierarchy level, DHCP snooping is
automatically enabled. Conversely, if you explicitly disable DHCP snooping by specifying `no-dhcp-snooping`, it automatically disables IP source guard for the specified VLAN.

<table>
<thead>
<tr>
<th>Default</th>
<th>Disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Privilege Level</td>
<td>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
| Related Documentation | • Example: Configuring IP Source Guard on a Data VLAN That Shares an Interface with a Voice VLAN  
• Example: Configuring IP Source Guard with Other EX Series Switch Features to Mitigate Address-Spoofing Attacks on Untrusted Access Interfaces  
• Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017  
• Configuring IP Source Guard (CLI Procedure)  
• Configuring IP Source Guard (CLI Procedure) on page 4029 |
mac

Syntax   
\[\text{mac mac-address;}\]

Hierarchy Level   
- For platforms with ELS:
\[\text{[edit vlans \textit{vlan-name} forwarding-options dhcp-security group \textit{group-name} interface \textit{interface-name} static-ip \textit{ip-address}]}\]
- For platforms without ELS:
\[\text{[edit ethernet-switching-options secure-access-port interface (all | \textit{interface-name}) static-ip \textit{ip-address} vlan \textit{vlan-name}]}\]

Release Information   

Description   
Media access control (MAC) address or hardware address of the device connected to the specified interface.

Options   
\texttt{mac-address}—Value (in hexadecimal format) of the address assigned to this device.

Required Privilege Level   
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation   
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure)
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 4034
packet-action

### Syntax

```
packet-action action;
```

### Hierarchy Level

- `edit bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name switch-options interface interface-name interface-mac-limit limit`
- `edit logical-systems logical-system-name switch-options interface interface-name interface-mac-limit limit`
- `edit protocols 12-learning global-mac-limit limit`
- `edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface interface-name interface-mac-limit limit`
- `edit routing-instances routing-instance-name bridge-domains bridge-domain-name switch-options interface interface-name interface-mac-limit limit`
- `edit routing-instances routing-instance-name bridge-domains bridge-domain-name switch-options interface interface-name interface-mac-limit limit`
- `edit routing-instances routing-instance-name protocols evpn interface-mac-limit`
- `edit routing-instances routing-instance-name protocols evpn interface interface-name interface-mac-limit`
- `edit routing-instances routing-instance-name protocols evpn mac-table-size limit`
- `edit routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit`
- `edit routing-instances routing-instance-name switch-options interface interface-name interface-mac-limit limit`
- `edit switch-options interface interface-name interface-mac-limit limit`
- `edit switch-options interface interface-name interface-mac-limit limit`
- `edit switch-options interface interface-name interface-mac-limit limit`
- `edit switch-options interface interface-name interface-mac-limit limit`
- `edit switch-options interface interface-name mac-table-size limit`
- `edit switch-options interface interface-name mac-table-size limit`
- `edit switch-options interface interface-name mac-table-size limit`
- `edit switch-options interface interface-name mac-table-size limit` on page 2027
- `edit vlans vlan-name switch-options interface interface-name interface-mac-limit limit`
- `edit vlans vlan-name switch-options interface-mac-limit limit`
- `edit vlans vlan-name switch-options mac-table-size limit`
- `edit vlans on page 2136 vlan-name switch-options interface interface-name interface-mac-limit limit`
- `edit vlans on page 2136 vlan-name switch-options interface interface-name interface-mac-limit limit`
- `edit vlans on page 2136 vlan-name switch-options interface interface-name interface-mac-limit limit`
- `edit vlans on page 2136 vlan-name switch-options mac-table-size limit`

### Release Information

Statement introduced in Junos OS Release 8.4.

Support for the `switch-options` statement added in Junos OS Release 9.2.

Support for top-level configuration for the `virtual-switch` type of routing instance added in Junos OS Release 9.2. In Junos OS Release 9.1 and earlier, the routing instances hierarchy...
supported this statement only for a VPLS instance or a bridge domain configured within a virtual switch.
Support for logical systems added in Junos OS Release 9.6.
Support for EVPNs introduced in Junos OS Release 13.2 on MX Series 3D Universal Edge Routers.

Description Specify the action taken when packets with new source MAC addresses are received after the MAC address limit is reached. If this statement is not configured, packets with new source MAC addresses are forwarded by default.

Default Disabled. The default is for packets for new source MAC addresses to be forwarded after the MAC address limit is reached.

Options drop—Drop packets with new source MAC addresses, and do not learn the new source MAC addresses.

drop-and-log—(EX Series switches only) Drop packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

log—(EX Series switches only) Hold packets with new source MAC addresses, and generate an alarm, an SNMP trap, or a system log entry.

none—(EX Series switches only) Forward packets with new source MAC addresses, and learn the new source MAC address.

shutdown—(EX Series switches only) Disable the specified interface, and generate an alarm, an SNMP trap, or a system log entry.

Required Privilege routing—To view this statement in the configuration.

Level routing-control—To add this statement to the configuration.
persistent-learning

**Syntax**

```
persistent-learning;
```

**Hierarchy Level**

```
[edit switch-options on page 2027 interface interface-name]
```

**Release Information**

Hierarchy level [edit switch-options interface interface-name] introduced in Junos OS Release 13.2X50-D10

**Description**

Specify that learned MAC addresses persist on the specified interfaces across restarts of the switch and link-down conditions. This feature is also known as sticky MAC.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system–control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Basic Port Security Features
- Configuring Persistent MAC Learning (CLI Procedure) on page 4032
recovery-timeout

Syntax

```plaintext
recovery-timeout seconds;
```

Hierarchy Level

```plaintext
[edit interfaces interface-name family ethernet-switching]
```

Release Information

Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Statement introduced in Junos OS Release 13.2 for the QFX Series.

Description

Disable rather than block an interface when enforcing MAC limiting, MAC move limiting, or rate-limiting configuration options for shutting down the interface, and allow the interface to recover automatically from the error condition after the specified period of time:

- If you have enabled MAC limiting with the `shutdown` option and you enable `recovery-timeout`, the switch disables (rather than shuts down) the interface when the MAC address limit is reached.
- If you have enabled MAC move limiting (Not supported on EX9200) with the `shutdown` option and you enable `recovery-timeout`, the switch disables (rather than shuts down) the interface when the maximum number of moves to a new interface is reached.
- If you have enabled storm control with the `action-shutdown` option and you enable `recovery-timeout` the switch disables (rather than shuts down) the interface when applicable traffic exceeds the specified levels. Depending upon the configuration, applicable traffic could include broadcast, unknown unicast, and multicast traffic.

NOTE: The `recovery-timeout` configuration does not apply to pre-existing error conditions. It impacts only error conditions that are detected after `recovery-timeout` has been enabled and committed. To clear a pre-existing error condition and restore the interface to service, use the operational mode command `clear ethernet-switching recovery-timeout`.

Default

Not enabled.

Options

`seconds`— Number of seconds that the interface remains in a disabled state due to a port error prior to automatic recovery.

Range: 10 through 3600

Required Privilege Level

system—To view this statement in the configuration.
system–control—To add this statement to the configuration.

Related Documentation

- `action-shutdown` on page 2029
- Configuring MAC Limiting (CLI Procedure) on page 2132
- Configuring MAC Move Limiting (CLI Procedure)
• Configuring or Disabling Storm Control (CLI Procedure) on page 2023
remote-id

Syntax

remote-id {  
  host-name host-name;  
  prefix hostname | mac | none; host  
  use-interface-description;  
  use-string string;  
}

Hierarchy Level

- For platforms with ELS:
  [edit vlans vlan-name forwarding-options dhcp-security option-82 ]
- For platforms without ELS:
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name) dhcp-option82],
  [edit forwarding-options helpers bootp dhcp-option82],
  [edit forwarding-options helpers bootp interface interface-name dhcp-option82]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Insert the remote-id suboption of DHCP option 82 (also known as the DHCP relay agent information option) in DHCP request packet headers before forwarding or relaying requests to a DHCP server. This suboption provides a trusted identifier for the host system that has forwarded or relayed requests to the server.

The remaining statements are explained separately, and their availability depends on the hierarchy level at which remote-id is specified, as follows:

- The statement prefix is not supported at the [edit vlans vlan-name forwarding-options dhcp-security option-82] hierarchy level.
- The statement host-name is supported only at the [edit vlans vlan-name forwarding-options dhcp-security option-82] hierarchy level.

Default

If remote-id is not explicitly set, no remote ID value is inserted in the DHCP request packet header.

If remote-id is explicitly set, but is not qualified by a keyword:

- At the [edit vlans vlan-name forwarding-options dhcp-security] hierarchy level, the default keyword value is interface-name.
- At all other hierarchy levels, the remote-id default keyword value of is the MAC address of the switch.

Required Privilege

Level system—To view this statement in the configuration.

system-control—To add this statement to the configuration.
Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)

**routing-instance-name (circuit-id)**

**Syntax**

```
route-instance-name;  
```

**Hierarchy Level**

```
[edit vlans vlan-name forwarding-options dhcp-security option-82 circuit-id prefix]  
```

**Release Information**

Statement introduced in Junos OS Release 13.2 for EX Series switches.

**Description**

Specify that the routing instance name used by the VLAN is included with the circuit ID suboption in the DHCP option 82 information that is inserted by the switch into the packet header of a DHCP request before it forwards or relays the request to a DHCP server.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
- Understanding DHCP Option 82 for Port Security on EX Series Switches on page 4000
### static-ip

**Syntax**

```plaintext
static-ip ip-address {
  vlan vlan-name;
  mac mac-address;
}
```

**Hierarchy Level**

- For platforms with ELS:
  ```plaintext
  [edit vlans vlan-name forwarding-options dhcp-security group group-name interface interface-name]
  ```
- For platforms without ELS:
  ```plaintext
  [edit ethernet-switching-options secure-access-port interface (all | interface-name)]
  ```

**Release Information**


**Description**

Configure a static IP address to MAC address (IP-MAC) binding to be added to the DHCP snooping database.

---

**NOTE:** The VLAN is specified at the higher hierarchy level when `static-ip` is configured at `[edit vlans vlan-name forwarding-options dhcp-security group group-name interface interface-name]`.

**Options**

- **ip-address**—Static IP address assigned to a device connected on the specified interface.
- **mac mac-address**—Static MAC address assigned to a device connected on the specified interface.

The remaining statements are explained separately.

**Required Privilege Level**

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure)
- Configuring Static IP Addresses for DHCP Bindings on Access Ports (CLI Procedure) on page 4034
trusted

Syntax trusted;

Hierarchy Level [edit vlans vlan-name forwarding-options dhcp-security group group-name overrides]

Release Information Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Allow DHCP responses from the specified interface. The interface is not subject to DHCP snooping, even if the VLAN is enabled for DHCP snooping.

Required Privilege Level interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

Related Documentation • Enabling a Trusted DHCP Server (CLI Procedure) on page 4036
• Understanding Trusted DHCP Servers for Port Security on page 4016
• Understanding DHCP Snooping for Port Security

untrusted

Syntax untrusted;

Hierarchy Level [edit vlans vlan-name forwarding-options dhcp-security group group-name overrides]

Release Information Statement introduced in Junos OS Release 13.2 for EX Series switches.

Description Override the default behavior of a trunk interface from trusted to untrusted.

Required Privilege Level interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

Related Documentation • Enabling a Trusted DHCP Server (CLI Procedure) on page 4036
• Understanding Trusted DHCP Servers for Port Security on page 4016
• Understanding DHCP Snooping for Port Security
use-interface-description

Syntax

```
use-interface-description;
```

Hierarchy Level

- For platforms with ELS:
  ```
  [edit vlans vlan-name forwarding-options dhcp-security option-82 circuit-id]
  ```

- For platforms without ELS:
  ```
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name) dhcp-option82 circuit-id],
  [edit forwarding-options helpers bootp dhcp-option82 circuit-id],
  [edit forwarding-options helpers bootp interface interface-name dhcp-option82 circuit-id],
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name) dhcp-option82 remote-id],
  [edit forwarding-options helpers bootp dhcp-option82 remote-id],
  [edit forwarding-options helpers bootp interface interface-name dhcp-option82 remote-id]
  ```

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description

Use the interface description rather than the interface name (which is the default value) in the circuit ID or remote ID value in the DHCP option 82 information.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
use-string

Syntax  
use-string string;

Hierarchy Level
- For platforms with ELS:
  [edit vlans vlan-name forwarding-options dhcp-security option-82 remote-id]
- For platforms without ELS:
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name) dhcp-option82 remote-id],
  [edit forwarding-options helpers bootp dhcp-option82 remote-id],
  [edit forwarding-options helpers bootp interface interface-name dhcp-option82 remote-id]

Release Information
Statement introduced in Junos OS Release 9.3 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Hierarchy level [edit vlans vlan-name forwarding-options dhcp-security] introduced in
Junos OS Release 13.2X50-D10. (See “Getting Started with Enhanced Layer 2 Software”
on page 3 for information about ELS.)

Description
Use a string rather than the MAC address of the host system (the default) in the remote
ID value in the DHCP option 82 information.

Options
string—Character string used as the remote ID value.

Range: 1–255 characters

Required Privilege
Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients
  and a DHCP Server
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients
  and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and
  DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP
  Server (CLI Procedure)
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and
  DHCP Server (CLI Procedure) on page 4039
**use-vlan-id**

**Syntax**

```
use-vlan-id;
```

**Hierarchy Level**

- For platforms with ELS:
  
  `[edit vlans vlan-name forwarding-options dhcp-security option-82 circuit-id]`

- For platforms without ELS:

  `[edit forwarding-options helpers bootp dhcp-option82-circuit-id],`
  
  `[edit forwarding-options helpers bootp interface interface-name dhcp-option82-circuit-id]`

**Release Information**

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Statement introduced in Junos OS Release 11.3 for the QFX Series.


**Description**

Use the VLAN ID rather than the VLAN name (the default) in the circuit ID value in the DHCP option 82 information.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
vendor-id

Syntax

vendor-id <string>;

Hierarchy Level

- For platforms with ELS:
  
  [edit vlans vlan-name forwarding-options dhcp-security option-82]
  
- For platforms without ELS:
  
  [edit ethernet-switching-options secure-access-port vlan (all | vlan-name) dhcp-option82],
  [edit forwarding-options helpers bootp dhcp-option82],
  [edit forwarding-options helpers bootp interface interface-name dhcp-option82]

Release Information

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Statement introduced in Junos OS Release 11.3 for the QFX Series.


Description

Insert a vendor ID in the DHCP option 82 information in a DHCP request packet header before forwarding or relaying the request to a DHCP server.

Default

If vendor-id is not explicitly configured for DHCP option 82, then no vendor ID is set.

Options

string—(Optional) A single string that designates the vendor ID.

Range: 1–255 characters

Default: If you specify vendor-id with no string value, then the default vendor ID Juniper is configured.

Required Privilege Level

- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation

- Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server
- Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure)
- Setting Up DHCP Option 82 on the Switch with No Relay Agent Between Clients and DHCP Server (CLI Procedure) on page 4039
- Setting Up DHCP Option 82 with the Switch as a Relay Agent Between Clients and DHCP Server (CLI Procedure)
write-interval

Syntax

write-interval seconds;

Hierarchy Level

- For platforms with ELS:
  [edit system processes] dhcp-service dhcp-snooping-file
- For platforms without ELS:
  [edit ethernet-switching-options secure-access-port dhcp-snooping-file]

Release Information


Description

Specify how frequently the switch writes the database entries from memory into the specified DHCP snooping database file.

- If you are configuring write-interval at the [edit ethernet-switching-options secure-access-port dhcp-snooping-file] hierarchy level, see Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure).
- If you are configuring write-interval at the [edit system processes dhcp-service dhcp-snooping-file] hierarchy level, see “Making IP-MAC Bindings in the DHCP Snooping Database Persistent (CLI Procedure)” on page 4038.

Default

None

Options

seconds—Value in seconds.

Range: 60–86,400 seconds

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

- Understanding DHCP Snooping for Port Security
CHAPTER 76

Administration

- Operational Commands on page 4071

Operational Commands
clear arp

**Syntax**
```
clear arp
<hostname hostname>
<interface interface-name>
<logical-system logical-system-name>
<vpn vpn>
```

**Release Information**
Command introduced before Junos OS Release 7.4.

**Description**
Remove entries from the Address Resolution Protocol (ARP) table for the current CLI view. To clear entries for a specific logical system, you must first enter the `set cli logical-system logical-system-name` command, and then issue the `clear arp` command.

**Options**
- `none`—Clear all entries from the ARP table.
- `hostname hostname`—(Optional) Clear only the specified host entry from the ARP table.
- `interface interface-name`—(Optional) Clear entries only for the specified interface from the ARP table.
- `logical-system logical-system-name`—(Optional) Clear entries for only the specified logical system from the ARP table (only available in main router context).
- `vpn vpn`—(Optional) Clear entries from the ARP table for the specified virtual private network (VPN).

**Required Privilege Level**
clear

**Related Documentation**
- `set cli logical-system`
- `show arp`
- `show dhcp-security arp inspection statistics on page 4076`

**List of Sample Output**
clear arp on page 4072
clear arp logical-system ls1 on page 4073

**Output Fields**
When you enter this command, you are provided feedback on the status of your request.

**Sample Output**
clear arp
```
user@host> clear arp
192.168.71.254 deleted
192.168.65.46 deleted
192.168.64.10 deleted
10.0.12.14 deleted
10.0.17.14 deleted
```
clear arp logical-system ls1

user@host> clear arp logical-system ls1
192.168.71.254  deleted
192.168.65.46   deleted
192.168.64.10   deleted
10.0.12.14       deleted
10.0.17.14       deleted
clear dhcp-security binding

Syntax

clear dhcp-security binding
  <interface interface-name>
  <ip-address ip-address>
  <statistics>
  <vlan vlan-name>

Release Information
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Clear the DHCP snooping database information.

Options
interface interface-name—(Optional) Clear DHCP snooping database information for the specified interface.

ip-address ip-address—(Optional) Clear DHCP snooping database information for the specified IP address.

statistics—(Optional) Clear all DHCP snooping database statistics.

vlan vlan-name—(Optional) Clear DHCP snooping database information for the specified VLAN.

Required Privilege Level
clear

Related Documentation
- show dhcp-security binding on page 4078
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017

List of Sample Output
clear dhcp-security binding on page 4074

Output Fields
This command produces no output.

Sample Output
clear dhcp-security binding

user@switch> clear dhcp-security binding
clear ethernet-switching recovery-timeout

**Syntax**
clear ethernet-switching recovery-timeout

**Release Information**
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**
Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch, and restore the interfaces to service.

**Options**
- **none**—Clear all MAC limiting, MAC move limiting, and storm control errors from all the Ethernet switching interfaces on the switch and restore these interfaces to service.

**Required Privilege Level**
clear

**Related Documentation**
- Configuring Autorecovery From the Disabled State on Secure or Storm Control Interfaces (CLI Procedure) on page 2023

**Output Fields**
This command produces no output.
show dhcp-security arp inspection statistics

**Syntax**
show dhcp-security arp inspection statistics

**Release Information**
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**
Display ARP inspection statistics.

**Required Privilege Level**
view

**Related Documentation**
- show dhcp-security binding on page 4078
- clear dhcp-security binding
- clear interfaces statistics
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017

**List of Sample Output**
show dhcp-security arp inspection statistics on page 4076

**Output Fields**
Table 497 on page 4076 lists the output fields for the show dhcp-security arp inspection statistics command. Output fields are listed in the approximate order in which they appear.

The IP source guard database table shows the untrusted access interfaces in VLANs that have been enabled for IP source guard. The entries include the VLAN 802.1Q tag IDs if there are any, and the IP addresses and MAC addresses that are bound to one another.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which ARP inspection has been applied.</td>
<td>All levels</td>
</tr>
<tr>
<td>Packets received</td>
<td>Total number of packets that underwent ARP inspection.</td>
<td>All levels</td>
</tr>
<tr>
<td>ARP inspection pass</td>
<td>Total number of packets that passed ARP inspection.</td>
<td>All levels</td>
</tr>
<tr>
<td>ARP inspection fail</td>
<td>Total number of packets that failed ARP inspection.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

**Sample Output**

show dhcp-security arp inspection statistics

user@switch> show dhcp-security arp inspection statistics

<table>
<thead>
<tr>
<th>Interface</th>
<th>Packets received</th>
<th>ARP inspection pass</th>
<th>ARP inspection fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/30.0</td>
<td>7</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>Interface</td>
<td>Connected</td>
<td>Connected Port</td>
<td>Status</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>3</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>72</td>
<td>4</td>
<td>68</td>
</tr>
</tbody>
</table>
**show dhcp-security binding**

**Syntax**

```
show dhcp-security binding
<interface interface-name>
<ip-address ip-address>
<vlan vlan-name>
```

**Release Information**

Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Display the DHCP snooping database information.

**Options**

- `interface interface-name`—(Optional) Display the DHCP snooping database information for an interface.
- `ip-address ip-address`—(Optional) Display the DHCP snooping database information for an IP address.
- `vlan vlan-name`—(Optional) Display the DHCP snooping database information for a VLAN.

**Required Privilege Level**

view

**Related Documentation**

- show dhcp-security binding ip-source-guard on page 4081
- clear dhcp-security binding
- Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017

**List of Sample Output**

- show dhcp-security binding on page 4079
- show dhcp-security binding interface on page 4079
- show dhcp-security binding ip-address on page 4079
- show dhcp-security binding vlan on page 4079

**Output Fields**

Table 498 on page 4078 lists the output fields for the `show dhcp-security binding` command. Output fields are listed in the approximate order in which they appear.

**Table 498: show dhcp-security binding Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the network device; bound to the MAC address.</td>
<td>All levels</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address of the network device; bound to the IP address.</td>
<td>All levels</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN name of the network device whose MAC address is shown.</td>
<td>All levels</td>
</tr>
<tr>
<td>Expires</td>
<td>The time, in seconds, remaining before the lease of the IP address to the MAC address expires.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 498: show dhcp-security binding Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Specifies whether the IP address is:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• BOUND: Leased to the MAC address for a limited period of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• STATIC: Attached to a fixed MAC address.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Interface address (port).</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show dhcp-security binding

```
user@switch> show dhcp-security binding
IP address        MAC address         Vlan     Expires State   Interface
30.1.1.10         00:10:00:20:00:01   vlan20   0       STATIC   ge-0/0/4.0
30.1.1.18         00:10:94:00:00:34   vlan20   86287   BOUND   ge-0/0/6.0
30.1.1.15         00:10:94:00:00:55   vlan20   86265   BOUND   ge-0/0/4.0
30.1.1.16         00:10:94:00:00:56   vlan20   86265   BOUND   ge-0/0/4.0
30.1.1.19         00:10:94:00:00:5b   vlan20   86287   BOUND   ge-0/0/6.0
30.1.1.20         00:10:94:00:00:5c   vlan20   86287   BOUND   ge-0/0/6.0
30.1.1.21         00:10:94:00:00:5d   vlan20   86287   BOUND   ge-0/0/6.0
30.1.1.17         00:10:94:00:00:68   vlan20   86265   BOUND   ge-0/0/4.0
```

show dhcp-security binding interface

```
user@switch> show dhcp-security binding interface ge-0/0/6
IP address        MAC address         Vlan     Expires State   Interface
30.1.1.18         00:10:94:00:00:34   vlan20   86282   BOUND   ge-0/0/6.0
30.1.1.19         00:10:94:00:00:5b   vlan20   86282   BOUND   ge-0/0/6.0
30.1.1.20         00:10:94:00:00:5c   vlan20   86282   BOUND   ge-0/0/6.0
30.1.1.21         00:10:94:00:00:5d   vlan20   86282   BOUND   ge-0/0/6.0
```

show dhcp-security binding ip-address

```
user@switch> show dhcp-security binding ip-address
IP address        MAC address         Vlan     Expires State   Interface
30.1.1.18         00:10:94:00:00:34   vlan20   86282   BOUND   ge-0/0/6.0
```

show dhcp-security binding vlan

```
user@switch> show dhcp-security binding vlan vlan20
```
<table>
<thead>
<tr>
<th>IIP address</th>
<th>MAC address</th>
<th>Vlan</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.1.1.18</td>
<td>00:10:94:00:00:34</td>
<td>vlan20</td>
<td>86282</td>
<td>BOUND</td>
<td>ge-0/0/6.0</td>
</tr>
</tbody>
</table>
show dhcp-security binding ip-source-guard

Syntax
show dhcp-security binding ip-source-guard

Release Information
Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description
Display IP source guard database table.

Required Privilege
Level
view

Related Documentation
• show dhcp-security binding on page 4078
• clear dhcp-security binding on page 4074
• Example: Configuring IP Source Guard and Dynamic ARP Inspection to Protect the Switch from IP Spoofing and ARP Spoofing on page 4017

List of Sample Output

show dhcp-security binding ip-source-guard on page 4082

Output Fields
Table 499 on page 4081 lists the output fields for the show dhcp-security binding ip-source-guard command. Output fields are listed in the approximate order in which they appear.

The IP source guard database table shows the untrusted access interfaces in VLANs that have been enabled for IP source guard. The entries include the IP addresses and MAC addresses that are bound to one another.

Table 499: show dhcp-security binding ip-source-guard Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the network device; bound to the MAC address.</td>
<td>All levels</td>
</tr>
<tr>
<td>MAC address</td>
<td>MAC address of the network device; bound to the IP address.</td>
<td>All levels</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN name of the network device whose MAC address is shown.</td>
<td>All levels</td>
</tr>
<tr>
<td>Expires</td>
<td>The time, in seconds, remaining before the lease of the IP address to the MAC address expires.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>Specifies whether the IP address is:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• BOUND: Temporarily leased to the MAC address for a limited period of time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• STATIC: Attached to a fixed MAC address.</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>Interface address (port).</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Sample Output

show dhcp-security binding ip-source-guard

```
user@switch> show dhcp-security binding ip-source-guard

<table>
<thead>
<tr>
<th>IP address</th>
<th>MAC address</th>
<th>Vlan</th>
<th>Expires</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.1.1.10</td>
<td>00:10:00:20:00:01</td>
<td>vlan20</td>
<td>0</td>
<td>STATIC</td>
<td>ge-0/0/4.0</td>
</tr>
<tr>
<td>30.1.1.18</td>
<td>00:10:94:00:00:34</td>
<td>vlan20</td>
<td>86276</td>
<td>BOUND</td>
<td>ge-0/0/6.0</td>
</tr>
<tr>
<td>30.1.1.15</td>
<td>00:10:94:00:00:55</td>
<td>vlan20</td>
<td>86254</td>
<td>BOUND</td>
<td>ge-0/0/4.0</td>
</tr>
<tr>
<td>30.1.1.16</td>
<td>00:10:94:00:00:56</td>
<td>vlan20</td>
<td>86254</td>
<td>BOUND</td>
<td>ge-0/0/4.0</td>
</tr>
<tr>
<td>30.1.1.19</td>
<td>00:10:94:00:00:5b</td>
<td>vlan20</td>
<td>86276</td>
<td>BOUND</td>
<td>ge-0/0/6.0</td>
</tr>
<tr>
<td>30.1.1.20</td>
<td>00:10:94:00:00:5c</td>
<td>vlan20</td>
<td>86276</td>
<td>BOUND</td>
<td>ge-0/0/6.0</td>
</tr>
<tr>
<td>30.1.1.21</td>
<td>00:10:94:00:00:5d</td>
<td>vlan20</td>
<td>86276</td>
<td>BOUND</td>
<td>ge-0/0/6.0</td>
</tr>
<tr>
<td>30.1.1.17</td>
<td>00:10:94:00:00:68</td>
<td>vlan20</td>
<td>86254</td>
<td>BOUND</td>
<td>ge-0/0/4.0</td>
</tr>
</tbody>
</table>
```
PART 25

Routing Policy and Packet Filtering

• Overview on page 4085
• Configuration on page 4161
• Administration on page 4259
• Troubleshooting Procedures on page 4291
Juniper Networks Junos operating system (Junos OS) is a network operating system that has been hardened through the separation of control forwarding and services planes, with each function running in protected memory. The control-plane CPU is protected by rate limiting, routing policy, and firewall filters to ensure switch uptime even under severe attack. Access port security features such as dynamic Address Resolution Protocol (ARP) inspection, DHCP snooping, and MAC limiting are controlled through a single Junos OS CLI command.

Juniper Networks EX Series Ethernet Switches provide the following hardware and software security features:

**Console Port**—Allows use of the console port to connect to the Routing Engine through an RJ-45 cable. You then use the command-line interface (CLI) to configure the switch.

**Out-of-Band Management**—A dedicated management Ethernet port on the rear panel allows out-of-band management.

**Software Images**—All Junos OS images are signed by Juniper Networks certificate authority (CA) with public key infrastructure (PKI).

**User Authentication, Authorization, and Accounting (AAA)**—Features include:

- User and group accounts with password encryption and authentication.
- Access privilege levels configurable for login classes and user templates.
- RADIUS authentication, TACACS+ authentication, or both, for authenticating users who attempt to access the switch.
- Auditing of configuration changes through system logging or RADIUS/TACACS+.
802.1X Authentication—Provides network access control. Supplicants (hosts) are authenticated when they initially connect to a LAN. Authenticating supplicants before they receive an IP address from a DHCP server prevents unauthorized supplicants from gaining access to the LAN. EX Series switches support Extensible Authentication Protocol (EAP) methods, including EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

Port Security—Access port security features include:

- DHCP snooping—Filters and blocks ingress DHCP server messages on untrusted ports; builds and maintains an IP-address/MAC-address binding database (called the DHCP snooping database).
- Dynamic ARP inspection (DAI)—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons.
- MAC limiting—Protects against flooding of the Ethernet switching table.
- MAC move limiting—Detects MAC movement and MAC spoofing on access ports.
- Trusted DHCP server—With a DHCP server on a trusted port, protects against rogue DHCP servers sending leases.
- IP source guard—Mitigates the effects of IP address spoofing attacks on the Ethernet LAN. The source IP address in the packet sent from an untrusted access interface is validated against the source MAC address in the DHCP snooping database. The packet is allowed for further processing if the source IP address to source MAC address binding is valid; if the binding is not valid, the packet is discarded.
- DHCP option 82—Also known as the DHCP relay agent information option. Helps protect the EX Series switch against attacks such as spoofing (forging) of IP addresses and MAC addresses and DHCP IP address starvation. Option 82 provides information about the network location of a DHCP client, and the DHCP server uses this information to implement IP addresses or other parameters for the client.
- Unrestricted proxy ARP—The switch responds to all ARP messages with its own MAC address. Hosts that are connected to the switch's interfaces cannot communicate directly with other hosts. Instead, all communications between hosts go through the switch.
- Restricted proxy ARP—The switch does not respond to an ARP request if the physical networks of the source and target of the ARP request are the same. It does not matter whether the destination host has the same IP address as the incoming interface or a different (remote) IP address. An ARP request for a broadcast address elicits no reply.

Device Security—Storm control permits the switch to monitor unknown unicast and broadcast traffic and drop packets, or shut down, or temporarily disable the interface when a specified traffic level is exceeded, thus preventing packets from proliferating and degrading the LAN. You can enable storm control on access interfaces or trunk interfaces.

Firewall Filters—Allow auditing of various types of security violations, including attempts to access the switch from unauthorized locations. Firewall filters can detect such attempts and create audit log entries when they occur. The filters can also restrict access by limiting
traffic to source and destination MAC addresses, specific protocols, or, in combination with policers, to specified data rates to prevent denial of service (DoS) attacks.

**Policers**—Provide rate-limiting capability to control the amount of traffic that enters an interface, which acts to counter DoS attacks.

**Encryption Standards**—Supported standards include:

- 128-, 192-, and 256-bit Advanced Encryption Standard (AES)
- 56-bit Data Encryption Standard (DES) and 168-bit 3DES

**Related Documentation**

- 802.1X for EX Series Switches Overview on page 1655
- Firewall Filters for EX Series Switches Overview on page 4088
- Port Security Overview on page 3995
- Understanding Proxy ARP on EX Series Switches on page 2070
- *Understanding Storm Control on EX Series Switches*
- Understanding the Use of Policers in Firewall Filters on page 4155
- *Understanding Centralized Network Access Control and EX Series Switches*

**Firewall Filters Overview**

- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding Planning of Firewall Filters on page 4091
- Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches on page 4094
- Understanding How Firewall Filters Control Packet Flows on page 4095
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- Support for Match Conditions and Actions for Loopback Firewall Filters on Switches on page 4107
- Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches on page 4111
- Understanding How Firewall Filters Are Evaluated on page 4149
- Understanding Firewall Filter Match Conditions on page 4151
- Understanding How Firewall Filters Test a Packet’s Protocol on page 4155
- Understanding the Use of Policers in Firewall Filters on page 4155
- Understanding Filter-Based Forwarding for EX Series Switches on page 4158
- Understanding Tricolor Marking Architecture on page 4159
Firewall Filters for EX Series Switches Overview

Firewall filters provide rules that define whether to permit, deny, or forward packets that are transiting an interface on a Juniper Networks EX Series Ethernet Switch from a source address to a destination address. You configure firewall filters to determine whether to permit, deny, or forward traffic before it enters or exits a port, VLAN, or Layer 3 (routed) interface to which the firewall filter is applied. To apply a firewall filter, you must first configure the filter and then apply it to an port, VLAN, or Layer 3 interface.

You can apply firewall filters to network interfaces, aggregated Ethernet interfaces (also known as link aggregation groups (LAGs)), loopback interfaces, management interfaces, virtual management Ethernet interfaces (VMEs), and routed VLAN interfaces (RVIs). For information on EX Series switches that support a firewall filter on these interfaces, see “EX Series Switch Software Features Overview” on page 27.

An ingress firewall filter is a filter that is applied to packets that are entering a network. An egress firewall filter is a filter that is applied to packets that are exiting a network. You can configure firewall filters to subject packets to filtering, class-of-service (CoS) marking (grouping similar types of traffic together, and treating each type of traffic as a class with its own level of service priority), and traffic policing (controlling the maximum rate of traffic sent or received on an interface).

This topic describes:

- Firewall Filter Types on page 4088
- Firewall Filter Components on page 4089
- Firewall Filter Processing on page 4090

Firewall Filter Types

The following firewall filter types are supported for EX Series switches:

- Port (Layer 2) firewall filter—Port firewall filters apply to Layer 2 switch ports. You can apply port firewall filters in both ingress and egress directions on a physical port.

- VLAN firewall filter—VLAN firewall filters provide access control for packets that enter a VLAN, are bridged within a VLAN, or leave a VLAN. You can apply VLAN firewall filters in both ingress and egress directions on a VLAN. VLAN firewall filters are applied to all packets that are forwarded to or forwarded from the VLAN.

- Router (Layer 3) firewall filter—You can apply a router firewall filter in both ingress and egress directions on Layer 3 (routed) interfaces and routed VLAN interfaces (RVIs). You can apply a router firewall filter in the ingress direction on the loopback interface (lo0) also. Firewall filters configured on loopback interfaces are applied only to packets that are sent to the Routing Engine CPU for further processing.

You can apply port, VLAN, or router firewall filters to both IPv4 and IPv6 traffic on these switches:

- EX3200 switch
- EX4200 switch
• EX4300 switch
• EX8200 switch

You can apply port, VLAN, or router firewall filters to only IPv4 traffic on these switches:
• EX2200 switch
• EX3300 switch
• EX4500 switch
• EX6200 switch

For information on firewall filters supported on different switches, see “Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 4111.

Firewall Filter Components

In a firewall filter, you first define the family address type (ethernet-switching, inet, or inet6), and then you define one or more terms that specify the filtering criteria (specified as terms with match conditions) and the action (specified as actions or action modifiers) to take if a match occurs.

The maximum number of terms allowed per firewall filter for EX Series switches is:
• 512 for EX2200 switches
• 1436 for EX3300 switches
• 7,042 for EX3200 and EX4200 switches—as allocated by the dynamic allocation of ternary content addressable memory (TCAM) for firewall filters.

On EX4300 switches, the following maximum number of terms are supported for ingress and egress traffic, for firewall filers configured on a port, VLAN and Layer 3 interface:
• For ingress traffic:
  • 3500 terms for firewall filters configured on a port
  • 3500 terms for firewall filters configured on a VLAN
  • 7000 terms for firewall filters configured on Layer 3 interfaces for IPv4 traffic
  • 3500 terms for firewall filters configured on Layer 3 interfaces for IPv6 traffic
• For egress traffic:
• 512 terms for firewall filters configured on a port
• 256 terms for firewall filters configured on a VLAN
• 512 terms for firewall filters configured on Layer 3 interfaces for IPv4 traffic
• 512 terms for firewall filters configured on Layer 3 interfaces for IPv6 traffic

NOTE: You can configure the maximum number of terms only when you configure one type of firewall filter (port, VLAN, or router (Layer 3) firewall filter) on the switch, and when storm control is not enabled on any interface in the switch.

• 1200 for EX4500 and EX4550 switches
• 1400 for EX6200 switches
• 32,768 for EX8200 switches

NOTE: The on-demand dynamic allocation of the shared space TCAM in EX8200 switches is achieved by assigning free space blocks to firewall filters. Firewall filters are categorized into two different pools. Port and VLAN filters are pooled together (the memory threshold for this pool is 22K) while router firewall filters are pooled separately (the threshold for this pool is 32K). The assignment happens based on the filter pool type. Free space blocks can be shared only among the firewall filters belonging to the same filter pool type. An error message is generated when you try to configure a firewall filter beyond the TCAM threshold.

Each term consists of the following components:

• Match conditions—Specify the values or fields that the packet must contain. You can define various match conditions, including the IP source address field, IP destination address field, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port field, IP protocol field, Internet Control Message Protocol (ICMP) packet type, TCP flags, and interfaces.

• Action—Specifies what to do if a packet matches the match conditions. Possible actions are to accept or discard the packet or to send the packet to a specific virtual routing interface. In addition, packets can be counted to collect statistical information. If no action is specified for a term, the default action is to accept the packet.

• Action modifier—Specifies one or more actions for the switch if a packet matches the match conditions. You can specify action modifiers such as count, mirror, rate limit, and classify packets.

Firewall Filter Processing
The order of the terms within a firewall filter configuration is important. Packets are tested against each term in the order in which the terms are listed in the firewall filter
configuration. For information on how firewall filters process packets, see “Understanding How Firewall Filters Are Evaluated” on page 4149.

Related Documentation

- Understanding Planning of Firewall Filters on page 4091
- Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches on page 4094
- Understanding How Firewall Filters Are Evaluated on page 4149
- Understanding Firewall Filter Match Conditions on page 4151
- Understanding the Use of Policers in Firewall Filters on page 4155
- Understanding Filter-Based Forwarding for EX Series Switches on page 4158
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183

Understanding Planning of Firewall Filters

Before you create a firewall filter and apply it to an interface, determine what you want the firewall filter to accomplish and how to use its match conditions and actions to achieve your goals. You must understand how packets are matched to match conditions, the default and configured actions of the firewall filter, and proper placement of the firewall filter.

You can configure and apply no more than one firewall filter per port, VLAN, or router interface, per direction. The following limits apply for the number of firewall filter terms allowed per filter on various switch models:

- On EX2200 switches, the number of terms per filter cannot exceed 512.
- On EX3300 switches, the number of terms per filter cannot exceed 1436.
- On EX3200 and EX4200 switches, the number of terms per filter cannot exceed 7042.
- On EX4300 switches, the following maximum number of terms are supported for ingress and egress traffic, for firewall filers configured on a port, VLAN and Layer 3 interface:
  - For ingress traffic:
    - 3500 terms for firewall filters configured on a port
    - 3500 terms for firewall filters configured on a VLAN
    - 7000 terms for firewall filters configured on Layer 3 interfaces for IPv4 traffic
    - 3500 terms for firewall filters configured on Layer 3 interfaces for IPv6 traffic
  - For egress traffic:
- 512 terms for firewall filters configured on a port
- 256 terms for firewall filters configured on a VLAN
- 512 terms for firewall filters configured on Layer 3 interfaces for IPv4 traffic
- 512 terms for firewall filters configured on Layer 3 interfaces for IPv6 traffic

**NOTE:** You can configure the maximum number of terms only when you configure one type of firewall filter (port, VLAN, or router (Layer 3) firewall filter) on the switch, and when storm control is not enabled on any interface in the switch.

- On EX4500 and EX4550 switches, the number of terms per filter cannot exceed 1200.
- On EX6200 switches, the number of terms per filter cannot exceed 1400.
- On EX8200 switches, the number of terms per filter cannot exceed 32,768.

In addition, try to be conservative in the number of terms (rules) that you include in each firewall filter because a large number of terms requires longer processing time during a commit and also can make firewall filter testing and troubleshooting more difficult. Similarly, applying firewall filters across many switch and router interfaces can make testing and troubleshooting the rules of those filters difficult.

Before you configure and apply firewall filters, answer the following questions for each of those firewall filters:

1. What is the purpose of the firewall filter?
   For example, you can use a firewall filter to limit traffic to source and destination MAC addresses, specific protocols, or certain data rates or to prevent denial of service (DoS) attacks.

2. What are the appropriate match conditions?
   a. Determine the packet header fields that the packet must contain for a match. Possible fields include:
      - Layer 2 header fields—Source and destination MAC addresses, dot1q tag, Ethernet type, and VLAN
      - Layer 3 header fields—Source and destination IP addresses, protocols, and IP options (IP precedence, IP fragmentation flags, TTL type)
      - TCP header fields—Source and destination ports and flags
      - ICMP header fields—Packet type and code
   b. Determine the port, VLAN, or router interface on which the packet was received.

3. What are the appropriate actions to take if a match occurs?
   Possible actions to take if a match occurs are accept, discard, and forward to a routing instance.
4. What additional action modifiers might be required?

Determine whether additional actions are required if a packet matches a match condition; for example, you can specify an action modifier to count, analyze, or police packets.

5. On what interface should the firewall filter be applied?

Start with the following basic guidelines:

- If all the packets entering a port need to be exposed to filtering, then use port firewall filters.
- If all the packets that are bridged need filtering, then use VLAN firewall filters.
- If all the packets that are routed need filtering, then use router firewall filters.

Before you choose the interface on which to apply a firewall filter, understand how that placement can impact traffic flow to other interfaces. In general, apply a firewall filter that filters on source and destination IP addresses, IP protocols, or protocol information—such as ICMP message types, and TCP and UDP port numbers—nearest to the source devices. However, typically apply a firewall filter that filters only on a source IP address nearest to the destination devices. When applied too close to the source device, a firewall filter that filters only on a source IP address could potentially prevent that source device from accessing other services that are available on the network.

**NOTE:** Egress firewall filters do not affect the flow of locally generated control packets from the Routing Engine.

6. In which direction should the firewall filter be applied?

You can apply firewall filters to ports on the switch to filter packets that are entering a port. You can apply firewall filters to VLANs, and Layer 3 (routed) interfaces to filter packets that are entering or exiting a VLAN or routed interface. Typically, you configure different sets of actions for traffic entering an interface than you configure for traffic exiting an interface.

**Related Documentation**

- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding the Use of Policers in Firewall Filters on page 4155
- Understanding How Firewall Filters Are Evaluated on page 4149
- Understanding Filter-Based Forwarding for EX Series Switches on page 4158
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183
Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches

Juniper Networks EX Series Ethernet Switches are multilayered switches that provide Layer 2 switching and Layer 3 routing. You apply firewall filters at multiple processing points in the packet forwarding path on EX Series switches. At each processing point, the action to be taken on a packet is determined based on the results of the lookup in the switch's forwarding table. A table lookup determines which exit port on the switch to use to forward the packet.

For both bridged unicast packets and routed unicast packets, firewall filters are evaluated and applied hierarchically. First, a packet is checked against the port firewall filter, if present. If the packet is permitted, it is then checked against the VLAN firewall filter, if present. If the packet is permitted, it is then checked against the router firewall filter, if present. The packet must be permitted by the router firewall filter before it is processed.

Figure 58 on page 4094 shows the various firewall filter processing points in the packet forwarding path in a multilayered switching platform.

Figure 58: Firewall Filter Processing Points in the Packet Forwarding Path

For a multicast packet that results in replications, an egress firewall filter is applied to each copy of the packet based on its corresponding egress VLAN.
For Layer 2 (bridged) unicast packets, the following firewall filter processing points apply:

- Ingress port firewall filter
- Ingress VLAN firewall filter
- Egress port firewall filter
- Egress VLAN firewall filter

For Layer 3 (routed and multilayer-switched) unicast packets, the following firewall filter processing points apply:

- Ingress port firewall filter
- Ingress VLAN firewall filter (Layer 2 CoS)
- Ingress router firewall filter (Layer 3 CoS)
- Egress router firewall filter
- Egress VLAN firewall filter

Related Documentation

- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding How Firewall Filters Control Packet Flows on page 4095
- Understanding Bridging and VLANs on EX Series Switches on page 2049
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161

Understanding How Firewall Filters Control Packet Flows

Juniper Networks EX Series Ethernet Switches support firewall filters that allow you to control flows of data packets and local packets. **Data packets** are chunks of data that transit the switch as they are forwarded from a source to a destination. **Local packets** are chunks of data that are destined for or sent by the switch. Local packets usually contain routing protocol data, data for IP services such as Telnet or SSH, and data for administrative protocols such as the Internet Control Message Protocol (ICMP).

You create firewall filters to protect your switch from excessive traffic transiting the switch to a network destination or destined for the Routing Engine on the switch. Firewall filters that control local packets can also protect your switch from external incidents such as denial-of-service (DoS) attacks.

Firewall filters affect packet flows entering in to or exiting from the switch’s interfaces:

- Ingress firewall filters affect the flow of data packets that are received by the switch's interfaces. The Packet Forwarding Engine handles this flow. When a switch receives a data packet on an interface, the switch determines where to forward the packet by looking in the forwarding table for the best route (Layer 2 switching, Layer 3 routing) to a destination. Data packets are forwarded to their destination through an outgoing interface. Locally destined packets are forwarded to the Routing Engine.
Egress firewall filters affect the flow of data packets that are transmitted from the switch’s interfaces but do not affect the flow of locally generated control packets from the Routing Engine. The Packet Forwarding Engine handles the flow of data packets that are transmitted from the switch, and egress firewall filters are applied here. The Packet Forwarding Engine also handles the flow of control packets from the Routing Engine.

Figure 59 on page 4096 illustrates the application of ingress and egress firewall filters to control the flow of packets through the switch.

Figure 59: Application of Firewall Filters to Control Packet Flow

1. Ingress firewall filter applied to control locally destined packets that are received on the switch’s interfaces and are destined for the Routing Engine.
2. Ingress firewall filter applied to control incoming packets on the switch’s interfaces.
3. Egress firewall filter applied to control packets that are transiting the switch’s interfaces.

Related Documentation
- Understanding Firewall Filter Processing Points for Bridged and Routed Packets on EX Series Switches on page 4094
- Understanding How Firewall Filters Are Evaluated on page 4149

Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches

When you define a firewall filter for an EX Series switch, you define filtering criteria (terms, with match conditions) for the packets and an action (and, optionally, an action modifier) for the switch to take if the packets match the filtering criteria. You can define a firewall filter to monitor IPv4, IPv6, or non-IP traffic.

This topic describes in detail the various match conditions, actions, and action modifiers that you can define in a firewall filter. For information about support for match conditions
on various EX Series switches, see “Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 4111.

This topic describes:

- Firewall Filter Elements on page 4097
- Match Conditions Supported on Switches on page 4097
- Actions for Firewall Filters on page 4104
- Action Modifiers for Firewall Filters on page 4105

**Firewall Filter Elements**

A firewall filter configuration contains a term, a match condition, an action, and, optionally, an action modifier. Table 500 on page 4097 describes each element in a firewall filter configuration.

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term</td>
<td>Defines the filtering criteria for the packets. Each term in the firewall filter consists of match conditions and an action. You can define a single term or multiple terms in the firewall filter. If you define multiple terms, each term must have a unique name.</td>
</tr>
<tr>
<td>Match condition</td>
<td>Consists of a string (called a <em>match statement</em>) that defines the match condition. Match conditions are the values or fields that a packet must contain. You can define a single match condition or multiple match conditions for a term. You can also opt not to define a match condition. If no match conditions are specified for a term, all packets are matched by default.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the action that the switch takes if a packet matches all the criteria specified in the match conditions.</td>
</tr>
<tr>
<td>Action modifier</td>
<td>Specifies one or more actions that the switch takes if a packet matches the match conditions for the specific term.</td>
</tr>
</tbody>
</table>

**Match Conditions Supported on Switches**

Based on the type of traffic that you want to monitor, you can configure a firewall filter to monitor IPv4, IPv6, or non-IP traffic. When you configure a firewall filter to monitor a particular type of traffic, ensure that you specify match conditions that are supported for that type of traffic. For information about match conditions supported for a specific type of traffic and switches on which they are supported, see “Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 4111.

Table 501 on page 4097 describes all the match conditions that are supported for firewall filters on EX Series Switches.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-address ip-address</td>
<td>IP destination address field, which is the address of the final destination node.</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ip-destination-address ip-address</td>
<td>IP destination address field, which is the address of the final destination node.</td>
</tr>
<tr>
<td>ip6-destination-address ip-address</td>
<td>IP destination address field, which is the address of the final destination node.</td>
</tr>
<tr>
<td>destination-mac-address mac-address</td>
<td>Destination media access control (MAC) address of the packet.</td>
</tr>
<tr>
<td></td>
<td>You can define a destination MAC address with a prefix, such as device-mac-address 00:01:02:03:04:05/24. If no prefix is specified, the default value 48 is used.</td>
</tr>
<tr>
<td>destination-port number</td>
<td>TCP or UDP destination port field. Typically, you specify this match condition in conjunction with the protocol or ip-protocol match condition to determine which protocol is used on the port. For number, you can specify one of the following text synonyms (the port numbers are also listed):</td>
</tr>
<tr>
<td></td>
<td>afs (1433), bgp (179), biff (512), bootpc (68), bootps (67), cmd (514), cvvsserver (2401), dhcp (67), domain (53), eklogin (2105), ekshell (2106), exec (512), finger (79), ftp (21), ftp-data (20), http (80), https (443), ident (113), imap (143), kerberos-sec (88), klogin (543), kpasswd (761), krb-prop (754), krbupdate (760), ksh (544), ldap (389), login (513), mobileip-agent (434), mobileip-mn (435), msdp (639), netbios-dgm (136), netbios-ns (137), netbios-ssn (139), nfld (2049), nntp (119), ntalk (518), ntp (123), pop3 (110), pptp (1723), printer (515), radaect (1813), radius (1812), rip (520), rkin (2108), smtp (25), smtp (161), smtptrap (162), snmp (19) 1080), ssh (22), sunrpc (111), syslog (514), tacacs-ds (65), talk (517), telnet (23), tftp (69), timed (525), who (513), xdmcp (177), zephyr-clt (2103), zephyr-hm (2104)</td>
</tr>
<tr>
<td>destination-prefix-list prefix-list</td>
<td>IP destination prefix list field. You can define a list of IP address prefixes under a prefix-list alias for frequent use. You define this match condition at the [edit policy-options] hierarchy level.</td>
</tr>
<tr>
<td>dot1q-tag number</td>
<td>The tag field in the Ethernet header. The tag values range from 1 through 4095. The dot1q-tag match condition and the vlan match condition are mutually exclusive.</td>
</tr>
<tr>
<td>user-vlan-id number</td>
<td>The tag field in the Ethernet header. The tag values range from 1 through 4095. The user-vlan-id match condition and the learn-vlan-id match condition are mutually exclusive.</td>
</tr>
</tbody>
</table>
Table 501: Firewall Filter Match Conditions Supported on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1q-user-priority number</td>
<td>User-priority field of the tagged Ethernet packet. User-priority values can range from 0 through 7. For number, you can specify one of the following text synonyms (the field values are also listed):</td>
</tr>
<tr>
<td></td>
<td>- background (1) — Background</td>
</tr>
<tr>
<td></td>
<td>- best-effort (0) — Best effort</td>
</tr>
<tr>
<td></td>
<td>- controlled-load (4) — Controlled load</td>
</tr>
<tr>
<td></td>
<td>- excellent-load (3) — Excellent load</td>
</tr>
<tr>
<td></td>
<td>- network-control (7) — Network control reserved traffic</td>
</tr>
<tr>
<td></td>
<td>- standard (2) — Standard or spare</td>
</tr>
<tr>
<td></td>
<td>- video (5) — Video</td>
</tr>
<tr>
<td></td>
<td>- voice (6) — Voice</td>
</tr>
<tr>
<td>user-vlan-1p-priority number</td>
<td>User-priority field of the tagged Ethernet packet. User-priority values can range from 0 through 7. For number, you can specify one of the following text synonyms (the field values are also listed):</td>
</tr>
<tr>
<td></td>
<td>- background (1) — Background</td>
</tr>
<tr>
<td></td>
<td>- best-effort (0) — Best effort</td>
</tr>
<tr>
<td></td>
<td>- controlled-load (4) — Controlled load</td>
</tr>
<tr>
<td></td>
<td>- excellent-load (3) — Excellent load</td>
</tr>
<tr>
<td></td>
<td>- network-control (7) — Network control reserved traffic</td>
</tr>
<tr>
<td></td>
<td>- standard (2) — Standard or spare</td>
</tr>
<tr>
<td></td>
<td>- video (5) — Video</td>
</tr>
<tr>
<td></td>
<td>- voice (6) — Voice</td>
</tr>
<tr>
<td>dscp number</td>
<td>Specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP. You can specify DSCP in hexadecimal, binary, or decimal form. For number, you can specify one of the following text synonyms (the field values are also listed):</td>
</tr>
<tr>
<td></td>
<td>- ef (46) — as defined in RFC 2598, An Expedited Forwarding PHB.</td>
</tr>
<tr>
<td></td>
<td>- af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38) These four classes, with three drop precedences in each class, are defined for 12 code points in RFC 2597, Assured Forwarding PHB Group.</td>
</tr>
</tbody>
</table>
Table 501: Firewall Filter Match Conditions Supported on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ether-type value</strong></td>
<td>Ethernet type field of a packet. The value specifies what protocol is being transported in the Ethernet frame. For value, you can specify one of the following text synonyms:</td>
</tr>
<tr>
<td></td>
<td>• aarp—EtherType value AARP (0x80F3)</td>
</tr>
<tr>
<td></td>
<td>• appletalk—EtherType value AppleTalk (0x809B)</td>
</tr>
<tr>
<td></td>
<td>• arp—EtherType value ARP (0x0806)</td>
</tr>
<tr>
<td></td>
<td>• ipv4—EtherType value IPv4 (0x0800)</td>
</tr>
<tr>
<td></td>
<td>• ipv6—EtherType value IPv6 (0x08DD)</td>
</tr>
<tr>
<td></td>
<td>• mpls multicast—EtherType value MPLS multicast (0x8848)</td>
</tr>
<tr>
<td></td>
<td>• mpls unicast—EtherType value MPLS unicast (0x8847)</td>
</tr>
<tr>
<td></td>
<td>• oam—EtherType value OAM (0x88AB)</td>
</tr>
<tr>
<td></td>
<td>• ppp—EtherType value PPP (0x880B)</td>
</tr>
<tr>
<td></td>
<td>• pppoe-discovery—EtherType value PPPoE Discovery Stage (0x8863)</td>
</tr>
<tr>
<td></td>
<td>• pppoe-session—EtherType value PPPoE Session Stage (0x8864)</td>
</tr>
<tr>
<td></td>
<td>• sna—EtherType value SNA (0x80D5)</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The following match conditions are not supported when ether-type is set to ipv6:</td>
</tr>
<tr>
<td></td>
<td>• dscp</td>
</tr>
<tr>
<td></td>
<td>• fragment-flags</td>
</tr>
<tr>
<td></td>
<td>• is-fragment</td>
</tr>
<tr>
<td></td>
<td>• precedence or ip-precedence</td>
</tr>
<tr>
<td></td>
<td>• protocol or ip-protocol</td>
</tr>
<tr>
<td><strong>fragment-flags</strong></td>
<td>IP fragmentation flags, specified in symbolic or hexadecimal formats. You can specify one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• dont-fragment (0x4000)</td>
</tr>
<tr>
<td></td>
<td>• more-fragments (0x2000)</td>
</tr>
<tr>
<td></td>
<td>• reserved (0x8000)</td>
</tr>
</tbody>
</table>
### Table 501: Firewall Filter Match Conditions Supported on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>icmp-code number</strong></td>
<td>ICMP code field. This value or option provides more specific information than icmp-type. Because the value’s meaning depends upon the associated icmp-type, you must specify icmp-type along with icmp-code. For number, you can specify one of the following text synonyms (the field values are also listed). The options are grouped by the ICMP type with which they are associated:</td>
</tr>
<tr>
<td>• parameter-problem—ip-header-bad (0), required-option-missing (1)</td>
<td></td>
</tr>
<tr>
<td>• redirect—redirect-for-host (1), redirect-for-network (0), redirect-for-tos-and-host (3), redirect-for-tos-and-net (2)</td>
<td></td>
</tr>
<tr>
<td>• time-exceeded—ttl-eq-zero-during-reassembly (1), ttl-eq-zero-during-transit (0)</td>
<td></td>
</tr>
<tr>
<td>• unreachable—communication-prohibited-by-filtering (13), destination-host-prohibited (10), destination-host-unknown (7), destination-network-prohibited (9), destination-network-unknown (6), fragmentation-needed (4), host-precedence-violation (14), host-unreachable (1), host-unreachable-for-TOS (12), network-unreachable (0), network-unreachable-for-TOS (11), port-unreachable (3), precedence-cutoff-in-effect (15), protocol-unreachable (2), source-host-isolated (8), source-route-failed (5)</td>
<td></td>
</tr>
<tr>
<td><strong>icmp-type number</strong></td>
<td>ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol or ip-protocol match condition to determine which protocol is being used on the port. For number, you can specify one of the following text synonyms (the field values are also listed):</td>
</tr>
<tr>
<td>echo-reply (0), echo-request (8), info-reply (16), info-request (15), mask-request (17), mask-reply (18), parameter-problem (12), redirect (5), router-advertisement (9), router-solicit (10), source-quench (4), time-exceeded (11), timestamp (13), timestamp-reply (14), unreachable (3)</td>
<td></td>
</tr>
<tr>
<td><strong>interface interface-name</strong></td>
<td>Interface on which the packet is received. You can specify the wildcard character (*) as part of an interface name.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The interface match condition is not supported for egress traffic on an EX8200 Virtual Chassis.</td>
<td></td>
</tr>
<tr>
<td><strong>ip-options</strong></td>
<td>Presence of the options field in the IP header.</td>
</tr>
</tbody>
</table>
### Table 501: Firewall Filter Match Conditions Supported on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-version version</strong></td>
<td>Version of the IP protocol for port and VLAN firewall filters. The value for version can be ipv4 or ipv6.</td>
</tr>
<tr>
<td><strong>match_condition(s)</strong></td>
<td>For <code>match_condition(s)</code>, you can specify one or more of the following match conditions:</td>
</tr>
<tr>
<td></td>
<td>• destination-address, ip-destination-address, or ip6-destination-address</td>
</tr>
<tr>
<td></td>
<td>• destination-port</td>
</tr>
<tr>
<td></td>
<td>• destination-prefix-list</td>
</tr>
<tr>
<td></td>
<td>• dscp</td>
</tr>
<tr>
<td></td>
<td>• fragment-flags</td>
</tr>
<tr>
<td></td>
<td>• icmp-code</td>
</tr>
<tr>
<td></td>
<td>• icmp-type</td>
</tr>
<tr>
<td></td>
<td>• is-fragment</td>
</tr>
<tr>
<td></td>
<td>• precedence or ip-precedence</td>
</tr>
<tr>
<td></td>
<td>• protocol or ip-protocol</td>
</tr>
<tr>
<td></td>
<td>• source-address or ip-source-address</td>
</tr>
<tr>
<td></td>
<td>• source-port</td>
</tr>
<tr>
<td></td>
<td>• source-prefix-list</td>
</tr>
<tr>
<td></td>
<td>• tcp-established</td>
</tr>
<tr>
<td></td>
<td>• tcp-flags</td>
</tr>
<tr>
<td></td>
<td>• tcp-initial</td>
</tr>
<tr>
<td><strong>is-fragment</strong></td>
<td>If the packet is a trailing fragment, this match condition does not match the first fragment of a fragmented packet. Use two terms to match both first and trailing fragments.</td>
</tr>
<tr>
<td><strong>l2-encap-type</strong></td>
<td>Match on logical link control (LLC) layer packets for non-Subnet Access Protocol (SNAP) Ethernet Encapsulation type.</td>
</tr>
<tr>
<td><strong>l2-encap-type llc-non-snap</strong></td>
<td>Match on logical link control (LLC) layer packets for non-Subnet Access Protocol (SNAP) Ethernet Encapsulation type.</td>
</tr>
<tr>
<td><strong>next-header bytes</strong></td>
<td>8-bit protocol field that identifies the type of header immediately following the IPv6 header. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): ah (51), dstops (60), egp (8), esp (50), fragment (44), gre (47), hop-by-hop (0), icmp (1), icmp6 (1), igmp (2), ipip (4), ipv6 (41), no-next-header (59), ospf (89), pim (103), routing (43), rsdp (46), sctp (132), tcp (6), udp (17), vrrp (112)</td>
</tr>
<tr>
<td><strong>packet-length bytes</strong></td>
<td>Length of the received packet, in bytes. The length refers only to the IP packet, including the packet header, and does not include any Layer 2 encapsulation overhead.</td>
</tr>
<tr>
<td><strong>precedence precedence</strong></td>
<td>IP precedence. For precedence, you can specify one of the following text synonyms (the field values are also listed): critical-ecp (5), flash (3), flash-override (4), immediate (2), internet-control (6), net-control (7), priority (1), routine (0)</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>ip-precedence precedence</code></td>
<td>IP precedence. For <em>precedence</em>, you can specify one of the following text synonyms (the field values are also listed): critical-ecp (5), flash (3), flash-override (4), immediate (2), internet-control (6), net-control (7), priority (1), routine (0)</td>
</tr>
<tr>
<td><code>protocol list of protocol</code></td>
<td>IPv4 protocol value. For <em>protocols</em>, you can specify one of the following text synonyms: egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ospf (89), pim (103), rsvp (46), tcp (6), udp (17)</td>
</tr>
<tr>
<td><code>ip-protocol list of protocol</code></td>
<td>IPv4 protocol value. For <em>protocols</em>, you can specify one of the following text synonyms: egp (8), esp (50), gre (47), icmp (1), igmp (2), ipip (4), ospf (89), pim (103), rsvp (46), tcp (6), udp (17)</td>
</tr>
<tr>
<td><code>source-address ip-address</code></td>
<td>IP source address field, which is the address of the source node sending the packet. For IPv6, the source-address field is 128 bits in length. The filter description syntax supports the text representations for IPv6 addresses that are described in RFC 2373, <em>IPv6 Addressing Architecture</em>.</td>
</tr>
<tr>
<td>`ip-source-address (ip-address</td>
<td>IPv6-address)`</td>
</tr>
<tr>
<td><code>source-mac-address mac-address</code></td>
<td>Source MAC address. You can define a source MAC address with a prefix, such as <em>source-mac-address 00:01:02:03:04:05/24</em>. If no prefix is specified, the default value 48 is used.</td>
</tr>
<tr>
<td><code>source-port number</code></td>
<td>TCP or UDP <em>source-port</em> field. Typically, you specify this match in conjunction with the <em>protocol</em> or <em>ip-protocol</em> match condition to determine which protocol is being used on the port. For <em>number</em>, you can specify one of the text synonyms listed under <em>destination-port</em>.</td>
</tr>
<tr>
<td><code>source-prefix-list prefix-list</code></td>
<td>IP source prefix list field. You can define a list of IP address prefixes under a prefix-list alias for frequent use. You define this match condition at the [edit policy-options] hierarchy level.</td>
</tr>
<tr>
<td><code>tcp-established</code></td>
<td>TCP packets of an established TCP connection. This condition matches packets other than the first packet of a connection. <em>tcp-established</em> is a synonym for the bit names &quot;(ack</td>
</tr>
<tr>
<td></td>
<td><em>tcp-established</em> does not implicitly check whether the protocol is TCP. To do so, specify the <em>next-header tcp</em> match condition.</td>
</tr>
</tbody>
</table>
### Table 501: Firewall Filter Match Conditions Supported on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tcp-flags (flags tcp-initial)</code></td>
<td>One or more TCP flags:</td>
</tr>
<tr>
<td></td>
<td>- bit-name—<code>fin</code>, <code>syn</code>, <code>rst</code>, <code>push</code>, <code>ack</code>, <code>urgent</code></td>
</tr>
<tr>
<td></td>
<td>- logical operators—<code>&amp;</code> (logical AND), `</td>
</tr>
<tr>
<td></td>
<td>- numerical value—0x01 through 0x20</td>
</tr>
<tr>
<td></td>
<td>- text synonym—<code>tcp-initial</code></td>
</tr>
<tr>
<td></td>
<td>To specify multiple flags, use logical operators.</td>
</tr>
</tbody>
</table>

- `tcp-initial` Matches the first TCP packet of a connection. `tcp-initial` is a synonym for the bit names `(syn&!ack)`.  
  `tcp-initial` does not implicitly check whether the protocol is TCP. To do so, specify the `protocol tcp` or `ip-protocol tcp` match condition.

- `traffic-class number` Specifies the DSCP code point for a packet.

- `ttl value` TTL type to match. The value ranges from 1 through 255.

- `vlan (vlan-name | vlan-id)` The VLAN that is associated with the packet. For `vlan-id`, you can specify either the VLAN ID or a VLAN range. The `vlan` match condition and the `dot1q-tag` match condition are mutually exclusive.

- `learn-vlan-id (vlan-name | vlan-id)` The VLAN that is associated with the packet. For `vlan-id`, you can specify either the VLAN ID or a VLAN range. The `vlan` match condition and the `user-vlan-id` match condition are mutually exclusive.

### Actions for Firewall Filters

You can define an action for the switch to take if a packet matches the filtering criteria defined in a match condition. Table 502 on page 4104 describes the actions supported in a firewall filter configuration.

### Table 502: Actions for Firewall Filters

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accept</code></td>
<td>Accept a packet.</td>
</tr>
<tr>
<td><code>discard</code></td>
<td>Discard a packet silently without sending an Internet Control Message Protocol (ICMP) message.</td>
</tr>
</tbody>
</table>
**Table 502: Actions for Firewall Filters (continued)**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reject message-type</td>
<td>Discard a packet, and send the ICMPv4 message (type 3) destination unreachable. You can log the rejected packets if you configure the syslog action modifier. You can specify one of the following message codes: administratively-prohibited (default), bad-host-tos, bad-network-tos, host-prohibited, host-unreachable, network-prohibited, network-unreachable, port-unreachable, precedence-cutoff, precedence-violation, protocol-unreachable, source-host-isolated, source-route-failed, tcp-reset. If you specify tcp-reset, a TCP reset is returned if the packet is a TCP packet. Otherwise nothing is returned. If you do not specify a message type, the ICMP notification destination unreachable is sent with the default message communication administratively filtered.</td>
</tr>
<tr>
<td>routing-instance</td>
<td>Forward matched packets to a virtual routing instance.</td>
</tr>
<tr>
<td>routing-instance-name</td>
<td>NOTE: EX4200 switches do not support firewall-filter-based redirection to the default routing instance.</td>
</tr>
<tr>
<td>vlan</td>
<td>Forward matched packets to a specific VLAN. Ensure that you specify the VLAN name or VLAN ID and not a VLAN range, because the vlan action does not support the vlan-range option. NOTE: If you have defined a VLAN that is enabled for dot1q tunneling, then that particular VLAN is not supported as an action (using the vlan vlan-name action) for an ingress VLAN firewall filter.</td>
</tr>
</tbody>
</table>

**Action Modifiers for Firewall Filters**

In addition to the actions described in Table 502 on page 4104, you can define action modifiers in a firewall filter configuration for a switch if packets match the filtering criteria defined in the match condition. Table 503 on page 4105 describes the action modifiers supported in a firewall filter configuration.

**Table 503: Action Modifiers for Firewall Filters**

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>analyzer analyzer-name</td>
<td>Mirror port traffic to a specified destination port or VLAN that is connected to a protocol analyzer application. Mirroring copies all packets seen on one switch port to a network monitoring connection on another switch port. The analyzer name must be configured under [edit ethernet-switching-options analyzer]. NOTE: analyzer is not a supported action modifier for a management interface. NOTE: On EX4500 switches, you can configure only one analyzer and include it in a firewall filter. If you configure multiple analyzers, you cannot include any one of those analyzers in a firewall filter.</td>
</tr>
<tr>
<td>Action Modifier</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dscp number</td>
<td>Change the DSCP value for matched packets to the DSCP value specified with this action modifier. <code>number</code> specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP.</td>
</tr>
<tr>
<td></td>
<td>You can specify DSCP in hexadecimal, binary, or decimal form.</td>
</tr>
<tr>
<td></td>
<td>For <code>number</code>, you can specify one of the following text synonyms (the field values are also listed):</td>
</tr>
<tr>
<td></td>
<td>• ef (46)—as defined in <a href="https://tools.ietf.org/html/rfc2598">RFC 2598, An Expedited Forwarding PHB</a>.</td>
</tr>
<tr>
<td></td>
<td>• af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38)</td>
</tr>
<tr>
<td></td>
<td>These four classes, with three drop precedences in each class, are defined for 12 code points in <a href="https://tools.ietf.org/html/rfc2597">RFC 2597, Assured Forwarding PHB Group</a>.</td>
</tr>
<tr>
<td>count counter-name</td>
<td>Count the number of packets that pass this filter, term, or policer. A policer enables you to specify rate limits on traffic that enters an interface on a switch.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> On EX4300 switches, you can configure the same number of counters and policers as the number of terms in the ternary content addressable memory (TCAM).</td>
</tr>
<tr>
<td>forwarding-class class</td>
<td>Classify the packet in one of the following forwarding classes:</td>
</tr>
<tr>
<td></td>
<td>• assured-forwarding</td>
</tr>
<tr>
<td></td>
<td>• best-effort</td>
</tr>
<tr>
<td></td>
<td>• expedited-forwarding</td>
</tr>
<tr>
<td></td>
<td>• network-control</td>
</tr>
<tr>
<td>interface interface-name</td>
<td>Forward the traffic to the specified interface bypassing the switching lookup.</td>
</tr>
<tr>
<td>log</td>
<td>Log the packet's header information in the Routing Engine. To view this information, issue the <code>show firewall log</code> command in the CLI.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If the log or the syslog action modifier is configured along with a vlan action or an interface action modifier, the events might not be logged. However, the redirect interface functionality works as expected.</td>
</tr>
<tr>
<td>loss-priority (high</td>
<td>Set the packet loss priority (PLP).</td>
</tr>
<tr>
<td>low)</td>
<td>policer policer-name</td>
</tr>
<tr>
<td></td>
<td>You can specify a policer in a firewall filter only for ingress traffic on a port, VLAN, and router.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> A counter for a policer is not supported on EX8200 switches.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> On EX4300 switches, you can configure the same number of counters and policers as the number of terms in the TCAM.</td>
</tr>
<tr>
<td>port-mirror</td>
<td>Mirror packets to the interface defined in the [edit forwarding-options analyzer] hierarchy.</td>
</tr>
</tbody>
</table>
Table 503: Action Modifiers for Firewall Filters (continued)

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port-mirror-instance instance-name</code></td>
<td>Mirror packets to the instance defined in the [edit forwarding-options analyzer] hierarchy.</td>
</tr>
<tr>
<td>syslog</td>
<td>Log an alert for this packet. You can specify that the log be sent to a server for storage and analysis. <strong>NOTE:</strong> If the <code>log</code> or the <code>syslog</code> action modifier is configured along with a <code>vlan</code> action or an <code>interface</code> action modifier, the events might not be logged. However, the redirect interface functionality works as expected.</td>
</tr>
</tbody>
</table>

| three-color-policer | Apply a three-color policer. |

Related Documentation

- Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches on page 4111
- Understanding Firewall Filter Match Conditions on page 4151
- Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches on page 4219
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183

Support for Match Conditions and Actions for Loopback Firewall Filters on Switches

On EX Series Ethernet switches, a loopback interface is a gateway for all the control traffic that enters the Routing Engine of the switch. If you want to monitor this control traffic, you must configure a firewall filter on the loopback interface (lo0). Loopback firewall filters are applied only to packets that are sent to the Routing Engine CPU for further processing. Therefore, you can apply a firewall filter only in the ingress direction on the loopback interface.

Each term in a firewall filter consists of match conditions and an action. Match conditions are the values or fields that a packet must contain. You can define multiple, single, or no match conditions. If no match conditions are specified for the term, all packets are matched by default. The string that defines a match condition is called a match statement. The action is the action that the switch takes if a packet matches the match conditions for the specific term. Action modifiers are optional and specify one or more actions that the switch takes if a packet matches the match conditions for the specific term.

The following tables list match conditions, actions, and action modifiers that are supported for a firewall filter configured on a loopback interface on a switch:

- Table 504 on page 4108
- Table 505 on page 4109
For information on match conditions, actions, and action modifiers supported for a firewall filter configured on a network interface, see “Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches” on page 4111.

Table 504: Match Conditions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX6200</th>
<th>EX8200</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Match conditions for IPv4 traffic:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>destination-address</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>destination-port</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>destination-prefix-list</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>dscp</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>icmp-code</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>icmp-type</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>interface</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>is-fragment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>packet-length</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>precedence or ip-precedence</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>protocol or ip-protocol</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>source-address</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>source-port</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>source-prefix-list</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Match conditions for IPv6 traffic:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>destination-address or ip6-destination-address</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>destination-port</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>destination-prefix-list</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>icmp-code</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
</tr>
</tbody>
</table>
Table 504: Match Conditions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX6200</th>
<th>EX8200</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-type</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>interface</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>next-header</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>packet-length</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>source-address or ip6-source-address</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>source-port</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>source-prefix-list</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>tcp-established</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>tcp-flags</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>tcp-initial</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>traffic-class</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 505: Actions for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch

<table>
<thead>
<tr>
<th>Action</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX6200</th>
<th>EX8200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions for IPv4 traffic:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>accept</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>discard</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Actions for IPv6 traffic:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>accept</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>discard</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
</tbody>
</table>
Table 506: Action Modifiers for Firewall Filters on Loopback Interfaces for IPv4 and IPv6 Traffic—Support per Switch

<table>
<thead>
<tr>
<th>Action Modifiers</th>
<th>EX2200</th>
<th>EX3200, EX4200</th>
<th>EX3300</th>
<th>EX4300</th>
<th>EX4500</th>
<th>EX6200</th>
<th>EX8200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action modifiers for IPv4 traffic:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>count</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>–</td>
</tr>
<tr>
<td>forwarding-class</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>loss-priority</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>port-mirror</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>port-mirror-instance</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Action modifiers for IPv6 traffic:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>count</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>forwarding-class</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>loss-priority</td>
<td>–</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
<td>✓</td>
<td>–</td>
<td>✓</td>
</tr>
<tr>
<td>port-mirror</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>port-mirror-instance</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

NOTE: On EX8200 switches, if an implicit or explicit discard action is configured on a loopback interface for IPv4 traffic, next hop resolve packets are accepted and allowed to pass through the switch. However, for IPv6 traffic, you must explicitly configure a rule to allow the neighbor discovery IPv6 resolve packets to pass through the switch.

Related Documentation
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches on page 4111
- Understanding Firewall Filter Match Conditions on page 4151
- Understanding How Firewall Filters Are Evaluated on page 4149
- Understanding How Firewall Filters Test a Packet’s Protocol on page 4155
- Understanding the Use of Policers in Firewall Filters on page 4155
Platform Support for Firewall Filter Match Conditions, Actions, and Action Modifiers on EX Series Switches

After you define a firewall filter on an EX Series switch, you must associate the filter to a bind point so that the filter can filter the packets that enter or exit the bind point. Port firewall filters, VLAN firewall filters, and Layer 3 (or router) firewall filters are the different types of firewall filters you can apply on a switch, depending on the bind points the filters are associated with. While a port firewall filter applies to Layer 2 interfaces, a VLAN firewall filter applies to packets that enter or leave a VLAN and also to packets that are bridged within a VLAN. A Layer 3 firewall filter applies to Layer 3 (routed) interfaces and routed VLAN interfaces (RVIs).

NOTE: If you want to control the traffic that enters the Routing Engine of the switch, you must configure a firewall filter on the loopback interface (lo0) of the switch. For information about match conditions, actions, and action modifiers supported on the loopback interface of a switch, see “Support for Match Conditions and Actions for Loopback Firewall Filters on Switches” on page 4107.

This topic describes the supported switches and bind points for match conditions, actions, and action modifiers for firewall filters supported on EX Series switches. For descriptions of the match conditions, actions, and action modifiers, see “Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 4096.

This topic describes:

- Firewall Filter Types and Their Bind Points on page 4111
- Support for IPv4 and IPv6 Firewall Filters on Switches on page 4112
- Platform Support for Match Conditions for IPv4 Traffic on page 4112
- Platform Support for Match Conditions for IPv6 Traffic on page 4125
- Platform Support for Match Conditions for Non-IP Traffic on page 4133
- Platform Support for Actions for IPv4 Traffic on page 4133
- Platform Support for Actions for IPv6 Traffic on page 4136
- Platform Support for Action Modifiers for IPv4 Traffic on page 4138
- Platform Support for Action Modifiers for IPv6 Traffic on page 4144

Firewall Filter Types and Their Bind Points

You can apply a firewall filter at specific bind points to filter IPv4, IPv6, or non-IP traffic. See the remaining sections in this topic for information about support on individual switches for different traffic types.

Table 507 on page 4112 lists the firewall filter types and their associated bind points that are supported on the switches.
Table 507: Bind Points Associated with Firewall Filter Types

<table>
<thead>
<tr>
<th>Bind Points</th>
<th>Firewall Filter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports (Layer 2 interfaces)</td>
<td>Port firewall filter</td>
</tr>
<tr>
<td>VLANs</td>
<td>VLAN firewall filter</td>
</tr>
<tr>
<td>Layer 3 interfaces (Layer 3 (routed) interfaces or routed VLAN interfaces (RVIs))</td>
<td>Router firewall filter</td>
</tr>
</tbody>
</table>

Support for IPv4 and IPv6 Firewall Filters on Switches

You can apply a port, VLAN, or router firewall filter to filter IPv4 traffic on all EX Series switches. You can apply port, VLAN, and router firewall filters for IPv6 traffic on EX3200, EX4200, EX4300, and EX8200 switches and only router firewall filters for IPv6 traffic on EX2200, EX3300, and EX4500 switches.

Table 508 on page 4112 briefly summarizes the support for IPv4 and IPv6 firewall filters on different switches. The support for port, VLAN, and router firewall filters on different switches is further discussed in the subsequent sections in this topic.

Table 508: Support for IPv4 and IPv6 Firewall Filters on Switches

<table>
<thead>
<tr>
<th>Switch</th>
<th>Support for IPv4 Firewall Filter</th>
<th>Support for IPv6 Firewall Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EX3200 and EX4200</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EX3300</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EX4300</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EX4500</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EX6200</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>EX8200</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Platform Support for Match Conditions for IPv4 Traffic

You can define port, VLAN, and router firewall filters for ingress and egress IPv4 traffic on all EX Series switches. Table 509 on page 4113 summarizes the support for match conditions on different bind points for ingress and egress IPv4 traffic on different switches.
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>destination-address</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>ip-address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>ip-destination-address</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td>ip-address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>destination-mac-address</strong></td>
<td>EX2200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>mac-address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
</tbody>
</table>
Table 509: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches *(continued)*

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-port number</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>destination-prefix-list</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>prefix-list</td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
</tbody>
</table>
Table 509: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>dot1q-tag number</strong></td>
<td>EX2200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>user-vlan-id number</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>dot1q-user-priority number</strong></td>
<td>EX2200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>user-vlan-1p-priority number</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Switch</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>dscp number</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>ether-type value</strong></td>
<td>EX2200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Switch</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX3200</td>
<td>Not supported</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX4200</td>
<td>Not supported</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX4300</td>
<td>Not supported</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX6200</td>
<td>Not supported</td>
</tr>
<tr>
<td>fragment-flags</td>
<td>EX8200</td>
<td>Not supported</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX3200</td>
<td>Ports and Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX4200</td>
<td>Ports and Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
</tbody>
</table>
Table 509: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-type number</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td>interface interface-name</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
</tbody>
</table>
### Table 509: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td>ip-options</td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td>ip-version</td>
<td>EX2200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>version match_condition(s)</td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
</tbody>
</table>
Table 509: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>is-fragment</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>precedence</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>ip-precedence</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Switch</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>----------------</td>
<td>--------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>protocol list of protocols</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>ip-protocol list of protocols</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>source-address</strong>&lt;br&gt;<strong>ip-address</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>ip-source-address</strong>&lt;br&gt;<strong>ip-address</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Switch</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Ingress</td>
<td>Egress</td>
</tr>
<tr>
<td><strong>source-mac-address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mac-address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX2200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>EX3300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>EX4500</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>EX6200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>EX8200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>source-port number</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
</tbody>
</table>
Table 509: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-prefix-list</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td>tcp-established</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td>Match Condition</td>
<td>Switch</td>
<td>Supported Bind Points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
<td>----------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>tcp-flags (flags tcp-initial)</strong></td>
<td><strong>EX2200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX3200 and EX4200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX3300</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX4300</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX4500</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX6200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX8200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td><strong>tcp-initial</strong></td>
<td><strong>EX2200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX3200 and EX4200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX3300</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX4300</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX4500</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX6200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>EX8200</strong></td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
</tbody>
</table>
Table 509: Firewall Filter Match Conditions Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td>ttl value</td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td>vlan (vlan-name</td>
<td>EX2200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>vlan-id)</td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
</tbody>
</table>

Platform Support for Match Conditions for IPv6 Traffic

You can define port, VLAN, and router firewall filters for ingress and egress IPv6 traffic on EX3200, EX4200, and EX8200 switches, and router firewall filters for ingress and egress IPv6 traffic on EX2200, EX3300, and EX4500 switches. Table 510 on page 4126 summarizes support for match conditions on different bind points for ingress and egress IPv6 traffic on different switches.
<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Ingress</strong></td>
</tr>
<tr>
<td><strong>destination-address</strong>&lt;br&gt; <em>ip-address</em>&lt;br&gt; <em>ip6-destination-address</em>&lt;br&gt; <em>ip-address</em></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX2200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>destination-mac-address</strong>&lt;br&gt; <em>mac-address</em></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>destination-port</strong>&lt;br&gt; <em>number</em></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>Match Condition</td>
<td>Switch</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>destination-prefix-list</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td>prefix-list</td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>dot1q-tag-number</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>user-vlan-id-number</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>dot1q-user-priority-number</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td><strong>user-vlan-1p-priority-number</strong></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
</tbody>
</table>
Table 510: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td>ether-type (ipv6)_value</td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>icmp-type number</td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
</tbody>
</table>
Table 510: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td>interface</td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td>interface-name</td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>ip-version</td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td>version</td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
</tr>
<tr>
<td>match_condition(s)</td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td>next-header</td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td>bytes</td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
</tbody>
</table>
### Table 510: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>packet-length bytes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>source-address ip-address</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>ip6-source-address ip-address</strong></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>source-mac-address mac-address</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
</tr>
</tbody>
</table>
Table 510: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>source-port number</strong></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>source-prefix-list prefix-list</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>tcp-established</strong></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
</tbody>
</table>
### Table 510: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>tcp-flags (flags</strong></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>tcp-initial**</td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td><strong>traffic-class number</strong></td>
<td>EX2200</td>
<td>Not supported</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
</tbody>
</table>
Table 510: Firewall Filter Match Conditions Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan (vlan-id</td>
<td>vlan-name)</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
<td></td>
</tr>
</tbody>
</table>

Platform Support for Match Conditions for Non-IP Traffic

You can define port, VLAN, and router firewall filters for ingress and egress non-IP traffic on all EX Series switches. Table 511 on page 4133 summarizes support for match conditions on different bind points for ingress and egress non-IP traffic on different switches.

Table 511: Firewall Filter Match Condition Supported for Non-IP Traffic on Switches

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2-encap-type llc-non-snap</td>
<td>EX2200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
<td></td>
</tr>
</tbody>
</table>

Platform Support for Actions for IPv4 Traffic

Table 512 on page 4134 summarizes the support for actions on different bind points for ingress and egress IPv4 traffic on different switches.
### Table 512: Firewall Filter Actions Supported for IPv4 Traffic on Switches

<table>
<thead>
<tr>
<th>Action</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Ingress</strong></td>
</tr>
<tr>
<td></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>accept</td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>discard</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>Action</td>
<td>Switch</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>reject message-type</strong></td>
<td><strong>EX2200</strong></td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td><strong>EX3200 and EX4200</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td><strong>EX3300</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td><strong>EX4300</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td><strong>EX4500</strong></td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td><strong>EX6200</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td><strong>EX8200</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>routing-instance</strong></td>
<td><strong>EX2200</strong></td>
<td>Not supported</td>
</tr>
<tr>
<td><strong>routing-instance-name</strong></td>
<td><strong>EX3200 and EX4200</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td><strong>EX3300</strong></td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td><strong>EX4300</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td><strong>EX4500</strong></td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td><strong>EX6200</strong></td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td><strong>EX8200</strong></td>
<td>Layer 3 interfaces</td>
</tr>
</tbody>
</table>
### Table 512: Firewall Filter Actions Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong><code>vlan</code> <code>vlan-name</code></strong></td>
<td>EX2200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
<td>Ports</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
<td>Ports and VLANs</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

*NOTE:* Supported only when used in conjunction with the `interface` action modifier. On EX8200 Virtual Chassis, the `vlan` action is supported only for VLANs.

---

### Platform Support for Actions for IPv6 Traffic

Table 513 on page 4136 summarizes the support for actions on different bind points for ingress and egress IPv6 traffic.

### Table 513: Firewall Filter Actions Supported for IPv6 Traffic on Switches

<table>
<thead>
<tr>
<th>Action</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accept</code></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>Action</td>
<td>Switch</td>
<td>Supported Bind Points</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
<td>Egress</td>
</tr>
<tr>
<td>discard</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>reject message-type</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td>routing-instance</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>routing-instance-name</td>
<td>EX3200 and EX4200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
### Table 513: Firewall Filter Actions Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan vlan-name</td>
<td>EX2200</td>
<td>Not supported Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs Not supported</td>
</tr>
</tbody>
</table>

**NOTE:** Supported only when used in conjunction with the `interface` action modifier. On EX8200 Virtual Chassis, the `vlan` action is supported only for VLANs.

### Platform Support for Action Modifiers for IPv4 Traffic

Table 514 on page 4139 summarizes support for action modifiers on different bind points for ingress and egress IPv4 traffic on different switches.
Table 514: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>analyzer</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td><strong>dscp</strong></td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
</tbody>
</table>
Table 514: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Ingress</strong></td>
</tr>
<tr>
<td>count</td>
<td>EX2200</td>
<td>VLANs and Layer 3 interfaces (me0 interfaces only)</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>VLANs and Layer 3 interfaces (me0 and vme0 interfaces only)</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>forwarding-class class</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
</tbody>
</table>
Table 514: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
<td>Egress</td>
</tr>
<tr>
<td>interface</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>interface-name</td>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

**NOTE:** On EX8200 Virtual Chassis, the `interface` action modifier is supported only for VLANs.

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
### Table 514: Firewall Filter Action Modifiers Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Ingress</strong></td>
</tr>
<tr>
<td>**loss-priority (high</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>or low)**</td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>policer policer-name</strong></td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td>Action Modifier</td>
<td>Switch</td>
<td>Supported Bind Points</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>port-mirror</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Not supported</td>
</tr>
<tr>
<td><strong>port-mirror-instance</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td><strong>instance-name</strong></td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
### Table 514: Firewall Filter ActionModifiers Supported for IPv4 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>three-color-policer</td>
<td>EX2200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX6200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
</tbody>
</table>

---

**Platform Support for Action Modifiers for IPv6 Traffic**

Table 515 on page 4145 summarizes support for action modifiers on different bind points for ingress and egress IPv6 traffic.
Table 515: Firewall Filter Action Modifiers Supported for IPv6 Traffic on Switches

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>analyzer</td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>dscp</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>count</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces (me0 and vme0 interfaces only)</td>
<td>Layer 3 interfaces (me0 and vme0 interfaces only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>Action Modifier</td>
<td>Switch</td>
<td>Supported Bind Points</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>-----------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
<td>Egress</td>
<td></td>
</tr>
<tr>
<td>forwarding-class class</td>
<td>EX2200</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports and Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Ports and Layer 3 interfaces</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interface interface-name</th>
<th>EX2200</th>
<th>Not supported</th>
<th>Not supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3200 and EX4200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>EX3300</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>EX4300</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>EX4500</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>EX8200</td>
<td>Ports and VLANs</td>
<td>Not supported</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** On EX8200 Virtual Chassis, the interface action modifier is supported only for VLANs.

<table>
<thead>
<tr>
<th>log</th>
<th>EX2200</th>
<th>Not supported</th>
<th>Not supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
<td>Layer 3 interfaces</td>
<td></td>
</tr>
<tr>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>EX4500</td>
<td>Not supported</td>
<td>Not supported</td>
<td></td>
</tr>
<tr>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
<td>Not supported</td>
<td></td>
</tr>
</tbody>
</table>
### Table 515: Firewall Filter Action Modifiers Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Ingress</strong></td>
</tr>
<tr>
<td><strong>loss-priority</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>high</td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td>low</td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>policer policer-name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX2200</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>port-mirror</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
### Table 515: Firewall Filter Action Modifiers Supported for IPv6 Traffic on Switches (continued)

<table>
<thead>
<tr>
<th>Action Modifier</th>
<th>Switch</th>
<th>Supported Bind Points</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ingress</td>
</tr>
<tr>
<td><strong>port-mirror-instance</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td><strong>instance-name</strong></td>
<td>EX3200 and EX4200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Not supported</td>
</tr>
<tr>
<td><strong>syslog</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Ports, VLANs, and Layer 3 interfaces</td>
</tr>
<tr>
<td><strong>three-color-policer</strong></td>
<td>EX2200</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX3200 and EX4200</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td>EX3300</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX4300</td>
<td>Not Supported</td>
</tr>
<tr>
<td></td>
<td>EX4500</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>EX8200</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>

**Related Documentation**
- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096](#)
- [Support for Match Conditions and Actions for Loopback Firewall Filters on Switches on page 4107](#)
- [Understanding Firewall Filter Match Conditions on page 4151](#)
Understanding How Firewall Filters Are Evaluated

A firewall filter consists of one or more terms, and the order of the terms within a firewall filter is important. Before you configure firewall filters, you should understand how Juniper Networks EX Series Ethernet Switches evaluate the terms within a firewall filter and how packets are evaluated against the terms.

When a firewall filter consists of a single term, the filter is evaluated as follows:

- If the packet matches all the conditions, the action in the `then` statement is taken.
- If the packet matches all the conditions, and no action is specified in the `then` statement, the default action `accept` is taken.

When a firewall filter consists of more than one term, the firewall filter is evaluated sequentially:

1. The packet is evaluated against the conditions in the `from` statement in the first term.
2. If the packet matches all the conditions in the term, the action in the `then` statement is taken and the evaluation ends. Subsequent terms in the filter are not evaluated.
3. If the packet does not match all the conditions in the term, the packet is evaluated against the conditions in the `from` statement in the second term.
   - This process continues until either the packet matches the conditions in the `from` statement in one of the subsequent terms or there are no more terms in the filter.
4. If a packet passes through all the terms in the filter without a match, the packet is discarded.

Figure 60 on page 4150 shows how an EX Series switch evaluates the terms within a firewall filter.
If a term does not contain a `from` statement, the packet is considered to match and the action in the `then` statement of the term is taken.

If a term does not contain a `then` statement, or if an action has not been configured in the `then` statement, and the packet matches the conditions in the `from` statement of the term, the packet is accepted.

Every firewall filter contains an implicit `deny` statement at the end of the filter, which is equivalent to the following explicit filter term:

```
term implicit-rule {
    then discard;
}
```

Consequently, if a packet passes through all the terms in a filter without matching any conditions, the packet is discarded. If you configure a firewall filter that has no terms, all packets that pass through the filter are discarded.

**NOTE:** Firewall filtering is supported on packets that are at least 48 bytes long.

---

**Related Documentation**

- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding Firewall Filter Match Conditions on page 4151
- Understanding the Use of Policers in Firewall Filters on page 4155
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
Understanding Firewall Filter Match Conditions

Before you define terms for firewall filters, you must understand how the match conditions that you specify in a term are handled and how to specify various types of match conditions to achieve the desired filtering results. A match condition consists of a string (called a match statement) that defines the match condition. Match conditions are the values or fields that a packet must contain.

This topic describes:

- Filter Match Conditions on page 4151
- Numeric Filter Match Conditions on page 4151
- Interface Filter Match Conditions on page 4152
- IP Address Filter Match Conditions on page 4152
- MAC Address Filter Match Conditions on page 4153
- Bit-Field Filter Match Conditions on page 4153

Filter Match Conditions

In the from statement of a firewall filter term, you specify the packet conditions that trigger the action in one of the then statements: then with various options, then interface or then vlan. All conditions in the from statement must match for the action to be taken. The order in which you specify match conditions is not important, because a packet must match all the conditions in a term for a match to occur.

If you specify no match conditions in a term, that term matches all packets.

An individual condition in a from statement cannot contain a list of values. For example, you cannot specify numeric ranges or multiple source or destination addresses.

Individual conditions in a from statement cannot be negated. A negated condition is an explicit mismatch.

Numeric Filter Match Conditions

Numeric filter conditions match packet fields that are identified by a numeric value, such as port and protocol numbers. For numeric filter match conditions, you specify a keyword that identifies the condition and a single value that a field in a packet must match.

You can specify the numeric value in one of the following ways:

- Single number—A match occurs if the value of the field matches the number. For example:
  
  source-port 25;

- Text synonym for a single number— A match occurs if the value of the field matches the number that corresponds to the synonym. For example:
  
  source-port http;
To specify more than one value in a filter term, you enter each value in its own match statement, which is a string that defines a match condition. For example, a match occurs in the following term if the value of `vlan` is 10 or 30.

```
[edit firewall family family-name filter filter-name term term-name from]
  vlan 10;
  vlan 30;
```

The following restrictions apply to numeric filter match conditions:

- You cannot specify a range of values.
- You cannot specify a list of comma-separated values.
- You cannot exclude a specific value in a numeric filter match condition. For example, you cannot specify a condition that would match only if the match condition was not equal to a given value.

### Interface Filter Match Conditions

Interface filter match conditions can match interface name values in a packet. For interface filter match conditions, you specify the name of the interface, for example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/0/1
```

Port and VLAN interfaces do not use logical unit numbers. However, a firewall filter that is applied to a router interface can specify the logical unit number in the interface filter match condition, for example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/1/0.0
```

You can include the `*` wildcard as part of the interface name, for example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set interface ge-0/*/1
user@switch# set interface ge-0/1/*
user@switch# set interface ge-*
```

### IP Address Filter Match Conditions

Address filter match conditions can match prefix values in a packet, such as IP source and destination prefixes. For address filter match conditions, you specify a keyword that identifies the field and one prefix of that type that a packet must match.

You specify the address as a single prefix. A match occurs if the value of the field matches the prefix. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10.2.1.0/28;
```

Each prefix contains an implicit 0/0 except statement, which means that any prefix that does not match the prefix that is specified is explicitly considered not to match.

To specify the address prefix, use the notation prefix/prefix-length. If you omit prefix-length, it defaults to /32. For example:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-address 10
To specify more than one IP address in a filter term, you enter each address in its own match statement. For example, a match occurs in the following term if the value of the source-address field matches either of the following source-address prefixes:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-address 10.0.0.0/8
user@switch# set source-address 10.1.0.0/16
```

### MAC Address Filter Match Conditions

MAC address filter match conditions can match source and destination MAC address values in a packet. For MAC address filter match conditions, you specify a keyword that identifies the field and one value of that type that a packet must match.

You can specify the MAC address as six hexadecimal bytes in the following formats:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set destination-mac-address 0011.2233.4455
user@switch# set destination-mac-address 00:11:22:33:44:55
user@switch# set destination-mac-address 001122334455
```

To specify more than one MAC address in a filter term, you enter each MAC address in its own match statement. For example, a match occurs in the following term if the value of the source-mac-address field matches either of the following addresses:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set source-mac-address 00:11:22:33:44:55
user@switch# set source-mac-address 00:11:22:33:20:15
```

### Bit-Field Filter Match Conditions

Bit-field filter conditions match packet fields if particular bits in those fields are or are not set. You can match the IP options, TCP flags, and IP fragmentation fields. For bit-field filter match conditions, you specify a keyword that identifies the field and tests to determine that the option is present in the field.

To specify the bit-field value to match, enclose the value in double quotation marks. For example, a match occurs if the RST bit in the TCP flags field is set:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "rst"
```

Typically, you specify the bits to be tested by using keywords. Bit-field match keywords always map to a single bit value. You also can specify bit fields as hexadecimal or decimal numbers.

To match multiple bit-field values, use the logical operators, which are described in Table 516 on page 4154. The operators are listed in order from highest precedence to lowest precedence. Operations are left-associative.
Table 516: Logical Operators for Matching Multiple Bit-Field Operators

<table>
<thead>
<tr>
<th>Logical Operators</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Negation.</td>
</tr>
<tr>
<td>&amp;</td>
<td>Logical AND.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To negate a match, precede the value with an exclamation point. For example, a match occurs only if the RST bit in the TCP flags field is not set:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "!rst"
```

In the following example of a logical AND operation, a match occurs if the packet is the initial packet on a TCP session:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn&!ack"
```

In the following example of a logical OR operation, a match occurs if the packet is not the initial packet on a TCP session:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags "syn|ack"
```

For a logical OR operation, you can specify a maximum of two match conditions in a single term. If you need to match more than two bit-field values in a logical OR operation, configure the same match condition in consecutive terms with additional bit-field values. In the following example, the two terms configured match the SYN, ACK, FIN, or RST bit in the TCP flags field:

```
[edit firewall family family-name filter filter-name term term-name1 from]
user@switch# set tcp-flags "syn|ack"
[edit firewall family family-name filter filter-name term term-name2 from]
user@switch# set tcp-flags "fin|rst"
```

You can use text synonyms to specify some common bit-field matches. You specify these matches as a single keyword. In the following example of a text synonym, a match occurs if the packet is the initial packet on a TCP session:

```
[edit firewall family family-name filter filter-name term term-name from]
user@switch# set tcp-flags tcp-initial
```

Related Documentation:
- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding How Firewall Filters Test a Packet’s Protocol on page 4155
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
Understanding How Firewall Filters Test a Packet's Protocol

When examining match conditions, Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches tests only the field that is specified. The software does not implicitly test the IP header to determine whether a packet is an IP packet. Therefore, in some cases, you must specify protocol field match conditions in conjunction with other match conditions to ensure that the filters are performing the expected matches.

If you specify a protocol match condition or a match of the ICMP type or TCP flags field, there is no implied protocol match. For the following match conditions, you must explicitly specify the protocol match condition in the same term:

- **destination-port**—Specify the match `protocol tcp` or `protocol udp`.
- **source-port**—Specify the match `protocol tcp` or `protocol udp`.

If you do not specify the protocol when using the preceding fields, design your filters carefully to ensure that they perform the expected matches. For example, if you specify a match of `destination-port ssh`, the switch deterministically matches any packets that have a value of 22 in the two-byte field that is two bytes beyond the end of the IP header without ever checking the IP protocol field.

Related Documentation

- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding Firewall Filter Match Conditions on page 4151
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161

Understanding the Use of Policers in Firewall Filters

Policing, or rate limiting, is an important component of firewall filters that lets you control the amount of traffic that enters an interface on Juniper Networks EX Series Ethernet Switches. You can achieve policing by including policers in firewall filter configurations.

This topic describes:

- Policers Overview on page 4155
- Policer Types on page 4156
- Policer Actions on page 4157
- Policer Levels on page 4157
- Color Modes on page 4158
- Naming Conventions for Policers on page 4158

Policers Overview

You can use policers to specify rate limits on traffic. A firewall filter configured with a policer permits only traffic within a specified set of rate limits, thereby providing protection from denial-of-service (DoS) attacks. Traffic that exceeds the rate limits specified by
the policer is either discarded immediately or is marked as lower priority than traffic that is within the rate limits. The switch discards the lower-priority traffic when there is traffic congestion.

A policer applies two types of rate limits on traffic:

- **Bandwidth**—The number of bits per second permitted, on average.
- **Maximum burst size**—The maximum size permitted for bursts of data that exceed the given bandwidth limit.

Policing uses an algorithm to enforce a limit on average bandwidth while allowing bursts up to a specified maximum value. You can define specific classes of traffic on an interface and apply a set of rate limits to each class. After you name and configure a policer, it is stored as a template. You can then use the policer in a firewall filter configuration.

On all EX Series switches except Juniper Networks EX8200 Ethernet Switches, each policer that you configure includes an implicit counter that counts the number of packets that exceed the rate limit specified for the policer. Each EX8200 switch contains three global management counters. You must assign ingress policers to these global management counters to obtain policer statistics. You can assign any number of ingress policers to each global management counter. The policer statistics for each global management counter are the aggregate of the policer statistics for all policers associated with that global management counter.

To get filter-specific packet counts, you must configure a different policer for each firewall filter. Policers give term-specific counts by default.

**Policer Types**

Switches support three types of policers:

- **Single-rate two-color**—A two-color policer (sometimes called simply “policer”) meters the traffic stream and classifies packets into two categories of packet loss priority (PLP) according to a configured bandwidth and burst-size limit. You can mark packets that exceed the bandwidth and burst-size limit or simply discard them. A two-color policer is most useful for metering traffic at the port (physical interface) level.

- **Single-rate three-color**—This type of policer is defined in RFC 2697, A *Single Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured committed information rate (CIR), committed burst size (CBS), and the excess burst size (EBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on whether the packets are arriving at rates that are below the CBS (green), exceed the CBS but not the EBS (yellow), or exceed the EBS (red). A single-rate three-color policer is most useful when a service is structured according to packet size and not according to peak arrival rate.

- **Two-rate three-color**—This type of policer is defined in RFC 2698, A *Two Rate Three Color Marker*, as part of an assured forwarding (AF) per-hop-behavior (PHB) classification system for a Differentiated Services (DiffServ) environment. This type of policer meters traffic based on the configured CIR and the peak information rate
(PIR), along with their associated burst sizes; the CBS, and the peak burst size (PBS). Traffic is marked as belonging to one of three categories (green, yellow, or red) based on packets are arriving at rates that are below the CIR (green), exceed the CIR but not the PIR (yellow), or exceed the PIR (red). A two-rate three-color policer is most useful when a service is structured according to arrival rates and not to packet size.

**Policer Actions**

Policer actions can be implicit or explicit and vary by policer type. The term implicit means that Junos OS assigns a loss-priority value automatically; explicit means that you configure the action. Table 517 on page 4157 lists policer actions.

<table>
<thead>
<tr>
<th>Policier</th>
<th>Marking</th>
<th>Implicit Action</th>
<th>Configurable Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-rate two-color</td>
<td>Green (Conforming)</td>
<td>Assign low loss priority</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Red (Nonconforming)</td>
<td>None</td>
<td>Assign low or high loss priority, assign a forwarding class, or discard</td>
</tr>
<tr>
<td></td>
<td>Yellow</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Single-rate three-color</td>
<td>Green (Conforming)</td>
<td>Assign low loss priority</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Red (Above the EBS)</td>
<td>Assign high loss priority</td>
<td>Discard</td>
</tr>
<tr>
<td></td>
<td>Yellow (Exceeds the CBS but not the EBS)</td>
<td>Assign high loss priority</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: Not supported on EX8200 switches</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: Not supported on EX8200 switches</td>
<td></td>
</tr>
<tr>
<td>Two-rate three-color</td>
<td>Green (Conforming)</td>
<td>Assign low loss priority</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Red (Above the PIR)</td>
<td>Assign high loss priority</td>
<td>Discard</td>
</tr>
<tr>
<td></td>
<td>Yellow (Exceeds the CIR but not the PIR)</td>
<td>Assign high loss priority</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: Not supported on EX8200 switches</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: Not supported on EX8200 switches</td>
<td></td>
</tr>
</tbody>
</table>

**Policer Levels**

You can configure policers at the queue level, logical interface level, or Layer 2 (MAC) level. Only a single policer is applied to a packet at the egress queue. The search for policers occurs in this order:

- Queue level
- Logical interface level
- Layer 2 (MAC) level
Color Modes

Tricolor marking (TCM) policers are not bound by a green-yellow-red coloring convention. Packets are marked with low or high PLP bit configurations based on color. Therefore, both three-color policer types (single-rate and two-rate) extend the functionality of class-of-service (CoS) traffic policing by providing three levels of drop precedence (loss priority) instead of the two normally available in policers. Both single-rate and two-rate three-color policer types can operate in two modes:

- **Color-blind**—In color-blind mode, the three-color policer operates without reference to whether the examined packets have been previously marked or metered. In other words, the three-color policer is *blind* to any previous coloring a packet might have had.

- **Color-aware**—In color-aware mode, the three-color policer operates with reference to any previous marking or metering of the examined packets. In other words, the three-color policer is aware of the previous coloring a packet might have had. In color-aware mode, the three-color policer can increase the PLP of a packet but can never decrease it. For example, if a color-aware three-color policer meters a packet with a low PLP marking, it can raise the PLP level to high. But it cannot reduce a high PLP level to low.

Naming Conventions for Policers

We recommend you use the naming convention `rate-TCMnumber-colortype` when configuring three-color policers. TCM stands for tricolor marking. Because policers can be numerous and must be applied correctly to work, observing a simple naming convention makes it easier to apply the policers properly.

For example, if you configure a single-rate, three-color, color-aware policer, name it `srTCM1-ca`. If you configure a two-rate, three-color, color-blind policer, name it `trTCM2-cb`. The **Related Documentation** section includes links to related resources.

Understanding Filter-Based Forwarding for EX Series Switches

Administrators of Juniper Networks EX Series Ethernet Switches can use firewall filters in conjunction with virtual routing instances to specify different routes for packets to travel in their networks. To set up this feature, which is called filter-based forwarding, you specify a filter and match criteria and then specify the virtual routing instance to send packets to.

You might want to use filter-based forwarding to route specific types of traffic through a firewall or security device before the traffic continues on its path. You can also use...
filter-based forwarding to give certain types of traffic preferential treatment or to improve load balancing of switch traffic.

**Related Documentation**
- Understanding Virtual Routing Instances on EX Series Switches on page 2062
- Firewall Filters for EX Series Switches Overview on page 4088
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183

**Understanding Tricolor Marking Architecture**

Tricolor marking (TCM) policers provide two functions: metering and marking. A policer meters each packet and passes the packet and the metering result to the marker.

The meter operates in two modes. In the color-blind mode, the meter treats the packet stream as uncolored. Any preset loss priorities are ignored. In the color-aware mode, the meter inspects the packet loss priority (PLP) field, which has been set by an upstream device as high or low; in other words, the PLP field has already been set by a behavior aggregate (BA) or multifield (MF) classifier. The marker changes the PLP of each incoming IP packet according to the results of the meter.

Single-rate TCM is so called because traffic is policed according to one rate—the committed burst rate (CBR)—and two burst sizes: the committed burst size (CBS) and the excess burst size (EBS). The configured information rate (CIR) specifies the average rate at which bits are admitted to the network. The CBS specifies the usual burst size in bytes and the EBS specifies the maximum burst size in bytes for packets that are admitted to the network. The EBS is greater than or equal to the CBS, and neither can be 0. As each packet enters the network, its bytes are counted. Packets that do not exceed the CBS are marked low PLP. Packets that exceed the peak information rate (PIR) are marked high PLP.

Two-rate TCM is so called because traffic is policed according to two rates: the CIR and the PIR. The PIR is greater than or equal to the CIR. The CIR specifies the average rate at which bits are admitted to the network, and the PIR specifies the maximum rate at which bits are admitted to the network. As each packet enters the network, its bits are counted. Bits in packets that do not exceed the CIR have their packets marked low PLP. Bits in packets that exceed the PIR have their packets marked high PLP.

**Related Documentation**
- Understanding the Use of Policers in Firewall Filters on page 4155
- Configuring Tricolor Marking Policers on page 4215
CHAPTER 78

Configuration

- Configuration Examples on page 4161
- Configuration Tasks on page 4191
- Configuration Statements on page 4217

Configuration Examples

- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch on page 4179
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183
- Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication on page 4186

Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches

This example shows how to configure and apply firewall filters to control traffic that is entering or exiting a port on the switch, a VLAN on the network, and a Layer 3 interface on the switch. Firewall filters define the rules that determine whether to forward or deny packets at specific processing points in the packet flow.

- Requirements on page 4162
- Overview on page 4162
- Configuring an Ingress Port Firewall Filter to Prioritize Voice Traffic and Rate-Limit TCP and ICMP Traffic on page 4165
- Configuring a VLAN Ingress Firewall Filter to Prevent Rogue Devices from Disrupting VoIP Traffic on page 4170
- Configuring a VLAN Firewall Filter to Count, Monitor, and Analyze Egress Traffic on the Employee VLAN on page 4172
- Configuring a VLAN Firewall Filter to Restrict Guest-to-Employee Traffic and Peer-to-Peer Applications on the Guest VLAN on page 4174
• Configuring a Router Firewall Filter to Give Priority to Egress Traffic Destined for the Corporate Subnet on page 4176
• Verification on page 4177

Requirements

This example uses the following software and hardware components:

• Junos OS Release 9.0 or later for EX Series switches.
• Two Juniper Networks EX3200-48T switches: one to be used as an access switch, the other to be used as a distribution switch
• One Juniper Networks EX-UM-4SFP uplink module
• One Juniper Networks J-series router

Before you configure and apply the firewall filters in this example, be sure you have:

• An understanding of firewall filter concepts, policers, and CoS
• Installed the uplink module in the distribution switch. See Installing an Uplink Module in an EX3200 Switch.

Overview

This configuration example show how to configure and apply firewall filters to provide rules to evaluate the contents of packets and determine when to discard, forward, classify, count, and analyze packets that are destined for or originating from the EX Series switches that handle all voice-vlan, employee-vlan, and guest-vlan traffic. Table 518 on page 4162 shows the firewall filters that are configured for the EX Series switches in this example.

Table 518: Configuration Components: Firewall Filters

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port firewall filter, ingress-port-voip-class-limit-tcp-icmp</td>
<td>This firewall filter performs two functions:</td>
</tr>
<tr>
<td></td>
<td>• Assigns priority queueing to packets with a source MAC address that matches the phone MAC addresses. The forwarding class expedited-forwarding provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service for all voice-vlan traffic.</td>
</tr>
<tr>
<td></td>
<td>• Performs rate limiting on packets that enter the ports for employee-vlan. The traffic rate for TCP and ICMP packets is limited to 1 Mbps with a burst size up to 30,000 bytes.</td>
</tr>
<tr>
<td>This firewall filter is applied to port interfaces on the access switch.</td>
<td></td>
</tr>
<tr>
<td>VLAN firewall filter, ingress-vlan-rogue-block</td>
<td>Prevents rogue devices from using HTTP sessions to mimic the gatekeeper device that manages call registration, admission, and call status for VoIP calls. Only TCP or UDP ports should be used; and only the gatekeeper uses HTTP. That is, all voice-vlan traffic on TCP ports should be destined for the gatekeeper device. This firewall filter applies to all phones on voice-vlan, including communication between any two phones on the VLAN and all communication between the gatekeeper device and VLAN phones.</td>
</tr>
<tr>
<td>This firewall filter is applied to VLAN interfaces on the access switch.</td>
<td></td>
</tr>
</tbody>
</table>
Table 518: Configuration Components: Firewall Filters (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN firewall filter, egress-vlan-watch-employee</td>
<td>Accepts <strong>employee-vlan</strong> traffic destined for the corporate subnet, but does not monitor this traffic. Employee traffic destined for the Web is counted and analyzed.</td>
</tr>
<tr>
<td></td>
<td>This firewall filter is applied to vlan interfaces on the access switch.</td>
</tr>
<tr>
<td>VLAN firewall filter, ingress-vlan-limit-guest</td>
<td>Prevents guests (non-employees) from talking with employees or employee hosts on <strong>employee-vlan</strong>. Also prevents guests from using peer-to-peer applications on <strong>guest-vlan</strong>, but allows guests to access the Web.</td>
</tr>
<tr>
<td></td>
<td>This firewall filter is applied to VLAN interfaces on the access switch.</td>
</tr>
<tr>
<td>Router firewall filter, egress-router-corp-class</td>
<td>Prioritizes <strong>employee-vlan</strong> traffic, giving highest forwarding-class priority to employee traffic destined for the corporate subnet.</td>
</tr>
<tr>
<td></td>
<td>This firewall filter is applied to a routed port (Layer 3 uplink module) on the distribution switch.</td>
</tr>
</tbody>
</table>

Figure 61 on page 4163 shows the application of port, VLAN, and Layer 3 routed firewall filters on the switch.

Figure 61: Application of Port, VLAN, and Layer 3 Routed Firewall Filters
Network Topology

The topology for this configuration example consists of one EX-3200-48T switch at the access layer, and one EX-3200-48T switch at the distribution layer. The distribution switch’s uplink module is configured to support a Layer 3 connection to a J-series router.

The EX Series switches are configured to support VLAN membership. Table 519 on page 4164 shows the VLAN configuration components for the VLANs.

Table 519: Configuration Components: VLANs

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>VLAN ID</th>
<th>VLAN Subnet and Available IP Addresses</th>
<th>VLAN Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice-vlan</td>
<td>10</td>
<td>192.0.2.0/28 192.0.2.1 through 192.0.2.14</td>
<td>Voice VLAN used for employee VoIP traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.0.2.15 is subnet’s broadcast address</td>
<td></td>
</tr>
<tr>
<td>employee-vlan</td>
<td>20</td>
<td>192.0.2.16/28 192.0.2.17 through 192.0.2.30 192.0.2.31 is subnet’s broadcast address</td>
<td>VLAN standalone PCs, PCs connected to the network through the hub in VoIP telephones, wireless access points, and printers. This VLAN completely includes the voice VLAN. Two VLANs (voice-vlan and employee-vlan) must be configured on the ports that connect to the telephones.</td>
</tr>
<tr>
<td>guest-vlan</td>
<td>30</td>
<td>192.0.2.32/28 192.0.2.33 through 192.0.2.46 192.0.2.47 is subnet’s broadcast address</td>
<td>VLAN for guests’ data devices (PCs). The scenario assumes that the corporation has an area open to visitors, either in the lobby or in a conference room, that has a hub to which visitors can plug in their PCs to connect to the Web and to their company’s VPN.</td>
</tr>
<tr>
<td>camera-vlan</td>
<td>40</td>
<td>192.0.2.48/28 192.0.2.49 through 192.0.2.62 192.0.2.63 is subnet’s broadcast address</td>
<td>VLAN for the corporate security cameras.</td>
</tr>
</tbody>
</table>

Ports on the EX Series switches support Power over Ethernet (PoE) to provide both network connectivity and power for VoIP telephones connecting to the ports. Table 520 on page 4165 shows the switch ports that are assigned to the VLANs and the IP and MAC addresses for devices connected to the switch ports.
Table 520: Configuration Components: Switch Ports on a 48-Port All-PoE Switch

<table>
<thead>
<tr>
<th>Switch and Port Number</th>
<th>VLAN Membership</th>
<th>IP and MAC Addresses</th>
<th>Port Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0, ge-0/0/1</td>
<td>voice-vlan, employee-vlan</td>
<td>IP addresses: 192.0.2.1 through 192.0.2.2</td>
<td>Two VoIP telephones, each connected to one PC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC addresses: 00.05.85.00.00.01, 00.05.85.00–00.02</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/2, ge-0/0/3</td>
<td>employee-vlan</td>
<td>192.0.2.17 through 192.0.2.18</td>
<td>Printer, wireless access points</td>
</tr>
<tr>
<td>ge-0/0/4, ge-0/0/5</td>
<td>guest-vlan</td>
<td>192.0.2.34 through 192.0.2.35</td>
<td>Two hubs into which visitors can plug in their PCs. Hubs are located in an area open to visitors, such as a lobby or conference room</td>
</tr>
<tr>
<td>ge-0/0/6, ge-0/0/7</td>
<td>camera-vlan</td>
<td>192.0.2.49 through 192.0.2.50</td>
<td>Two security cameras</td>
</tr>
<tr>
<td>ge-0/0/9</td>
<td>voice-vlan</td>
<td>IP address: 192.0.2.14</td>
<td>Gatekeeper device. The gatekeeper manages call registration, admission, and call status for VoIP phones.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MAC address: 00.05.85.00.00.0E</td>
<td></td>
</tr>
<tr>
<td>ge-0/1/0</td>
<td></td>
<td>IP address: 192.0.2.65</td>
<td>Layer 3 connection to a router; note that this is a port on the switch’s uplink module</td>
</tr>
</tbody>
</table>

Configuring an Ingress Port Firewall Filter to Prioritize Voice Traffic and Rate-Limit TCP and ICMP Traffic

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

**CLI Quick Configuration**

To quickly configure and apply a port firewall filter to prioritize voice traffic and rate-limit packets that are destined for the employee-vlan subnet, copy the following commands and paste them into the switch terminal window:

```bash
[edit]
set firewall policer tcp-connection-policer if-exceeding burst-size-limit 30k bandwidth-limit 1m
set firewall policer tcp-connection-policer then discard
set firewall policer icmp-connection-policer if-exceeding burst-size-limit 30k bandwidth-limit 1m
set firewall policer icmp-connection-policer then discard
set firewall family ethernet-switching filter ingress-port-voip-class-limit tcp-icmp term voip-high from source-mac-address 00.05.85.00.00.01
set firewall family ethernet-switching filter ingress-port-voip-class-limit tcp-icmp term voip-high from source-mac-address 00.05.85.00.00.02
set firewall family ethernet-switching filter ingress-port-voip-class-limit tcp-icmp term voip-high from protocol udp
set firewall family ethernet-switching filter ingress-port-voip-class-limit tcp-icmp term voip-high then forwarding-class expedited-forwarding
set firewall family ethernet-switching filter ingress-port-voip-class-limit tcp-icmp term voip-high then loss-priority low
```

Copyright © 2013, Juniper Networks, Inc.
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term network-control from precedence net-control
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term network-control then forwarding-class network-control
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term network-control then loss-priority low
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term tcp-connection from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term tcp-connection from protocol tcp
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term tcp-connection then policer tcp-connection-policer
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term tcp-connection then count tcp-counter
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term tcp-connection then forwarding-class best-effort
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term tcp-connection then loss-priority high
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term icmp-connection from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term icmp-connection from protocol icmp
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term icmp-connection then policer icmp-connection-policer
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term icmp-connection then count icmp-counter
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term icmp-connection then forwarding-class best-effort
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term icmp-connection then loss-priority high
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term best-effort then forwarding-class best-effort
set firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp term best-effort then loss-priority high
set interfaces ge-0/0/0 description "voice priority and tcp and icmp traffic rate-limiting filter at ingress port"
set interfaces ge-0/0/0/0 family ethernet-switching filter input ingress-port-voip-class-limit-tcp-icmp
set interfaces ge-0/0/1 description "voice priority and tcp and icmp traffic rate-limiting filter at ingress port"
set interfaces ge-0/0/1/0 family ethernet-switching filter input ingress-port-voip-class-limit-tcp-icmp
set class-of-service schedulers voice-high buffer-size percent 15
set class-of-service schedulers voice-high priority high
set class-of-service schedulers net-control buffer-size percent 10
set class-of-service schedulers net-control priority high
set class-of-service schedulers best-effort buffer-size percent 75
set class-of-service schedulers best-effort priority low
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class expedited-forwarding scheduler voice-high
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class network-control scheduler net-control
set class-of-service scheduler-maps ethernet-diffsrv-cos-map forwarding-class best-effort scheduler best-effort
Step-by-Step Procedure

To configure and apply a port firewall filter to prioritize voice traffic and rate-limit packets that are destined for the employee-vlan subnet:

1. Define the policers tcp-connection-policer and icmp-connection-policer:

   ```
   [edit]
   user@switch# set firewall policer tcp-connection-policer if-exceeding burst-size-limit 30k bandwidth-limit 1m
   user@switch# set firewall policer tcp-connection-policer then discard
   user@switch# set firewall policer icmp-connection-policer if-exceeding burst-size-limit 30k bandwidth-limit 1m
   user@switch# set firewall policer icmp-connection-policer then discard
   ```

2. Define the firewall filter ingress-port-voip-class-limit-tcp-icmp:

   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp
   ```

3. Define the term voip-high:

   ```
   [edit firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp ]
   user@switch# set term voip-high from source-mac-address 00.05.85.00.00.01
   user@switch# set term voip-high from source-mac-address 00.05.85.00.00.02
   user@switch# set term voip-high from protocol udp
   user@switch# set term voip-high then forwarding-class expedited-forwarding
   user@switch# set term voip-high then loss-priority low
   ```

4. Define the term network-control:

   ```
   [edit firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp ]
   user@switch# set term network-control from precedence net-control
   user@switch# set term network-control then forwarding-class network-control
   user@switch# set term network-control then loss-priority low
   ```

5. Define the term tcp-connection to configure rate limits for TCP traffic:

   ```
   [edit firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp ]
   user@switch# set term tcp-connection from destination-address 192.0.2.16/28
   user@switch# set term tcp-connection from protocol tcp
   user@switch# set term tcp-connection then policer tcp-connection-policer
   user@switch# set term tcp-connection then count tcp-counter
   user@switch# set term tcp-connection then forwarding-class best-effort
   user@switch# set term tcp-connection then loss-priority high
   ```

6. Define the term icmp-connection to configure rate limits for ICMP traffic:

   ```
   [edit firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp ]
   user@switch# set term icmp-connection from destination-address 192.0.2.16/28
   user@switch# set term icmp-connection from protocol icmp
   user@switch# set term icmp-connection then policer icmp-policer
   user@switch# set term icmp-connection then count icmp-counter
   user@switch# set term icmp-connection then forwarding-class best-effort
   user@switch# set term icmp-connection then loss-priority high
   ```

7. Define the term best-effort with no match conditions for an implicit match on all packets that did not match any other term in the firewall filter:

   ```
   [edit firewall family ethernet-switching filter ingress-port-voip-class-limit-tcp-icmp ]
   user@switch# set term best-effort then forwarding-class best-effort
   user@switch# set term best-effort then loss-priority high
   ```
8. Apply the firewall filter `ingress-port-voip-class-limit-tcp-icmp` as an input filter to the port interfaces for `employee-vlan`:

   ```
   [edit interfaces]
   user@switch# set ge-0/0/0 description "voice priority and tcp and icmp traffic rate-limiting filter at ingress port"
   user@switch# set ge-0/0/0 unit 0 family ethernet-switching filter input ingress-port-voip-class-limit-tcp-icmp
   user@switch# set ge-0/0/1 description "voice priority and tcp and icmp traffic rate-limiting filter at ingress port"
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input ingress-port-voip-class-limit-tcp-icmp
   ```

9. Configure the parameters that are desired for the different schedulers.

   ```
   NOTE: When you configure parameters for the schedulers, define the numbers to match your network traffic patterns.
   ```

10. Assign the forwarding classes to schedulers with a scheduler map:

    ```
    [edit class-of-service]
    user@switch# set scheduler-maps ethernet-diffsrv-cos-map
    user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class expedited-forwarding scheduler voice-high
    user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class network-control scheduler network-control
    user@switch# set scheduler-maps ethernet-diffsrv-cos-map forwarding-class best-effort scheduler best-effort
    ```

11. Associate the scheduler map with the outgoing interface:

    ```
    [edit class-of-service]
    user@switch# set interfaces ge–0/1/0 scheduler-map ethernet-diffsrv-cos-map
    ```

**Results** Display the results of the configuration:

```python
user@switch# show firewall {
  policer tcp-connection-policer {
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 30k;
    }
    then {
      discard;
    }
  }
  policer icmp-connection-policer {
    if-exceeding {
      bandwidth-limit 1m;
    }
  }
}
```
burst-size-limit 30K;
}
then {
discard;
}
}
family ethernet-switching {
filter ingress-port-voip-class-limit-tcp-icmp {
term voip-high {
  from {
    destination-mac-address 00.05.85.00.00.01;
    destination-mac-address 00.05.85.00.00.02;
    protocol udp;
  }
  then {
    forwarding-class expedited-forwarding;
    loss-priority low;
  }
}
term network-control {
  from {
    precedence net-control;
  }
  then {
    forwarding-class network-control;
    loss-priority low;
  }
}
term tcp-connection {
  from {
    destination-address 192.0.2.16/28;
    protocol tcp;
  }
  then {
    policer tcp-connection-policer;
    count tcp-counter;
    forwarding-class best-effort;
    loss-priority high;
  }
}
term icmp-connection {
  from {
    protocol icmp;
  }
  then {
    policer icmp-connection-policer;
    count icmp-counter;
    forwarding-class best-effort;
    loss-priority high;
  }
}
term best-effort {
  then {
    forwarding-class best-effort;
    loss-priority high;
  }
}
### CLI Quick Configuration

To quickly configure a VLAN firewall filter on voice-vlan to prevent rogue devices from using HTTP sessions to mimic the gatekeeper device that manages VoIP traffic, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family ethernet-switching filter ingress-vlan-rogue-block term to-gatekeeper from
destination-address 192.0.2.14
set firewall family ethernet-switching filter ingress-vlan-rogue-block term to-gatekeeper from
destination-port 80
set firewall family ethernet-switching filter ingress-vlan-rogue-block term to-gatekeeper then
accept
```

---

**Configuring a VLAN Ingress Firewall Filter to Prevent Rogue Devices from Disrupting VoIP Traffic**

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:
**Step-by-Step Procedure**

To configure and apply a VLAN firewall filter on **voice-vlan** to prevent rogue devices from using HTTP to mimic the gatekeeper device that manages VoIP traffic:

1. Define the firewall filter **ingress-vlan-rogue-block** to specify filter matching on the traffic you want to permit and restrict:
   
   ```
   [edit firewall]
   user@switch# set family ethernet-switching filter ingress-vlan-rogue-block
   ```

2. Define the term **to-gatekeeper** to accept packets that match the destination IP address of the gatekeeper:
   
   ```
   [edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
   user@switch# set term to-gatekeeper from destination-address 192.0.2.14
   user@switch# set term to-gatekeeper from destination-port 80
   user@switch# set term to-gatekeeper then accept
   ```

3. Define the term **from-gatekeeper** to accept packets that match the source IP address of the gatekeeper:
   
   ```
   [edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
   user@switch# set term from-gatekeeper from source-address 192.0.2.14
   user@switch# set term from-gatekeeper from source-port 80
   user@switch# set term from-gatekeeper then accept
   ```

4. Define the term **not-gatekeeper** to ensure all **voice-vlan** traffic on TCP ports is destined for the gatekeeper device:

   ```
   [edit firewall family ethernet-switching filter ingress-vlan-rogue-block]
   user@switch# set term not-gatekeeper from destination-port 80
   user@switch# set term not-gatekeeper then count rogue-counter
   user@switch# set term not-gatekeeper then discard
   ```

5. Apply the firewall filter **ingress-vlan-rogue-block** as an input filter to the VLAN interface for the VoIP telephones:

   ```
   [edit]
   user@switch# set vlans voice-vlan description "block rogue devices on voice-vlan"
   user@switch# set vlans voice-vlan filter input ingress-vlan-rogue-block
   ```

**Results**

Display the results of the configuration:

```
user@switch# show
firewall {
    family ethernet-switching {
        filter ingress-vlan-rogue-block {
            term to-gatekeeper {
                from {
```
destination-address 192.0.2.14/32
destination-port 80;
}
then {
accept;
}
}
term from-gatekeeper {
from {
source-address 192.0.2.14/32
source-port 80;
}
then {
accept;
}
}
term not-gatekeeper {
from {
destination-port 80;
}
then {
count rogue-counter;
discard;
}
}
}
vlans {
voice-vlan {
description "block rogue devices on voice-vlan";
filter {
input ingress-vlan-rogue-block;
}
}
}

Configuring a VLAN Firewall Filter to Count, Monitor, and Analyze Egress Traffic on the Employee VLAN

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

A firewall filter is configured and applied to VLAN interfaces to filter employee-vlan egress traffic. Employee traffic destined for the corporate subnet is accepted but not monitored. Employee traffic destined for the Web is counted and analyzed.

To quickly configure and apply a VLAN firewall filter, copy the following commands and paste them into the switch terminal window:

[edit]
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-corp
from destination-address 192.0.2.16/28
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-corp
then accept
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-web
from destination-port 80
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-web then count employee-web-counter
set firewall family ethernet-switching filter egress-vlan-watch-employee term employee-to-web then analyzer employee-monitor
set vlans employee-vlan description "filter at egress VLAN to count and analyze employee to Web traffic"
set vlans employee-vlan filter output egress-vlan-watch-employee

Step-by-Step Procedure

To configure and apply an egress port firewall filter to count and analyze employee-vlan traffic that is destined for the Web:

1. Define the firewall filter egress-vlan-watch-employee:

   [edit firewall]
   user@switch# set family ethernet-switching filter egress-vlan-watch-employee

2. Define the term employee-to-corp to accept but not monitor all employee-vlan traffic destined for the corporate subnet:

   [edit firewall family ethernet-switching filter egress-vlan-watch-employee]
   user@switch# set term employee-to-corp from destination-address 192.0.2.16/28
   user@switch# set term employee-to-corp then accept

3. Define the term employee-to-web to count and monitor all employee-vlan traffic destined for the Web:

   [edit firewall family ethernet-switching filter egress-vlan-watch-employee]
   user@switch# set term employee-to-web from destination-port 80
   user@switch# set term employee-to-web then count employee-web-counter
   user@switch# set term employee-to-web then analyzer employee-monitor

   NOTE: See Example: Configuring Port Mirroring for Local Monitoring of Employee Resource Use on EX Series Switches for information about configuring the employee-monitor analyzer.

4. Apply the firewall filter egress-vlan-watch-employee as an output filter to the port interfaces for the VoIP telephones:

   [edit]
   user@switch# set vlans employee-vlan description "filter at egress VLAN to count and analyze employee to Web traffic"
   user@switch# set vlans employee-vlan filter output egress-vlan-watch-employee

Results

Display the results of the configuration:

user@switch# show
firewall {
  family ethernet-switching {
    filter egress-vlan-watch-employee {
      term employee-to-corp {
        from {
          destination-address 192.0.2.16/28
        }
        then {
          accept;
        }
      }
    }
  }
}
term employee-to-web {
    from {
        destination-port 80;
    }
    then {
        count employee-web-counter:
        analyzer employee-monitor;
    }
}

vls {
    employee-vlan {
        description "filter at egress VLAN to count and analyze employee to Web traffic";
        filter {
            output egress-vlan-watch-employee;
        }
    }
}

Configuring a VLAN Firewall Filter to Restrict Guest-to-Employee Traffic and Peer-to-Peer Applications on the Guest VLAN

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

CLI Quick Configuration

In the following example, the first filter term permits guests to talk with other guests but not employees on employee-vlan. The second filter term allows guests Web access but prevents them from using peer-to-peer applications on guest-vlan.

To quickly configure a VLAN firewall filter to restrict guest-to-employee traffic, blocking guests from talking with employees or employee hosts on employee-vlan or attempting to use peer-to-peer applications on guest-vlan, copy the following commands and paste them into the switch terminal window:

[edit]
set firewall family ethernet-switching filter ingress-vlan-limit-guest term guest-to-guest from destination-address 192.0.2.33/28
set firewall family ethernet-switching filter ingress-vlan-limit-guest term guest-to-guest then accept
set firewall family ethernet-switching filter ingress-vlan-limit-guest term no-guest-employee-no-peer-to-peer from destination-mac-address 00.05.85.00.00.DF
set firewall family ethernet-switching filter ingress-vlan-limit-guest term no-guest-employee-no-peer-to-peer then accept
set vlans guest-vlan description "restrict guest-to-employee traffic and peer-to-peer applications on guest VLAN"
set vlans guest-vlan filter input ingress-vlan-limit-guest
To configure and apply a VLAN firewall filter to restrict guest-to-employee traffic and peer-to-peer applications on guest-vlan:

1. Define the firewall filter ingress-vlan-limit-guest:
   ```
   [edit firewall]
   set firewall family ethernet-switching filter ingress-vlan-limit-guest
   ``

2. Define the term guest-to-guest to permit guests on the guest-vlan to talk with other guests but not employees on the employee-vlan:
   ```
   [edit firewall family ethernet-switching filter ingress-vlan-limit-guest]
   user@switch# set term guest-to-guest from destination-address 192.0.2.33/28
   user@switch# set term guest-to-guest then accept
   ``

3. Define the term no-guest-employee-no-peer-to-peer to allow guests on guest-vlan Web access but prevent them from using peer-to-peer applications on the guest-vlan.
   ```
   [edit firewall family ethernet-switching filter ingress-vlan-limit-guest]
   user@switch# set term no-guest-employee-no-peer-to-peer from destination-mac-address 00.05.85.00.00.DF
   user@switch# set term no-guest-employee-no-peer-to-peer then accept
   ``

4. Apply the firewall filter ingress-vlan-limit-guest as an input filter to the interface for guest-vlan:
   ```
   [edit]
   user@switch# set vlans guest-vlan description "restrict guest-to-employee traffic and peer-to-peer applications on guest VLAN"
   user@switch# set vlans guest-vlan filter input ingress-vlan-limit-guest
   ```

Results
Display the results of the configuration:

```bash
user@switch# show
firewall {
    family ethernet-switching {
        filter ingress-vlan-limit-guest {
            term guest-to-guest {
                from {
                    destination-address 192.0.2.33/28;
                }
                then {
                    accept;
                }
            }
            term no-guest-employee-no-peer-to-peer {
                from {
                    destination-mac-address 00.05.85.00.00.DF;
                }
                then {
                    accept;
                }
            }
        }
    }
}
```
Configuring a Router Firewall Filter to Give Priority to Egress Traffic Destined for the Corporate Subnet

To configure and apply firewall filters for port, VLAN, and router interfaces, perform these tasks:

**CLI Quick Configuration**

To quickly configure a firewall filter for a routed port (Layer 3 uplink module) to filter *employee-vlan* traffic, giving highest forwarding-class priority to traffic destined for the corporate subnet, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family inet filter egress-router-corp-class term corp-expedite from destination-address 192.0.2.16/28
set firewall family inet filter egress-router-corp-class term corp-expedite then forwarding-class expedited-forwarding
set firewall family inet filter egress-router-corp-class term corp-expedite then loss-priority low
set firewall family inet filter egress-router-corp-class term not-to-corp then accept
set interfaces ge-0/1/0 unit 0 family inet address 103.104.105.1
set interfaces ge-0/1/0 unit 0 family inet filter output egress-router-corp-class
```

**Step-by-Step Procedure**

To configure and apply a firewall filter to a routed port (Layer 3 uplink module) to give highest priority to *employee-vlan* traffic destined for the corporate subnet:

1. Define the firewall filter *egress-router-corp-class*:
   
   ```
   [edit]
   user@switch# set firewall family inet filter egress-router-corp-class
   ```

2. Define the term *corp-expedite*:
   
   ```
   [edit firewall]
   user@switch# set family inet filter egress-router-corp-class term corp-expedite from destination-address 192.0.2.16/28
   ```

3. Define the term *not-to-corp*:
   
   ```
   [edit firewall]
   user@switch# set family inet filter egress-router-corp-class term not-to-corp then accept
   ```

4. Apply the firewall filter *egress-router-corp-class* as an output filter for the port on the switch's uplink module, which provides a Layer 3 connection to a router:
[edit interfaces]
user@switch# set ge-0/1/0 description "filter at egress router to expedite employee traffic destined for corporate network"
user@switch# set ge-0/1/0 unit 0 family inet address 103.104.105.1
user@switch# set ge-0/1/0 unit 0 family inet filter output egress-router-corp-class

Results
Display the results of the configuration:

user@switch# show firewall {
  family inet {
    filter egress-router-corp-class {
      term corp-expedite {
        from {
          destination-address 192.0.2.16/28;
        }
        then {
          forwarding-class expedited-forwarding;
          loss-priority low;
        }
      }
      term not-to-corp {
        then {
          accept;
        }
      }
    }
  }
}

  interfaces {
    ge-0/1/0 {
      unit 0 {
        description "filter at egress router interface to expedite employee traffic destined for corporate network";
        family inet {
          source-address 103.104.105.1
          filter {
            output egress-router-corp-class;
          }
        }
      }
    }
  }
}

Verification
To confirm that the firewall filters are working properly, perform the following tasks:

- Verifying that Firewall Filters and Policers are Operational on page 4177
- Verifying that Schedulers and Scheduler-Maps are Operational on page 4178

Purpose
Verify the operational state of the firewall filters and policers that are configured on the switch.
**Action**  Use the operational mode command:

```bash
user@switch> show firewall
```

Filter: ingress-port-voip-class-limit-tcp-icmp

Counters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-counter</td>
<td>0</td>
</tr>
<tr>
<td>tcp-counter</td>
<td>0</td>
</tr>
</tbody>
</table>

Policers:

<table>
<thead>
<tr>
<th>Name</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-connection-policer</td>
<td>0</td>
</tr>
<tr>
<td>tcp-connection-policer</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter: ingress-vlan-rogue-block

Filter: egress-vlan-watch-employee

Counters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>employee-web-counter</td>
<td>0</td>
</tr>
</tbody>
</table>

**Meaning**  The `show firewall` command displays the names of the firewall filters, policers, and counters that are configured on the switch. The output fields show byte and packet counts for all configured counters and the packet count for all policers.

**Verifying that Schedulers and Scheduler-Maps are Operational**

**Purpose**  Verify that schedulers and scheduler-maps are operational on the switch.

**Action**  Use the operational mode command:

```bash
user@switch> show class-of-service scheduler-map
```

Scheduler map: default, Index: 2

Scheduler: default-be, Forwarding class: best-effort, Index: 20
Transmit rate: 95 percent, Rate Limit: none, Buffer size: 95 percent,
Priority: low

Drop profiles:

<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>non-TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
<tr>
<td>Low</td>
<td>TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
</tbody>
</table>

Scheduler: default-nc, Forwarding class: network-control, Index: 22
Transmit rate: 5 percent, Rate Limit: none, Buffer size: 5 percent,
Priority: low

Drop profiles:

<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>non-TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
<tr>
<td>Low</td>
<td>TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>default-drop-profile</td>
</tr>
</tbody>
</table>

Scheduler: ethernet-diffsrv-cos-map, Index: 21657

Scheduler: best-effort, Forwarding class: best-effort, Index: 61257
Transmit rate: remainder, Rate Limit: none, Buffer size: 75 percent,
Priority: low

Drop profiles:
<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>Low</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
</tbody>
</table>

Scheduler: voice-high, Forwarding class: expedited-forwarding, Index: 3123
Transmit rate: remainder, Rate Limit: none, Buffer size: 15 percent, Priority: high
Drop profiles:
<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>Low</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
</tbody>
</table>

Scheduler: net-control, Forwarding class: network-control, Index: 2451
Transmit rate: remainder, Rate Limit: none, Buffer size: 10 percent, Priority: high
Drop profiles:
<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>Low</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>non-TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
<tr>
<td>High</td>
<td>TCP</td>
<td>1</td>
<td>&lt;default-drop-profile&gt;</td>
</tr>
</tbody>
</table>

Meaning Displays statistics about the configured schedulers and schedulers-maps.

Related Documentation
- Example: Configuring Port Mirroring for Remote Monitoring of Employee Resource Use on EX Series Switches
- Example: Configuring CoS on EX Series Switches on page 1895
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- [edit firewall] Configuration Statement Hierarchy on EX Series Switches on page 4217

Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch

You can configure a firewall filter on a management interface on an EX Series switch to filter ingress or egress traffic on the management interface on the switch. You can use utilities such as SSH or Telnet to connect to the management interface over the network and then use management protocols such as SNMP to gather statistical data from the switch.

This example discusses how to configure a firewall filter on a management interface to filter SSH packets egressing from an EX Series switch:

- Requirements on page 4180
- Overview and Topology on page 4180
Requirements

This example uses the following hardware and software components:

- One EX Series switch and one management PC
- Junos OS Release 10.4 or later for EX Series switches

Overview and Topology

In this example, a management PC establishes an SSH connection with the management interface on a switch to remotely manage the switch. The IP address configured for the management interface is 10.204.33.103/20. A firewall filter is configured on the management interface to count the number of packets egressing from a source SSH port on the management interface. When the management PC establishes the SSH session with the management interface, the management interface returns SSH packets to the management PC to confirm that the session is established. These SSH packets are filtered based on the match condition specified in the firewall filter before they are forwarded to the management PC. As these packets are generated from the source SSH port on the management interface, they fulfill the match condition specified for the management interface. The number of matched SSH packets provides a count of the number of packets that have traversed the management interface. A system administrator can use this information to monitor the management traffic and take any action if required.

Figure 62 on page 4180 shows the topology for this example in which a management PC establishes an SSH connection with the switch.

Figure 62: SSH Connection From a Management PC to an EX Series Switch

CLI Quick Configuration

To quickly create and configure a firewall filter on the management interface to filter SSH packets egressing from the management interface, copy the following commands and paste them into the switch terminal window:

```
[edit]
set firewall family inet filter mgmt_filter term t1 from source-port ssh
set firewall family inet filter mgmt_filter term t1 then count c1
set firewall family inet filter mgmt_filter term t2 then accept
set interfaces me0 unit 0 family inet filter output mgmt_filter
```
Step-by-Step Procedure

To configure a firewall filter on the management interface to filter SSH packets:

1. Configure the firewall filter that matches SSH packets from the source port:

   [edit]
   user@switch# set firewall family inet filter (Firewall Filters) mgmt_filter term t1 from source-port ssh
   user@switch# set firewall family inet filter mgmt_filter term t1 then count c1
   user@switch# set firewall family inet filter mgmt_filter term t2 then accept

   These statements set a counter c1 to count the number of SSH packets that egress from the source SSH interface on the management interface.

2. Set the firewall filter for the management interface:

   [edit]
   user@switch# set interfaces me0 unit 0 family inet filter output mgmt_filter

   NOTE: You can also set the firewall filter for a VME interface.

Results

Check the results of the configuration:

[edit]
user@switch# show interfaces { me0 { unit 0 { family inet { filter { output mgmt_filter; } address 10.93.54.6/24; } } } }

firewall { family inet { filter mgmt_filter [ term t1 { from [ source-port ssh; then count c1; ] } term t2 { then accept; ] } ] } }
Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That the Firewall Filter Is Configured on a Management Interface on page 4182

**Verifying That the Firewall Filter Is Configured on a Management Interface**

**Purpose**
Verify that the firewall filter has been enabled on the management interface on the switch.

**Action**
1. Verify that the firewall filter is applied to the management interface:

   ```
   [edit]
   user@switch# show interfaces me0
   unit 0 {
     family inet {
       filter {
         output mgmt_fil1;
       }
       address 10.204.33.103/20;
     }
   }
   ``

2. Check the counter value that is associated with the firewall filter:

   ```
   user@switch> show firewall
   Filter: mgmt_fil1
   Counters:
   Name      Bytes    Packets
   c1        0         0
   ```

3. From the management PC, establish a secure shell session with the switch:

   ```
   [user@management-pc ~]$ ssh user@10.204.33.103
   ```

4. Check counter values after SSH packets are generated from the switch in response to the secure shell session request by the management PC:

   ```
   user@switch> show firewall
   Filter: mgmt_fil1
   Counters:
   Name      Bytes    Packets
   c1        3533      23
   ```

**Meaning**
The output indicates that the firewall filter has been applied to the management interface and the counter value indicates that 23 SSH packets were generated from the switch.

**Related Documentation**
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches

Administrators can configure filter-based forwarding on an EX Series switch by using a firewall filter to forward matched traffic to a specific virtual routing instance. This example describes how to set up filter-based forwarding:

- Requirements on page 4183
- Overview and Topology on page 4183
- Configuration on page 4183
- Verification on page 4185

Requirements

This example uses the following software and hardware components:

- One EX Series switch
- Junos OS Release 9.4 or later for EX Series switches

Overview and Topology

In this example, traffic from one application server that is destined for a different application server is matched by a firewall filter based on the IP address. Any matching packets are routed to a particular virtual routing instance that first sends all traffic to a security device, then forwards it to the designated destination address.

Configuration

To configure filter-based forwarding:

1. Create interfaces to the application servers:

```
user@switch# set interfaces ge-0/0/0 unit 0 family inet address 10.1.0.1/24
user@switch# set interfaces ge-0/0/3 unit 0 family inet address 10.1.3.1/24
```

2. Create a firewall filter that matches the correct source address:

```
set firewall family inet filter fil term t1 from source-address 1.1.1.1/32
set firewall family inet filter fil term t1 from protocol tcp
```

3. Configure the virtual routing instance:

```
set routing-instances vrf01 instance-type virtual-router
set routing-instances vrf01 interface ge-0/0/1.0
set routing-instances vrf01 interface ge-0/0/3.0
set routing-instances vrf01 routing-options static route 12.34.56.0/24 next-hop 10.1.3.254
set firewall family inet filter fil term t1 then routing-instance vrf01
```
3. Associate the filter with the source application server’s interface:

```
[edit]
user@switch# set interfaces ge-0/0/0 unit 0 family inet filter input fil
```

4. Create a virtual router:

```
[edit]
user@switch# set routing-instances vrf01 instance-type virtual-router
```

5. Associate the interfaces with the virtual router:

```
[edit]
user@switch# set routing-instances vrf01 interface ge-0/0/1.0
user@switch# set routing-instances vrf01 interface ge-0/0/3.0
```

6. Configure the routing information for the virtual routing instance:

```
[edit]
user@switch# set routing-instances vrf01 routing-options static route 12.34.56.0/24 next-hop 10.1.3.254
```

7. Set the filter to forward packets to the virtual router you created:

```
[edit]
user@switch# set firewall family inet filter fil term t1 then routing-instance vrf01
```

**Results**

Check the results of the configuration:

```
user@switch> show configuration
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        filter {
          input fil;
        }
        address 10.1.0.1/24;
      }
    }
  }
  ge-0/0/3 {
    unit 0 {
      family inet {
        address 10.1.3.1/24;
      }
    }
  }
}
firewall {
  family inet {
    filter fil {
      term t1 {
        from {
          source-address {
            1.1.1.1/32;
          }
        protocol tcp;
```
then {
    routing-instance vrf01;
}
}

} routing-instances {
 vrf01 {
    instance-type virtual-router;
    interface ge-0/0/1.0;
    interface ge-0/0/3.0;
    routing-options {
        static {
            route 12.34.56.0/24 next-hop 10.1.3.254;
        }
    }
}
}

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying That Filter-Based Forwarding Was Configured on page 4185

Verifying That Filter-Based Forwarding Was Configured

**Purpose**
Verify that filter-based forwarding was properly enabled on the switch.

**Action**
1. Use the `show interfaces filters` command:

```
user@switch> show interfaces filters ge-0/0/0.0
Interface        Admin Link Proto Input Filter         Output Filter
ge-0/0/0.0       up    down inet  fil
```

2. Use the `show route forwarding-table` command:

```
user@switch> show route forwarding-table
Routing table: default.inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            user     1 0:12:f2:21:cf:0    ucst   331     4 me0.0
default            perm     0                    rjct    36     3
0.0.0.0/32         perm     0                    dscd    34     1
10.1.0.0/24        ifdn     0 10.1.0.0           rslv   611     1 ge-0/0/0.0
10.1.0.0/32        iddn     0 10.1.0.0           recv   611     1 ge-0/0/0.0
10.1.0.1/32        user     0                    rjct    36     3
10.1.0.1/32        intf     0 10.1.0.1           locl   612     2
10.1.0.1/32        iddn     0 10.1.0.1           locl   612     2
10.1.0.255/32      iddn     0 10.1.0.255         bcst   610     1 ge-0/0/0.0
10.1.1.0/26        ifdn     0 10.1.0.0           rslv   583     1 vlan.0
10.1.1.0/32        iddn     0 10.1.0.0           recv   611     1 ge-0/0/0.0
10.1.1.1/32        user     0                    rjct    36     3
10.1.1.1/32        intf     0 10.1.1.1           locl   582     2
10.1.1.1/32        iddn     0 10.1.1.1           locl   582     2
10.1.1.63/32       iddn     0 10.1.1.63          bcst   610     1 ge-0/0/0.0
```
255.255.255.255/32 perm 0 bcst 32 1

Routing table: vrf01.inet

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>559</td>
<td>2</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>0.0.0.0/32</td>
<td>perm</td>
<td>0</td>
<td>dscd</td>
<td>545</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.3.0/24</td>
<td>ifdn</td>
<td>0</td>
<td>rslv</td>
<td>617</td>
<td>1 ge-0/0/3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.3.0/32</td>
<td>iddn</td>
<td>0 10.1.3.0</td>
<td>recv</td>
<td>615</td>
<td>1 ge-0/0/3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.3.1/32</td>
<td>user</td>
<td>0</td>
<td>rjct</td>
<td>559</td>
<td>2</td>
<td>1</td>
<td>ge-0/0/3.0</td>
</tr>
<tr>
<td>10.1.3.1/32</td>
<td>intf</td>
<td>0 10.1.3.1</td>
<td>locl</td>
<td>616</td>
<td>2</td>
<td>1</td>
<td>ge-0/0/3.0</td>
</tr>
<tr>
<td>10.1.3.1/32</td>
<td>iddn</td>
<td>0 10.1.3.1</td>
<td>locl</td>
<td>616</td>
<td>2</td>
<td>1</td>
<td>ge-0/0/3.0</td>
</tr>
<tr>
<td>10.1.3.255/32</td>
<td>iddn</td>
<td>0 10.1.3.255</td>
<td>bcst</td>
<td>614</td>
<td>1 ge-0/0/3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>perm</td>
<td>0</td>
<td>mdsc</td>
<td>546</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>224.0.0.1/32</td>
<td>perm</td>
<td>0 224.0.0.1</td>
<td>mcst</td>
<td>529</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>255.255.255.255/32</td>
<td>perm</td>
<td>0</td>
<td>bcst</td>
<td>543</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Routing table: default.iso

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>60</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Routing table: vrf01.iso

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type</th>
<th>RtRef</th>
<th>Next hop</th>
<th>Type</th>
<th>Index</th>
<th>NhRef</th>
<th>Netif</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>perm</td>
<td>0</td>
<td>rjct</td>
<td>600</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

### Meaning

The output indicates that the filter was created on the interface and that the virtual routing instance is forwarding matching traffic to the correct IP address.

### Related Documentation

- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Static Routing (CLI Procedure) on page 3024
- Configuring Static Routing (J-Web Procedure) on page 3024
- Understanding Filter-Based Forwarding for EX Series Switches on page 4158

### Example: Applying Firewall Filters to Multiple Supplicants on Interfaces Enabled for 802.1X or MAC RADIUS Authentication

On EX Series switches, firewall filters that you apply to interfaces enabled for 802.1X or MAC RADIUS authentication are dynamically combined with the per-user policies sent to the switch from the RADIUS server. The switch uses internal logic to dynamically combine the interface firewall filter with the user policies from the RADIUS server and create an individualized policy for each of the multiple users or nonresponsive hosts that are authenticated on the interface.

This example describes how dynamic firewall filters are created for multiple supplicants on an 802.1X-enabled interface (the same principles shown in this example apply to interfaces enabled for MAC RADIUS authentication):

- Requirements on page 4187
- Overview and Topology on page 4187
Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.5 or later for EX Series switches
- One EX Series switch
- One RADIUS authentication server. The authentication server acts as the backend database and contains credential information for hosts (supplicants) that have permission to connect to the network.

Before you apply firewall filters to an interface for use with multiple supplicants, be sure you have:

- Set up a connection between the switch and the RADIUS server. See “Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch” on page 1675.
- Configured 802.1X authentication on the switch, with the authentication mode for interface ge-0/0/2 set to multiple. See “Configuring 802.1X Interface Settings (CLI Procedure)” on page 1740 and “Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX Series Switch” on page 1684.
- Configured users on the RADIUS authentication server.

Overview and Topology

When the 802.1X configuration on an interface is set to multiple supplicant mode, the system dynamically combines interface firewall filter with the user policies sent to the switch from the RADIUS server during authentication and creates separate terms for each user. Because there are separate terms for each user authenticated on the interface, you can, as shown in this example, use counters to view the activities of individual users that are authenticated on the same interface.

When a new user (or a nonresponsive host) is authenticated on an interface, the system adds a term to the firewall filter associated with the interface, and the term (policy) for each user is associated with the MAC address of the user. The term for each user is based on the user-specific filters set on the RADIUS server and the filters configured on the interface. For example, as shown in Figure 18 on page 1727, when User1 is authenticated by the EX Series switch, the system creates the firewall filter `dynamic-filter-example`. When User2 is authenticated, another term is added to the firewall filter, and so on.
This is a conceptual model of the internal process—you cannot access or view the dynamic filter.

**NOTE:** If the firewall filter on the interface is modified after the user (or nonresponsive host) is authenticated, the modifications are not reflected in the dynamic filter unless the user is reauthenticated.

In this example, you configure a firewall filter to count the requests made by each endpoint authenticated on interface `ge-0/0/2` to the file server, which is located on subnet `192.0.2.16/28`, and set policer definitions to rate limit the traffic. Figure 19 on page 1728 shows the network topology for this example.
Figure 64: Multiple Supplicants on an 802.1X-Enabled Interface Connecting to a File Server

Configuration

To configure firewall filters for multiple supplicants on 802.1X-enabled interfaces:

- Configuring Firewall Filters on Interfaces with Multiple Supplicants on page 4189

**Configuring Firewall Filters on Interfaces with Multiple Supplicants**

**CLI Quick Configuration**

To quickly configure firewall filters for multiple supplicants on an 802.1X-enabled interface copy the following commands and paste them into the switch terminal window:

```
[edit]
set protocols dot1x authenticator interface ge-0/0/2 supplicant multiple
set firewall family ethernet-switching filter filter1 term term1 from destination-address 192.0.2.16/28
set firewall policer p1 if-exceeding bandwidth-limit 1m
set firewall policer p1 if-exceeding burst-size-limit 1k
set firewall family ethernet-switching filter filter1 term term1 then count counter1
set firewall family ethernet-switching filter filter1 term term2 then policer p1
```

**Step-by-Step Procedure**

To configure firewall filters on an interface enabled for multiple supplicants:

1. Configure interface `ge-0/0/2` for multiple supplicant mode authentication:

   ```
   [edit protocols dot1x]
   user@switch# set authenticator interface ge-0/0/2 supplicant multiple
   ```

2. Set policer definition:
3. Configure a firewall filter to count packets from each user and a policer that limits the traffic rate. As each new user is authenticated on the multiple supplicant interface, this filter term will be included in the dynamically created term for the user:

```
[edit firewall family ethernet-switching]
user@switch# set filter filter1 term term1 from destination-address 192.0.2.16/28
user@switch# set filter filter1 term term1 then count counter1
user@switch# set filter filter1 term term2 then policer p1
```

**Results**  
Check the results of the configuration:

```
user@switch> show configuration

firewall {
    family ethernet-switching {
        filter filter1 {
            term term1 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then count counter1;
            }
            term term2 {
                from {
                    destination-address {
                        192.0.2.16/28;
                    }
                }
                then policer p1;
            }
        }
    }
    policer p1 {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 1k;
        }
        then discard;
    }
}
protocols {
    dot1x {
        authenticator
        interface ge-0/0/2 {
            supplicant multiple;
        }
    }
}
```
Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying Firewall Filters on Interfaces with Multiple Supplicants on page 4191

**Verifying Firewall Filters on Interfaces with Multiple Supplicants**

**Purpose**
Verify that firewall filters are functioning on the interface with multiple supplicants.

**Action**

1. Check the results with one user authenticated on the interface. In this case, the user is authenticated on **ge-0/0/2**:

```shell
user@switch> show dot1x firewall
Filter: dot1x_ge-0/0/2
Counters
counter1_dot1x_ge-0/0/2_user1 100
```

2. When a second user, User2, is authenticated on the same interface, **ge-0/0/2**, you can verify that the filter includes the results for both of the users authenticated on the interface:

```shell
user@switch> show dot1x firewall
Filter: dot1x-filter-ge-0/0/0
Counters
counter1_dot1x_ge-0/0/2_user1 100
counter1_dot1x_ge-0/0/2_user2 400
```

**Meaning**
The results displayed by the `show dot1x firewall` command output reflect the dynamic filter created with the authentication of each new user. User1 accessed the file server located at the specified destination address 100 times, while User2 accessed the same file server 400 times.

**Related Documentation**

- Example: Applying a Firewall Filter to 802.1X-Authenticated Supplicants Using RADIUS Server Attributes on an EX Series Switch on page 1719
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Filtering 802.1X Supplicants Using RADIUS Server Attributes on page 1742

**Configuration Tasks**

- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Assigning Multifield Classifiers in Firewall Filters to Specify Packet-Forwarding Behavior (CLI Procedure) on page 4209
- Configuring Routing Policies (J-Web Procedure) on page 4210
- Configuring Tricolor Marking Policers on page 4215
You configure firewall filters on EX Series switches to control traffic that enters ports on the switch or enters and exits VLANs on the network and Layer 3 (routed) interfaces. To configure a firewall filter you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

This topic describes:

- Configuring a Firewall Filter on page 4192
- Configuring a Term Specifically for IPv4 or IPv6 Traffic on page 4196
- Applying a Firewall Filter to a Port on a Switch on page 4197
- Applying a Firewall Filter to a Management Interface on a Switch on page 4198
- Applying a Firewall Filter to a VLAN on a Network on page 4199
- Applying a Firewall Filter to a Layer 3 (Routed) Interface on page 4200

**Configuring a Firewall Filter**

Before you can apply a firewall filter to a port, VLAN, or Layer 3 interface, you must configure a firewall filter with the required details, such as type of family for the firewall filter, firewall filter name, and match conditions. A match condition in the firewall filter configuration can contain multiple terms that define the criteria for the match condition. For each term, you must specify an action to be performed if a packet matches the conditions in the term. For information on different match conditions and actions, see “Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 4096.

To configure a firewall filter:
1. Configure the family address type for the firewall filter:

   - For a firewall filter that is applied to a port or VLAN, specify the family address type **ethernet-switching** to filter Layer 2 (Ethernet) packets and Layer 3 (IP) packets, for example:
     
     ```
     [edit firewall]
     user@switch# set family ethernet-switching
     ```

   - For a firewall filter that is applied to a Layer 3 (routed) interface:
     
     - To filter IPv4 packets, specify the family address type **inet**, for example:
       
       ```
       [edit firewall]
       user@switch# set family inet
       ```
     
     - To filter IPv6 packets, specify the family address type **inet6**, for example:
       
       ```
       [edit firewall]
       user@switch# set family inet6
       ```

     **NOTE:** You can configure firewall filters for both IPv4 and IPv6 traffic on the same Layer 3 interface.

2. Specify the filter name:

   ```
   [edit firewall family ethernet-switching]
   user@switch# set filter ingress-port-filter
   ```

   The filter name can contain letters, numbers, and hyphens (-) and can have a maximum of 64 characters. Each filter name must be unique.

3. If you want to apply a firewall filter to multiple interfaces and name individual firewall counters specific to each interface, configure the **interface-specific** option:

   ```
   [edit firewall family ethernet-switching filter ingress-port-filter]
   user@switch# set interface-specific
   ```

4. Specify a term name:

   ```
   [edit firewall family ethernet-switching filter ingress-port-filter]
   user@switch# set term term-one
   ```

   The term name can contain letters, numbers, and hyphens (-) and can have a maximum of 64 characters.

   A firewall filter can contain one or more terms. Each term name must be unique within a filter.
The maximum number of terms allowed per firewall filter for EX Series switches is:

- 512 for EX2200 switches
- 1,436 for EX3300 switches

On EX3300 switches, if you add and delete filters with a large number of terms (on the order of 1000 or more) in the same commit operation, not all the filters are installed. You must add filters in one commit operation, and delete filters in a separate commit operation.

- 7,168 for EX3200 and EX4200 switches
- On EX4300 switches, following are the number of terms supported for ingress and egress traffic, for firewall filers configured on a port, VLAN and Layer 3 interface:
  - For ingress traffic:
    - 3,500 terms for firewall filters configured on a port
    - 3,500 terms for firewall filters configured on a VLAN
    - 7,000 terms for firewall filters configured on Layer 3 interfaces for IPv4 traffic
    - 3,500 terms for firewall filters configured on Layer 3 interfaces for IPv6 traffic
  - For egress traffic:
    - 512 terms for firewall filters configured on a port
    - 256 terms for firewall filters configured on a VLAN
    - 512 terms for firewall filters configured on Layer 3 interfaces for IPv4 traffic
    - 512 terms for firewall filters configured on Layer 3 interfaces for IPv6 traffic

You can configure these maximum number of terms only when you configure one type of firewall filter (Port, VLAN, or Router (Layer 3) firewall filter) on the switch, and when storm control is not enabled on all interfaces in the switch.

- 1,200 for EX4500 and EX4550 switches
• 1,400 for EX6200 switches
• 32,768 for EX8200 switches

If you attempt to configure a firewall filter that exceeds these limits, the switch returns an error message when you commit the configuration.

5. In each firewall filter term, specify the match conditions to use to match components of a packet.

To specify match conditions to match on packets that contain a specific source address and source port—for example:

```plaintext
[edit firewall family ethernet-switching filter ingress-port-filter term term-one]
user@switch# set from source-address 192.0.2.14
user@switch# set from source-port 80
```

You can specify one or more match conditions in a single **from** statement. For a match to occur, the packet must match all the conditions in the term.

The **from** statement is optional, but if included in a term, the **from** statement cannot be empty. If you omit the **from** statement, all packets are considered to match.

6. In each firewall filter term, specify the action to take if the packet matches all the conditions in that term.

You can specify an action and/or action modifiers:

• To specify a filter action, for example, to discard packets that match the conditions of the filter term:

  ```plaintext
  [edit firewall family ethernet-switching filter ingress-port-filter term term-one]
  user@switch# set then discard
  ```

  You can specify no more than one action per filter term.

• To specify an action modifier, for example, to count and classify packets in a forwarding class:

  ```plaintext
  [edit firewall family ethernet-switching filter ingress-port-filter term term-one]
  user@switch# set then count counter-one
  user@switch# set then forwarding-class expedited-forwarding
  ```

  In a **then** statement, you can specify the following action modifiers:

  • **analyzer analyzer-name**—Mirror port traffic to a specified destination port or VLAN that is connected to a protocol analyzer application. An **analyzer** must be configured under the **ethernet-switching** family address type. See Configuring Port Mirroring to Analyze Traffic (CLI Procedure).

  • **count counter-name**—Count the number of packets that pass this filter term.
NOTE: We recommend that you configure a counter for each term in a firewall filter, so that you can monitor the number of packets that match the conditions specified in each filter term.

- **forwarding-class class**—Classify packets in a forwarding class.
- **loss-priority priority**—Set the priority for dropping a packet.
- **policer policer-name**—Apply rate limiting to the traffic.
- **interface interface-name**—Forward the traffic to the specified interface, bypassing the switching lookup.
- **log**—Log the packet's header information in the Routing Engine.

If you omit the *then* statement or do not specify an action, packets that match all the conditions in the *from* statement are accepted. However, you must always explicitly configure an action and/or action modifier in the *then* statement. You can include no more than one action, but you can use any combination of action modifiers. For an action or action modifier to take effect, all conditions in the *from* statement must match.

NOTE: Implicit discard is also applicable to a firewall filter applied to the loopback interface, lo0.

On Juniper Networks EX8200 Ethernet Switches, if an implicit or explicit discard action is configured on a loopback interface for IPv4 traffic, next hop resolve packets are accepted and allowed to pass through the switch. However, for IPv6 traffic, you must explicitly configure a rule to allow the next hop IPv6 resolve packets to pass through the switch.

### Configuring a Term Specifically for IPv4 or IPv6 Traffic

To configure a term in a firewall filter configuration specifically for IPv4 traffic:

1. Verify that neither `ether-type ipv6` nor `ip-version ipv6` is specified in the term in the configuration. By default, a configuration that does not contain either `ether-type ipv6` or `ip-version ipv6` in a term applies to IPv4 traffic.

2. (Optional) Perform one of these tasks:
   - Define `ether-type ipv4` in a term in the configuration.
   - Define `ip-version ipv4` in a term in the configuration.
   - Define both `ether-type ipv4` and `ip-version ipv4` in a term in the configuration.
   - Verify that neither `ether-type ipv6` nor `ip-version ipv6` is specified in a term in the configuration—by default, a configuration that does not contain either `ether-type ipv6` or `ip-version ipv6` in a term applies to IPv4 traffic if it does not contain `ether-type ipv6` or `ip-version ipv6`. 
3. Ensure that other match conditions in the term are valid for IPv4 traffic.

To configure a term in a firewall filter configuration specifically for IPv6 traffic:

1. Perform one of these tasks:
   - Define \texttt{ether-type ipv6} in a term in the configuration.
   - Define \texttt{ip-version ipv6} in a term in the configuration.
   - Define both \texttt{ether-type ipv6} and \texttt{ip-version ipv4} in a term in the configuration.

   \textbf{NOTE:} By default, a configuration that does not contain either \texttt{ether-type ipv6} or \texttt{ip-version ipv6} in a term applies to IPv4 traffic.

2. Ensure that other match conditions in the term are valid for IPv6 traffic.

   \textbf{NOTE:} If the term contains either of the match conditions \texttt{ether-type ipv6} or \texttt{ip-version ipv6}, with no other IPv6 match condition specified, all IPv6 traffic is matched.

   \textbf{NOTE:} To configure a firewall filter for both IPv4 and IPv6 traffic, you must include two separate terms, one for IPv4 traffic and the other for IPv6 traffic.

\section*{Applying a Firewall Filter to a Port on a Switch}

You can apply a firewall filter to a port on a switch to filter ingress or egress traffic on the switch. When you configure the firewall filter, you can specify any match condition, action, and action modifiers specified in "Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches" on page 4096. The action specified in the match condition indicates the action for the matched packets in the ingress or egress traffic.

To apply a firewall filter to a port to filter ingress or egress traffic:

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

   \begin{verbatim}
   [edit interfaces]
   user@switch# set ge-0/0/1 description "filter to limit tcp traffic filter at trunk port for employee-vlan and voice-vlan applied on the interface"
   \end{verbatim}

   \textbf{NOTE:} Providing the description is optional.
2. Specify the unit number and family address type for the interface:

   [edit interfaces]
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching
   
   For firewall filters that are applied to ports, the family address type must be "ethernet-switching".

3. To apply a firewall filter to filter packets that are entering a port:

   [edit interfaces]
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter input ingress-port-filter
   
   To apply a firewall filter to filter packets that are exiting a port:

   [edit interfaces]
   user@switch# set ge-0/0/1 unit 0 family ethernet-switching filter output egress-port-filter
   
   **NOTE:** You can apply no more than one firewall filter per port, per direction.

Applying a Firewall Filter to a Management Interface on a Switch

You can configure and apply a firewall filter to a management interface to control traffic that is entering or exiting the interface on a switch. You can use utilities such as SSH or Telnet to connect to the management interface over the network and then use management protocols such as SNMP to gather statistical data from the switch. Similar to configuring a firewall filter on other types of interfaces, you can configure a firewall filter on a management interface using any match condition, action, and action modifier specified in "Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches" on page 4096 except for the following action modifiers:

- loss-priority
- forwarding-class

You can apply a firewall filter to the management Ethernet interface on any EX Series switch. You can also apply a firewall filter to the virtual management Ethernet (VME) interface on the EX4200 switch. For more information on the management Ethernet interface and the VME interface, see "EX Series Switches Interfaces Overview" on page 2267.

To apply a firewall filter on the management interface to filter ingress or egress traffic:

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

   [edit interfaces]
   user@switch# set me0 description "filter to limit tcp traffic filter at management interface"

   **NOTE:** Providing the description is optional.

2. Specify the unit number and family address type for the management interface:

   [edit interfaces]
   user@switch# set me0 unit 0 family inet
NOTE: For firewall filters that are applied to management interfaces, the family address type can be either inet or inet6.

3. To apply a firewall filter to filter packets that are entering a management interface:

```
[edit interfaces]
user@switch# set me0 unit 0 family inet filter input ingress-port-filter
```

To apply a firewall filter to filter packets that are exiting a management interface:

```
[edit interfaces]
user@switch# set me0 unit 0 family inet filter output egress-port-filter
```

NOTE: You can apply no more than one firewall filter per management interface, per direction.

Applying a Firewall Filter to a VLAN on a Network

You can apply a firewall filter to a VLAN on a network to filter ingress or egress traffic on the network. To apply a firewall filter to a VLAN, specify the VLAN name and ID, and then apply the firewall filter to the VLAN. When you configure the firewall filter, you can specify any match condition, action, and action modifiers specified in "Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches" on page 4096. The action specified in the match condition indicates the action for the matched packets in the ingress or egress traffic.

To apply a firewall filter to a VLAN:

1. Specify the VLAN name and VLAN ID and provide a meaningful description of the firewall filter and the VLAN to which the filter is applied:

```
[edit vlans]
user@switch# set employee-vlan vlan-id (802.1Q Tagging) 20 vlan-description "filter to rate limit traffic applied on employee-vlan"
```

NOTE: Providing the description is optional.

2. Apply firewall filters to filter packets that are entering or exiting the VLAN:

- To apply a firewall filter to filter packets that are entering the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan-id 20 filter input ingress-vlan-filter
```

(On EX4300 switches) To apply a firewall filter to filter packets that are entering the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan-id 20 forwarding-options input ingress-vlan-filter
```

- To apply a firewall filter to filter packets that are exiting the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan-id 20 filter output egress-vlan-filter
```
To apply a firewall filter to filter packets that are exiting the VLAN:

```
[edit vlans]
user@switch# set employee-vlan vlan-id 20 forwarding-options output egress-vlan-filter
```

**NOTE:** You can apply no more than one firewall filter per VLAN, per direction.

---

### Applying a Firewall Filter to a Layer 3 (Routed) Interface

You can apply a firewall filter to a Layer 3 (routed) interface to filter ingress or egress traffic on the switch. When you configure the firewall filter, you can specify any match condition, action, and action modifiers specified in “Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches” on page 4096. The action specified in the match condition indicates the action for the matched packets in the ingress or egress traffic.

To apply a firewall filter to a Layer 3 interface on a switch:

1. Specify the interface name and provide a meaningful description of the firewall filter and the interface to which the filter is applied:

```
[edit interfaces]
user@switch# set ge-0/1/0 description "filter to count and monitor employee-vlan traffic applied on layer 3 interface"
```

**NOTE:** Providing the description is optional.

2. Specify the unit number, family address type, and address for the interface:

```
[edit interfaces]
user@switch# set ge-0/1/0 unit 0 family inet address 10.10.10.1/24
```

For firewall filters applied to Layer 3 interfaces, the family address type must be **inet** (for IPv4 traffic) or **inet6** (for IPv6 traffic).

3. You can apply firewall filters to filter packets that are entering or exiting a Layer 3 (routed) interface:
   - To apply a firewall filter to filter packets that are entering a Layer 3 interface:
     ```
     [edit interfaces]
     user@switch# set ge-0/1/0 unit 0 family inet address 10.10.10.1/24 filter input ingress-router-filter
     ```
   - To apply a firewall filter to filter packets that are exiting a Layer 3 interface:
     ```
     [edit interfaces]
     user@switch# set ge-0/1/0 unit 0 family inet address 10.10.10.1/24 filter output egress-router-filter
     ```
You can apply no more than one firewall filter per Layer 3 interface, per direction.

Related Documentation

- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183
- Example: Configuring a Firewall Filter on a Management Interface on an EX Series Switch on page 4179
- Verifying That Firewall Filters Are Operational on page 4259
- Monitoring Firewall Filter Traffic on page 4261
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206

Configuring Firewall Filters (J-Web Procedure)

You configure firewall filters on EX Series switches to control traffic that enters ports on the switch or enters and exits VLANs on the network and Layer 3 (routed) interfaces. To configure a firewall filter, you must configure the filter and then apply it to a port, VLAN, or Layer 3 interface.

To configure firewall filter settings by using the J-Web interface:

1. Select Configure > Security > Filters.

   The Firewall Filter Configuration page displays a list of all configured ports or VLANs or router filters and the ports or VLANs associated with a particular filter.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Select this option to create a new filter. Enter information as specified in Table 521 on page 4202.
   - **Edit**—Select this option to edit an existing filter. Enter information as specified in Table 521 on page 4202.
   - **Delete**—Select this option to delete a filter.
• **Term Up**—Select this option to move a term up in the filter term list.
• **Term Down**—Select this option to move a term down in the filter term list.

### Table 521: Create a New Filter

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Filter type</td>
<td>Specifies the filter type: port or VLAN firewall filter or router firewall filter.</td>
<td>Select the filter type.</td>
</tr>
<tr>
<td>Filter name</td>
<td>Specifies the name for the filter.</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>Select terms to be part of the filter</td>
<td>Specifies the terms to be associated with the filter. Add new terms or edit existing terms.</td>
<td>Click <strong>Add</strong> to add new terms. Enter information as specified in Table 522 on page 4202 and Table 523 on page 4203.</td>
</tr>
</tbody>
</table>

### Association tab

| Port Associations      | Specifies the ports with which the filter is associated. | 1. Click **Add**.  
|                        | **NOTE:** For a port or VLAN filter type, only ingress direction is supported for port association. | 2. Select the direction: Ingress or Egress.  
|                        |                                                           | 3. Select the ports. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the available ports from the list.  
|                        |                                                           | 4. Click **OK**. |
| VLAN Associations      | Specifies the VLANs with which the filter is associated. | 1. Click **Add**.  
|                        | **NOTE:** Because router firewall filters can be associated with ports only, this section is not displayed for a router firewall filter. | 2. Select the direction: Ingress or Egress.  
|                        |                                                           | 3. Select the VLANs.  
|                        |                                                           | 4. Click **OK**. |

### Table 522: Create a New Term

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term Name</td>
<td>Specifies the name of the term.</td>
<td>Enter a name.</td>
</tr>
</tbody>
</table>
| Protocols  | Specifies the protocols to be associated with the term. | 1. Click **Add**.  
|            |                                               | 2. Select the protocols.  
|            |                                               | 3. Click **OK**. |
### Table 522: Create a New Term (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Specifies the source IP address, MAC address, and available ports.</td>
<td>To specify the IP address, click <strong>Add &gt; IP</strong> and enter the IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> MAC address is specified only for port or VLAN filters.</td>
<td>To specify the MAC address, click <strong>Add &gt; MAC</strong> and enter the MAC address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To specify the ports (interfaces), click <strong>Add &gt; Ports</strong> and enter the port number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete the IP address, MAC address, or port details, select it and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Destination</td>
<td>Specifies the destination IP address, MAC address, and available ports.</td>
<td>To specify the IP address, click <strong>Add &gt; IP</strong> and enter the IP address.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> MAC address is specified only for port or VLAN filters.</td>
<td>To specify the MAC address, click <strong>Add &gt; MAC</strong> and enter the MAC address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To specify the ports (interfaces), click <strong>Add &gt; Ports</strong> and enter the port number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete the IP address, MAC address, or port details, select it and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the packet action for the term.</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Accept</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Discard</td>
</tr>
<tr>
<td>More</td>
<td>Specifies advanced configuration options for the filter.</td>
<td>Select the match conditions as specified in Table 523 on page 4203.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the packet action for the term as specified in Table 523 on page 4203.</td>
</tr>
</tbody>
</table>

### Table 523: Advanced Options for Terms

<table>
<thead>
<tr>
<th>Table</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Type</td>
<td>Specifies the ICMP packet type field. Typically, you specify this match condition in conjunction with the protocol match condition to determine which protocol is being used on the port.</td>
<td>Select the option from the list.</td>
</tr>
<tr>
<td>ICMP Code</td>
<td>Specifies more specific information than the ICMP type. Because the value's meaning depends upon the associated ICMP type, you must specify icmp-type along with icmp-code. The keywords are grouped by the ICMP type with which they are associated.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Specifies the Differentiated Services code point (DSCP). The DiffServ protocol uses the type-of-service (ToS) byte in the IP header. The most significant six bits of this byte form the DSCP.</td>
<td>Select the DSCP number from the list.</td>
</tr>
</tbody>
</table>
Table 523: Advanced Options for Terms (continued)

<table>
<thead>
<tr>
<th>Table</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precedence</td>
<td>Specifies the IP precedence.</td>
<td>Select the option from the list.</td>
</tr>
<tr>
<td></td>
<td>NOTE: The IP precedence and the DSCP number cannot be specified together for the same term.</td>
<td></td>
</tr>
<tr>
<td>IP Options</td>
<td>Specifies the presence of the options field in the IP header.</td>
<td>Select the option from the list.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interface on which the packet is received.</td>
<td>Select the interface from the list.</td>
</tr>
<tr>
<td>Ether type</td>
<td>Specifies the Ethernet type field of a packet.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Dot 1q user priority</td>
<td>Specifies the user-priority field of the tagged Ethernet packet.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td></td>
<td>User-priority values can be 0–7. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• background (1)—Background</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• best-effort (0)—Best effort</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• controlled-load (4)—Controlled load</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• excellent-load (3)—Excellent load</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• network-control (7)—Network control reserved traffic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• standard (2)—Standard or spare</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• video (5)—Video</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• voice (6)—Voice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is not applicable for a routing filter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>Specifies the VLAN to be associated with the packet.</td>
<td>Select the VLAN from the list.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is not applicable for a routing filter.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>TCP Flags</td>
<td>Specifies one or more TCP flags.</td>
<td>Select the option TCP Initial or enter a combination of TCP flags.</td>
</tr>
<tr>
<td></td>
<td>NOTE: TCP flags are supported on ingress ports, VLANs, and router interfaces.</td>
<td></td>
</tr>
<tr>
<td>Fragmentation Flags</td>
<td>Specifies the IP fragmentation flags.</td>
<td>Select either the option is-fragment or enter a combination of fragment action flags.</td>
</tr>
</tbody>
</table>
### Table 523: Advanced Options for Terms (continued)

<table>
<thead>
<tr>
<th>Table</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dot1q tag</td>
<td>Specifies the value for the tag field in the Ethernet header. The value can be from 1 through 4095.</td>
<td>Enter the value.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is not supported on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Vlan Id</td>
<td>Specifies the value of the VLAN ID. The value can be from 0 through 4095 or a range of values.</td>
<td>Enter a value.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Vlan 1P Priority</td>
<td>Specifies the priority value. The values can be from 0 through 7.</td>
<td>Enter a value.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learn Vlan Id</td>
<td>Specifies the value of the learnt VLAN ID. The value can be from 0 through 4095 or a range of values.</td>
<td>Enter a value.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This option is supported only on EX4300 switches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Counter name</td>
<td>Specifies the count of the number of packets that pass this filter, term, or policer.</td>
<td>Enter a value.</td>
</tr>
<tr>
<td>Forwarding class</td>
<td>Classifies the packet into one of the following forwarding classes:</td>
<td>Select the option from the list.</td>
</tr>
<tr>
<td></td>
<td>• assured-forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• best-effort</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• expedited-forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• network-control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• None</td>
<td></td>
</tr>
<tr>
<td>Loss priority</td>
<td>Specifies the packet loss priority.</td>
<td>Enter the value.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> Forwarding class and loss priority should be specified together for the same term.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyzer</td>
<td>Specifies whether to perform port mirroring on packets. Port mirroring copies all packets entering one switch port to a network monitoring connection on another switch port.</td>
<td>Select the analyzer (port mirroring configuration) from the list.</td>
</tr>
</tbody>
</table>
Table 523: Advanced Options for Terms *(continued)*

<table>
<thead>
<tr>
<th>Table</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Mirror Instance</td>
<td>Specifies whether to perform port mirroring on packets. Port mirroring copies all packets entering one switch port to a network- monitoring connection on another switch port.</td>
<td>Select the port mirroring instance from the list. Default is selected by default.</td>
</tr>
</tbody>
</table>

**Related Documentation**
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Verifying That Firewall Filters Are Operational on page 4259
- Firewall Filters for EX Series Switches Overview on page 4088
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096

**Configuring Policers to Control Traffic Rates (CLI Procedure)**

You can configure policers to rate limit traffic on EX Series switches. After you configure a policer, you can include it in an ingress firewall filter configuration.

When you configure a firewall filter, you can specify a policer action for any term or terms within the filter. All traffic that matches a term that contains a policer action goes through the policer that the term references. Each policer that you configure includes an implicit counter. To get term-specific packet counts, you must configure a separate policer for each filter term that requires policing.

**NOTE:** On all EX Series switches except EX8200 switches, each policer that you configure includes an implicit counter. To ensure term-specific packet counts, configure a policer for each term in the filter that requires policing. For EX8200 switches, configure a policer and associate it with a global management counter using the `counter` option.

The following policer limits apply on a switch:

- A maximum of 512 policers can be configured for port firewall filters.
- A maximum of 512 policers can be configured for VLAN and Layer 3 firewall filters.

If the number of policers in the firewall filter configuration exceeds these limits, the switch returns the following message when you commit the configuration:

*Cannot assign policers: Max policer limit reached*
This topic includes these tasks:

1. **Configuring Policers on page 4207**
2. **Specifying Policers in a Firewall Filter Configuration on page 4208**
3. **Applying a Firewall Filter That Is Configured with a Policer on page 4208**

**Configuring Policers**

To configure a policer:

1. Specify the name of the policer:

   ```
   [edit firewall]
   user@switch# set policer policer-one
   ```
   The policer name can include letters, numbers, and hyphens (-) and can contain up to 64 characters.

2. Specify the *filter-specific* statement to configure a policer to act as a filter-specific policer; else proceed to step 3:

   ```
   [edit firewall]
   user@switch# set policer policer-one filter-specific
   ```
   If you do not specify the *filter-specific* statement, the policer acts as a term-specific policer by default.

3. Configure rate limiting for the policer:

   a. Specify the bandwidth limit in bits per second (bps) to control the traffic rate on an interface:

      ```
      [edit firewall policer policer-one]
      user@switch# set if-exceeding bandwidth-limit 300k
      ```
      The range for the bandwidth limit is 1k through 102.3g bps.

   b. Specify the burst-size limit (the maximum allowed burst size in bytes) to control the amount of traffic bursting:

      ```
      [edit firewall policer policer-one]
      user@switch# set if-exceeding burst-size-limit 500k
      ```
      To determine the value for the burst-size limit, multiply the bandwidth of the interface on which the filter is applied by the amount of time to allow a burst of traffic at that bandwidth to occur:

      \[
      \text{burst size} = (\text{bandwidth}) \times (\text{allowable time for burst traffic})
      \]
      The range for the burst-size limit is 1 through 2,147,450,880 bytes.

4. Specify the policer action **discard** to discard packets that exceed the rate limits:

   ```
   [edit firewall policer]
   user@switch# set policer-one then (Policer Action) discard
   ```
   Discard is the only supported policer action.

5. On EX8200 switches, you must assign a global management counter to the policer to obtain policer statistics:

   ```
   [edit firewall policer]
   user@switch# set policer-one counter counter-id 0
   ```
In this sample statement, the global management counter ID is 0. You can assign any number of policers to the global management counter. The policer statistics displayed for each counter are the collective statistics of all policers assigned to that counter.

**Specifying Policers in a Firewall Filter Configuration**

To reference a policer for a single firewall, configure a filter term that includes the policer action:

```
[edit firewall family ethernet-switching]
user@switch# set filter limit-hosts term term-one from source-address 192.0.2.16/28
user@witch# set filter limit-hosts term term-one then policer policer-one
```

**Applying a Firewall Filter That Is Configured with a Policer**

A firewall filter that is configured with one or more policer actions, like any other firewall filter, must be applied to a port, VLAN, or Layer 3 interface. For information about applying firewall filters, see the sections on applying firewall filters in “Configuring Firewall Filters (CLI Procedure)” on page 4192.

**Related Documentation**

- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Verifying That Policers Are Operational on page 4260
- Understanding the Use of Policers in Firewall Filters on page 4155
Assigning Multifield Classifiers in Firewall Filters to Specify Packet-Forwarding Behavior (CLI Procedure)

You can configure firewall filters with multifield classifiers to classify packets transiting a port, VLAN, or Layer 3 interface on an EX Series switch.

You specify multifield classifiers in a firewall filter configuration to set the forwarding class and packet loss priority (PLP) for incoming or outgoing packets. By default, the data traffic that is not classified is assigned to the best-effort class associated with queue 0.

You can specify any of the following default forwarding classes:

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>0</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>1</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>5</td>
</tr>
<tr>
<td>network-control</td>
<td>7</td>
</tr>
</tbody>
</table>

To assign multifield classifiers in firewall filters:

1. Configure the family name and filter name for the filter at the [edit firewall] hierarchy level, for example:

   [edit firewall]
   user@switch# set family ethernet-switching
   user@switch# set family ethernet-switching filter ingress-filter

2. Configure the terms of the filter, including the forwarding-class and loss-priority action modifiers as appropriate. When you specify a forwarding class you must also specify the packet loss priority. For example, each of the following terms examines different packet header fields and assigns an appropriate classifier and the packet loss priority:

   - The term voice-traffic matches packets on the voice-vlan and assigns the forwarding class expedited-forwarding and packet loss priority low:

     [edit firewall family ethernet-switching filter ingress-filter]
     user@switch# set term voice-traffic from vlan-id voice-vlan
     user@switch# set term voice-traffic then forwarding-class expedited-forwarding
     user@switch# set term voice-traffic then loss-priority low

   - The term data-traffic matches packets on employee-vlan and assigns the forwarding class assured-forwarding and packet loss priority low:

     [edit firewall family ethernet-switching filter ingress-filter]
     user@switch# set term data-traffic from vlan-id employee-vlan
     user@switch# set term data-traffic then forwarding-class assured-forwarding
     user@switch# set term data-traffic then loss-priority low

   - Because loss of network-generated packets can jeopardize proper network operation, delay is preferable to discard of packets. The following term,
network-traffic, assigns the forwarding class network-control and packet loss priority low:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch#  set term network-traffic from precedence net-control
user@switch#  set term network-traffic then forwarding-class network
user@switch#  set term network-traffic then loss-priority low
```

- The last term accept-traffic matches any packets that did not match on any of the preceding terms and assigns the forwarding class best-effort and packet loss priority low:

```
[edit firewall family ethernet-switching filter ingress-filter]
user@switch#  set term accept-traffic from precedence net-control
user@switch#  set term accept-traffic then forwarding-class best-effort
user@switch#  set term accept-traffic then loss-priority low
```

3. Apply the filter ingress-filter to a port, VLAN or Layer 3 interface. For information about applying the filter, see “Configuring Firewall Filters (CLI Procedure)” on page 4192.

### Related Documentation
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Verifying That Firewall Filters Are Operational on page 4259
- Monitoring Firewall Filter Traffic on page 4261
- Defining CoS Classifiers (CLI Procedure) on page 1923
- Defining CoS Classifiers (J-Web Procedure) on page 1925
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201

### Configuring Routing Policies (J-Web Procedure)

All routing protocols use the Junos OS routing table to store the routes that they learn and to determine which routes are advertised in the protocol packets. Routing policy allows you to control which routes the routing protocols store in and retrieve from the routing table on the routing device.

To configure routing policies for an EX Series switch using the J-Web interface:


   **NOTE:** After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
• **Global Options**—Configures global options for policies. Enter information into the configuration page as described in Table 524 on page 4211.

• **Add**—Configures a new policy. Select New and specify a policy name. To add terms, enter information into the configuration page as described in Table 525 on page 4212. Select Clone to create a copy of an existing policy.

• **Edit**—Edits an existing policy. To modify an existing term, enter information into the configuration page as described in Table 525 on page 4212.

• **Term Up**—Moves a term up in the list.

• **Term Down**—Moves a term down in the list.

• **Delete**—Deletes the selected policy.

• **Test Policy**—Tests the policy. Use this option to check whether the policy produces the results that you expect.

### Table 524: Policies Global Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix List</td>
<td>Specifies a list of IPv4 address prefixes for use in a routing policy statement.</td>
<td>To add a prefix list:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter a name for the prefix list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. To add an IP address, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enter the IP address and the subnet mask and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To edit a prefix list, click <strong>Edit</strong>. Edit the settings and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a prefix list, select it and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>BGP Community</td>
<td>Specifies a BGP community.</td>
<td>To add a BGP community:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter a name for the community.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. To add a community, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enter the community ID and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To edit a BGP community, click <strong>Edit</strong>. Edit the settings and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a BGP community, select it and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
Table 524: Policies Global Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Path</td>
<td>Specifies an AS path. This is applicable to BGP only.</td>
<td>To add an AS path:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter the AS path name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter the regular expression and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To edit an AS path, click <strong>Edit</strong>. Edit the settings and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete an AS path, select it and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

Table 525: Terms Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term Name</td>
<td>Specifies a term name.</td>
<td>Type or select and edit the name.</td>
</tr>
<tr>
<td>Source tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Family</td>
<td>Specifies an address family protocol.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Specifies a routing instance.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>RIB</td>
<td>Specifies the name of a routing table.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Preference</td>
<td>Specifies the individual preference value for the route.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Metric</td>
<td>Specifies a metric value. You can specify up to four metric values.</td>
<td>Type or select and edit the value.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies a name or IP address of one or more routing device interfaces.</td>
<td>To add an interface, select <strong>Add &gt; Interface</strong>. Select the interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list. To add an address, select <strong>Add &gt; Address</strong>. Select the address from the list. To remove an interface, select it and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Prefix List</td>
<td>Specifies a named list of IP addresses. You can specify an exact match with incoming routes.</td>
<td>Click <strong>Add</strong>. Select the prefix list from the list and click <strong>OK</strong>. To remove a prefix list, select it and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the name of the protocol from which the route was learned or to which the route is being advertised.</td>
<td>Click <strong>Add</strong> and select the protocol from the list. To remove a protocol, select it and click <strong>Remove</strong>.</td>
</tr>
</tbody>
</table>
Table 525: Terms Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Specifies the name of a policy to evaluate as a subroutine.</td>
<td>Click <strong>Add</strong>. Select the policy from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To remove a policy, select it and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>More</td>
<td>Specifies advanced configuration options for policies.</td>
<td>Click <strong>More</strong> for advanced configuration.</td>
</tr>
<tr>
<td>OSPF Area ID</td>
<td>Specifies the area identifier.</td>
<td>Type the IP address.</td>
</tr>
<tr>
<td>BGP Origin</td>
<td>Specifies the origin of the AS path information.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>Specifies the BGP local preference.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Route</td>
<td>Specifies the type of route.</td>
<td>Select <strong>External</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Select the OSPF type from the list.</td>
</tr>
<tr>
<td>AS Path</td>
<td>Specifies the name of an AS path regular expression.</td>
<td>Click <strong>Add</strong>. Select the AS path from the list.</td>
</tr>
<tr>
<td>Community</td>
<td>Specifies the name of one or more communities.</td>
<td>Click <strong>Add</strong>. Select the community from the list.</td>
</tr>
<tr>
<td>Destination tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Family</td>
<td>Specifies an address family protocol.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Routing Instance</td>
<td>Specifies a routing instance.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>RIB</td>
<td>Specifies the name of a routing table.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Preference</td>
<td>Specifies the individual preference value for the route.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Metric</td>
<td>Specifies a metric value.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies a name or IP address of one or more routing device interfaces. Do not use this qualifier with protocols that are not interface-specific, such as internal BGP (IBGP).</td>
<td>To add an interface, select <strong>Add &gt; interface</strong>. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To add an address, select <strong>Add &gt; Address</strong>. Select the address from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete an interface, select it and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the name of the protocol from which the route was learned or to which the route is being advertised.</td>
<td>Click <strong>Add</strong> and select the protocol from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a protocol, select it and click <strong>Remove</strong>.</td>
</tr>
</tbody>
</table>
Table 525: Terms Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the action to take if the conditions match.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Default Action</td>
<td>Specifies that any action that is intrinsic to the protocol is</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td></td>
<td>overridden. This action is also nonterminating, so that various</td>
<td></td>
</tr>
<tr>
<td></td>
<td>policy terms can be evaluated before the policy is terminated.</td>
<td></td>
</tr>
<tr>
<td>Next</td>
<td>Specifies the default control action if a match occurs, and</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td></td>
<td>there are no further terms in the current routing policy.</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies a priority for prefixes included in an OSPF import</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td></td>
<td>policy. Prefixes learned through OSPF are installed in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>routing table based on the priority assigned to the prefixes.</td>
<td></td>
</tr>
<tr>
<td>BGP Origin</td>
<td>Specifies the BGP origin attribute.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>AS Path Prepend</td>
<td>Affixes an AS number at the beginning of the AS path. The AS numbers</td>
<td>Enter a value.</td>
</tr>
<tr>
<td></td>
<td>are added after the local AS number has been added to the path. This</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action adds an AS number to AS sequences only, not to AS sets. If the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>existing AS path begins with a confederation sequence or set, the affixed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AS number is placed within a confederation sequence. Otherwise, the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>affixed AS number is placed with a nonconfederation sequence.</td>
<td></td>
</tr>
<tr>
<td>AS Path Expand</td>
<td>Extracts the last AS number in the existing AS path and affixes</td>
<td>Select the type and type a value.</td>
</tr>
<tr>
<td></td>
<td>that AS number to the beginning of the AS path n times, where n is a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>number from 1 through 32. The AS number is added before the local AS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>number has been added to the path. This action adds AS numbers to AS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sequences only, not to AS sets. If the existing AS path begins with a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>confederation sequence or set, the affixed AS numbers are placed within</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a confederation sequence. Otherwise, the affixed AS numbers are placed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>within a nonconfederation sequence. This option is typically used in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>non-IBGP export policies.</td>
<td></td>
</tr>
<tr>
<td>Load Balance Per Packet</td>
<td>Specifies that all next-hop addresses in the forwarding table must be</td>
<td>Select the check box to enable the option.</td>
</tr>
<tr>
<td></td>
<td>installed and have the forwarding table perform per-packet load</td>
<td></td>
</tr>
<tr>
<td></td>
<td>balancing. This policy action allows you to optimize VPLS traffic flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td>across multiple paths.</td>
<td></td>
</tr>
<tr>
<td>Tag</td>
<td>Specifies the tag value. The tag action sets the 32-bit tag field in</td>
<td>Select the action and type a value.</td>
</tr>
<tr>
<td></td>
<td>OSPF external link-state advertisement (LSA) packets.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Changes the metric (MED) value by the specified negative or positive</td>
<td>Select the action and type a value.</td>
</tr>
<tr>
<td></td>
<td>offset. This action is useful only in an external BGP (EBGP) export</td>
<td></td>
</tr>
<tr>
<td></td>
<td>policy.</td>
<td></td>
</tr>
<tr>
<td>Route</td>
<td>Specifies whether the route is external.</td>
<td>Select the External check box to enable the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>option, and select the OSPF type.</td>
</tr>
</tbody>
</table>
### Table 525: Terms Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preference</td>
<td>Specifies the preference value.</td>
<td>Select the preference action and type a value.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>Specifies the BGP local preference attribute.</td>
<td>Select the action and type a value.</td>
</tr>
</tbody>
</table>
| Class of Service | Specifies and applies the class-of-service parameters to routes installed into the routing table. | Type the source class.  
Type the destination class.  
Type the forwarding class. |

#### Related Documentation
- Configuring BGP Sessions (J-Web Procedure) on page 2557
- Configuring an OSPF Network (J-Web Procedure) on page 2811
- Configuring a RIP Network (J-Web Procedure) on page 2951
- Configuring Static Routing (J-Web Procedure) on page 3024
- Layer 3 Protocols Supported on EX Series Switches on page 2553

## Configuring Tricolor Marking Policers

You can rate-limit traffic on EX Series switches by configuring a policer and specifying it as an action modifier for a term in a firewall filter. By default, if you specify the same policer in multiple terms, Junos OS creates a separate policer instance for each term and applies rate limiting separately for each instance. For example, if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, each policer instance enforces a 1-Gbps limit. In this case, the total bandwidth allowed by the filter is 3 Gbps.

You can also configure a policer to be filter-specific, which means that Junos OS creates only one policer instance regardless of how many times the policer is referenced. When you do this, rate limiting is applied in aggregate, so if you configure a policer to discard traffic that exceeds 1 Gbps and reference that policer in three different terms, the total bandwidth allowed by the filter is 1 Gbps.

This topic describes how to configure single-rate and two-rate tricolor marking (TCM) policers, also known as single-rate and two-rate three-color policers. If you want to
configure a single-rate two-color policer (also known just as a "policer"), see "Configuring Policers to Control Traffic Rates (CLI Procedure)" on page 4206.

This topic includes:

- Configuring a Tricolor Marking Policer on page 4216
- Applying Tricolor Marking Policers to Firewall Filters on page 4216

Configuring a Tricolor Marking Policer

A tricolor marking policer polices traffic on the basis of metering rates, including the configured information rate (CIR), the peak information rate (PIR), their associated burst sizes, and any policing actions configured for the traffic. With tri-color marking, you can configure traffic policing according to two separate modes—color-blind and color-aware. In color-blind mode, the current packet loss priority (PLP) value is ignored. In color-aware mode, the current PLP values are considered by the policer, and the policer can increase those values but cannot decrease them.

To configure a tricolor marking (TCM) policer:

1. Specify the name of the policer and (optionally) whether to automatically discard packets with high loss priority (PLP):

   ```
   [edit firewall]
   user@switch# set three-color-policer policer-name
   user@switch# set three-color-policer policer-name action loss-priority high then discard
   ```

2. Specify the policer as either single-rate or two-rate and as color-aware or color-blind:

   ```
   [edit firewall three-color-policer policer-name]
   user@switch# set rate mode
   ```

   For example:

   ```
   [edit firewall three-color-policer srTCM-1a]
   user@switch# set single-rate color-aware
   [edit firewall three-color-policer trTCM2-cb]
   user@switch# set two-rate color-blind
   ```

3. For a single-rate TCM policer, configure the CIR, committed burst size (CBS), and excess burst size (EBS):

   ```
   [edit firewall three-color-policer policer-name single-rate]
   user@switch# set committed-information-rate bps
   user@switch# set committed-burst-size bytes
   user@switch# set excess-burst-size bytes
   ```

4. For a two-rate TCM policer, configure the CIR, CBS, PIR, and peak burst size (PBS):

   ```
   [edit firewall three-color-policer policer-name single-rate]
   user@switch# set committed-information-rate bps
   user@switch# set committed-burst-size bytes
   user@switch# set peak-information-rate bps
   user@switch# set peak-burst-size bytes
   ```

Applying Tricolor Marking Policers to Firewall Filters

To rate-limit traffic by applying a tricolor marking (TCM) policer to a firewall filter:

```
[edit firewall family family filter filter-name term term-name then]
user@switch# set three-color-policer rate srTCM1-ca
```
For example:

```
[edit firewall family inet filter test1 term term1 then]
user@switch# set three-color-policer single-rate policer
```

You must include either the single-rate statement or the two-rate statement in the reference to the policer in the firewall filter configuration, and this statement must match the configured TCM policer. Otherwise, an error message appears in the configuration listing.

For example, if you configure `srTCM1-ca` as a single-rate TCM policer and try to apply it as a two-rate policer, the following message appears:

```
[edit firewall]
user@switch# show three-color-policer srTCM1-ca
single-rate {
  color-aware;
  ...
}
user@switch# show filter TESTER
term A {
  then {
    three-color-policer {
      #
      # Warning: Referenced two-rate policer does not exist
      #
      two-rate srTCM;
    }
  }
}
```

**Related Documentation**
- Understanding Tricolor Marking Architecture on page 4159
- Understanding the Use of Policers in Firewall Filters on page 4155

**Configuration Statements**

- [edit firewall] Configuration Statement Hierarchy on EX Series Switches on page 4217
- Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches on page 4219

**[edit firewall] Configuration Statement Hierarchy on EX Series Switches**

This topic lists supported and unsupported configuration statements in the [edit firewall] hierarchy level on EX Series switches.

- **Supported** statements are those that you can use to configure some aspect of a software feature on the switch.
- **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.
This topic lists:

- Supported Statements in the [edit firewall] Hierarchy Level on page 4218
- Unsupported Statements in the [edit firewall] Hierarchy Level on page 4219

**Supported Statements in the [edit firewall] Hierarchy Level**

The following hierarchy shows the [edit firewall] configuration statements supported on EX Series switches:

```plaintext
firewall {
    family family-name {
        filter filter-name {
            interface-specific;
            term term-name {
                from {
                    match-conditions;
                }
                then {
                    action;
                    action-modifiers;
                }
            }
        }
    }
    policer policer-name {
        filter-specific;
        if-exceeding {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
        then {
            policer-action;
        }
    }
    three-color-policer policer-name {
        action {
            loss-priority high then discard;
        }
        filter-specific;
        single-rate {
            (color-aware | color-blind);
            committed-burst-size bytes;
            committed-information-rate bps;
            excess-burst-size bytes;
        }
        two-rate {
            (color-aware | color-blind);
            committed-burst-size bytes;
            committed-information-rate bps;
            peak-information-rate bps;
            peak-burst-size bytes;
        }
    }
}
```
Unsupported Statements in the [edit firewall] Hierarchy Level

All statements in the [edit firewall] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.

Related Documentation

- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches on page 4219
- Firewall Filters for EX Series Switches Overview on page 4088

Firewall Filter Configuration Statements Supported by Junos OS for EX Series Switches

You configure firewall filters to filter packets based on their components and to perform an action on packets that match the filter.

Table 526 on page 4219 lists the options that are supported for the firewall statement in Junos OS for EX Series switches.

Table 526: Supported Options for Firewall Filter Statements

<table>
<thead>
<tr>
<th>Statement and Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>family family-name {</code></td>
<td>The <code>family-name</code> option specifies the version or type of addressing protocol:</td>
</tr>
<tr>
<td><code>}</code></td>
<td>• <code>any</code>—Filter packets based on protocol-independent match conditions.</td>
</tr>
<tr>
<td></td>
<td>• <code>ethernet-switching</code>—Filter Layer 2 (Ethernet) packets and Layer 3 (IP) packets</td>
</tr>
<tr>
<td></td>
<td>• <code>inet</code>—Filter IPv4 packets</td>
</tr>
<tr>
<td></td>
<td>• <code>inet6</code>—Filter IPv6 packets</td>
</tr>
<tr>
<td><code>filter filter-name {</code></td>
<td>The <code>filter-name</code> option identifies the filter. The name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose the name in quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td><code>}</code></td>
<td></td>
</tr>
<tr>
<td><code>interface-specific</code></td>
<td>The <code>interface-specific</code> statement configures unique names for individual firewall counters specific to each interface.</td>
</tr>
<tr>
<td><code>term term-name {</code></td>
<td>The <code>term-name</code> option identifies the term. The name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose the entire name in quotation marks (&quot; &quot;). Each term name must be unique within a filter.</td>
</tr>
<tr>
<td><code>}</code></td>
<td></td>
</tr>
</tbody>
</table>
### Table 526: Supported Options for Firewall Filter Statements (continued)

<table>
<thead>
<tr>
<th>Statement and Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>from {</code></td>
<td>The <code>from</code> statement is optional. If you omit it, all packets are considered to match.</td>
</tr>
<tr>
<td><code>match-conditions;</code></td>
<td><code>then {</code> For information about the <code>action</code> and <code>action-modifiers</code> options, see &quot;Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches&quot; on page 4096.</td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>policer policer-name</code> {</td>
</tr>
<tr>
<td></td>
<td>The <code>policer-name</code> option identifies the policer. The name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose the name in quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>filter-specific</code> The <code>filter-specific</code> statement configures policers and counters for a specific filter name.</td>
</tr>
<tr>
<td><code>if-exceeding {</code></td>
<td>The <code>bandwidth-limit bps</code> option specifies the traffic rate in bits per second (bps).</td>
</tr>
<tr>
<td><code>burst-size-limit bytes</code></td>
<td>You can specify <code>bps</code> as a decimal value or as a decimal number followed by one of the following abbreviations:</td>
</tr>
<tr>
<td><code>}</code></td>
<td>• k (thousand)</td>
</tr>
<tr>
<td></td>
<td>• m (million)</td>
</tr>
<tr>
<td></td>
<td>• g (billion, which is also called a thousand million)</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 1000 (1k) through 102,300,000,000 (102.3g) bps</td>
</tr>
<tr>
<td></td>
<td><code>burst-size-limit bytes</code> option specifies the maximum allowed burst size to control the amount of traffic bursting. To determine the value for the burst-size limit, you can multiply the bandwidth of the interface on which the filter is applied by the amount of time (in seconds) to allow a burst of traffic at that bandwidth to occur:</td>
</tr>
<tr>
<td></td>
<td>burst size = bandwidth * allowable time for burst traffic</td>
</tr>
<tr>
<td></td>
<td>You can specify a decimal value or a decimal number followed by k (thousand) or m (million).</td>
</tr>
<tr>
<td></td>
<td><strong>Range</strong>: 1 through 2,147,450,880 bytes</td>
</tr>
<tr>
<td><code>}</code></td>
<td><code>then {</code> Use the <code>policer-action</code> option to specify <code>discard</code> to discard traffic that exceeds the rate limits.</td>
</tr>
<tr>
<td><code>policer-action</code></td>
<td></td>
</tr>
</tbody>
</table>

Junos OS for EX Series switches does not support some of the firewall filter statements that are supported by other Junos OS packages. Table 527 on page 4221 shows the firewall filter statements that are not supported by Junos OS for EX Series switches.
### Table 527: Firewall Filter Statements That Are Not Supported by Junos OS for EX Series Switches

<table>
<thead>
<tr>
<th>Statements Not Supported</th>
<th>Statement Hierarchy Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>• interface-set interface-set-name { }</td>
<td>[edit firewall]</td>
</tr>
<tr>
<td>• load-balance-group group-name { }</td>
<td></td>
</tr>
<tr>
<td>• three-color-policer name { }</td>
<td></td>
</tr>
<tr>
<td>• logical-interface-policer;</td>
<td></td>
</tr>
<tr>
<td>• single-rate { }</td>
<td></td>
</tr>
<tr>
<td>• two-rate { }</td>
<td></td>
</tr>
<tr>
<td>• prefix-action name { }</td>
<td>[edit firewall family family-name]</td>
</tr>
<tr>
<td>• prefix-policer { }</td>
<td></td>
</tr>
<tr>
<td>• service-filter filter-name { }</td>
<td></td>
</tr>
<tr>
<td>• simple-filter simple-filter-name { }</td>
<td></td>
</tr>
<tr>
<td>• accounting-profile name;</td>
<td>[edit firewall family family-name filter filter-name]</td>
</tr>
<tr>
<td>• logical-bandwidth-policer;</td>
<td>[edit firewall policer policer-name]</td>
</tr>
<tr>
<td>• logical-interface-policer;</td>
<td></td>
</tr>
<tr>
<td>bandwidth-percent number;</td>
<td>[edit firewall policer policer-name if-exceeding]</td>
</tr>
</tbody>
</table>

### Related Documentation
- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches](#) on page 4096
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](#) on page 4161
- [Configuring Firewall Filters (CLI Procedure)](#) on page 4192
- [Configuring Policers to Control Traffic Rates (CLI Procedure)](#) on page 4206
- [Firewall Filters for EX Series Switches Overview](#) on page 4088
**action (TCM Policers)**

Syntax

```plaintext
action [ 
  loss-priority high then discard;
]
```

Hierarchy Level

```
[edit firewall three-color-policer name]
```

Release Information

Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description

Discard traffic on a logical interface using tricolor marking policing.

The remaining statement is explained separately.

Required Privilege Level

- firewall—To view this statement in the configuration.
- firewall-control—To add this statement to the configuration.

Related Documentation

- Configuring Tricolor Marking Policers on page 4215

**apply-path**

Syntax

```plaintext
apply-path path;
```

Hierarchy Level

```
[edit logical-systems logical-system-name policy-options prefix-list name],
[edit policy-options prefix-list name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Expand a prefix list to include all prefixes pointed to by a defined path.

Options

- `path`—String of elements composed of identifiers or configuration keywords that points to a set of prefixes. You can include wildcards (enclosed in angle brackets) to match more than one identifier. You cannot add a path element, including wildcards, after a leaf statement. Path elements, including wildcards, can only be used after a container statement.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Prefix Lists
- Example: Configuring Routing Policy Prefix Lists
- Example: Configuring a Filter to Limit TCP Access to a Port Based On a Prefix List

Copyright © 2013, Juniper Networks, Inc.
### as-path (Policy Options)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>as-path name regular-expression;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit dynamic policy-options],</td>
</tr>
<tr>
<td></td>
<td>[edit logical-systems logical-system-name policy-options],</td>
</tr>
<tr>
<td></td>
<td>[edit policy-options]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced before Junos OS Release 7.4.</td>
</tr>
<tr>
<td></td>
<td>Statement introduced in Junos OS Release 9.0 for EX Series switches.</td>
</tr>
<tr>
<td></td>
<td>Support for configuration in the dynamic database introduced in Junos OS Release 9.5.</td>
</tr>
<tr>
<td></td>
<td>Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Define an autonomous system (AS) path regular expression for use in a routing policy match condition.</td>
</tr>
<tr>
<td>Options</td>
<td>name—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 65,536 characters long. To include spaces in the name, enclose it in quotation marks (&quot; &quot;).</td>
</tr>
<tr>
<td></td>
<td>regular-expression—One or more regular expressions used to match the AS path.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>routing—To view this statement in the configuration.</td>
</tr>
<tr>
<td></td>
<td>routing-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• Understanding AS Path Regular Expressions for Use as Routing Policy Match Conditions</td>
</tr>
<tr>
<td></td>
<td>• Example: Using AS Path Regular Expressions</td>
</tr>
<tr>
<td></td>
<td>• dynamic-db on page 4235</td>
</tr>
</tbody>
</table>
as-path-group

Syntax

```
as-path-group group-name {
  as-path name regular-expression;
}
```

Hierarchy Level

[edit dynamic policy-options],
[edit logical-systems logical-system-name policy-options],
[edit policy-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for dynamic database configuration introduced in Junos OS Release 9.5.
Support for dynamic database configuration introduced in Junos OS Release 9.5 for EX Series switches.

Description

Define a group containing multiple AS path regular expressions for use in a routing policy match condition.

Options

- `group-name`—Name that identifies the AS path group. One or more AS path regular expressions must be listed below the `as-path-group` hierarchy.

- `name`—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").

- `regular-expression`—One or more regular expressions used to match the AS path.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- Understanding AS Path Regular Expressions for Use as Routing Policy Match Conditions
- dynamic-db on page 4235
bandwidth-limit

**Syntax**

bandwidth-limit bps;

**Hierarchy Level**

[edit firewall policer policer-name if-exceeding]
[edit logical-systems logical-system-name firewall policer policer-name if-exceeding]

**Release Information**

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Logical systems support introduced in Junos OS Release 9.3.

**Description**

Specify the traffic rate in bits per second.

**Options**

**bps** — Traffic rate to be specified in bits per second. Specify **bps** as a decimal value or as a decimal number followed by one of the following abbreviations:

- k (thousand)
- m (million)
- g (billion, which is also called a thousand million)

**Range:**

- 1000 (1k) through 102,300,000,000 (102.3g) bps (EX Series switches)
- 8000 (8k) through 40,000,000,000 (40g) bps (routers)

**Required Privilege Level**

firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Understanding the Use of Policers in Firewall Filters on page 4155
- *Basic Single-Rate Two-Color Policers*
### burst-size-limit

**Syntax**

`burst-size-limit bytes;`

**Hierarchy Level**

- [edit firewall policer policer-name if-exceeding]
- [edit logical-systems logical-system-name firewall policer policer-name if-exceeding]

**Release Information**

- Statement introduced before Junos OS Release 7.4.
- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Logical systems support introduced in Junos OS Release 9.3.

**Description**

Specify the maximum allowed burst size to control the amount of traffic bursting.

**Options**

- `bytes` — Decimal value or a decimal number followed by k (thousand) or m (million).

**Range:**

- 1 through 2,147,450,880 bytes (EX Series switches)
- 1500 through 1,000,000,000,000 bytes (routers)

**Required Privilege Level**

- firewall—To view this statement in the configuration.
- firewall-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Understanding the Use of Policers in Firewall Filters on page 4155
- *Basic Single-Rate Two-Color Policers*
color-aware

Syntax

Color-aware;

Hierarchy Level

[edit firewall three-color-policer policer-name single-rate]
[edit firewall three-color-policer policer-name two-rate]

Release Information

Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description

Configure the way preclassified packets are metered. In color-aware mode, the local switch can assign a higher packet loss priority but cannot assign a lower packet loss priority.

Default

If you omit the color-aware statement, the default behavior is color-aware mode.

Required Privilege Level

firewall—to view this statement in the configuration.
firwall-control—to add this statement to the configuration.

Related Documentation

• Configuring Tricolor Marking Policers on page 4215

color-blind

Syntax

Color-blind;

Hierarchy Level

[edit firewall three-color-policer policer-name single-rate]
[edit firewall three-color-policer policer-name two-rate]

Release Information

Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description

Configure the way preclassified packets are metered. In color-blind mode, the local switch ignores the preclassification of packets and can assign a higher or lower packet loss priority.

Default

If you omit the color-blind statement, the default behavior is color-aware mode.

Required Privilege Level

firewall—to view this statement in the configuration.
firwall-control—to add this statement to the configuration.

Related Documentation

• Configuring Tricolor Marking Policers on page 4215
committed-burst-size

Syntax
committed-burst-size bytes;

Hierarchy Level
[edit firewall three-color-policer policer-name single-rate],
[edit firewall three-color-policer policer-name two-rate]

Release Information
Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description
Configure the maximum number of bytes allowed for incoming packets to burst above
the committed information rate (CIR) and still be marked with low packet loss priority
(green).

NOTE: When you include the committed-burst-size statement in the
configuration, you must also include the committed-information-rate
statement at the same hierarchy level.

Options
bytes—Number of bytes. You can specify a value in bytes either as a complete decimal
number or as a decimal number followed by the abbreviation k (1000),
m (1,000,000), or g (1,000,000,000).
Range: 1500 through 100,000,000,000 bytes

Required Privilege Level
firewall—to view this statement in the configuration.
firewall-control—to add this statement to the configuration.

Related Documentation
• Configuring Tricolor Marking Policers on page 4215
committed-information-rate

Syntax  
committed-information-rate bps;

Hierarchy Level  
[edit firewall three-color-policer policer-name single-rate],  
[edit firewall three-color-policer policer-name two-rate]

Release Information  
Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description  
Configure the guaranteed bandwidth under normal line conditions and the average rate up to which packets are marked with low packet loss priority (green).

NOTE: When you include the committed-information-rate statement in the configuration, you must also include the committed-burst-size statement at the same hierarchy level.

Options  
**bps**—Number of bits per second. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

Range: 32,000 through 40,000,000,000 bps

Required Privilege Level  
firewall—To view this statement in the configuration.

firewall-control—To add this statement to the configuration.

Related Documentation  
• Configuring Tricolor Marking Policers on page 4215
community (Policy Options)

Syntax

```
community name {
  invert-match;
  members [community-ids];
}
```

Hierarchy Level

[edit dynamic policy-options],
[edit logical-systems logical-system-name policy-options],
[edit policy-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.

Description

Define a community or extended community for use in a routing policy match condition.

Options

- **name**—Name that identifies the regular expression. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters. To include spaces in the name, enclose it in quotation marks (" ").
- **invert-match**—Invert the results of the community expression matching. The community match condition defines a regular expression and if it matches the community attribute of the received prefix, Junos OS returns a TRUE result. If not, Junos OS returns a FALSE result. The invert-match statement makes Junos OS behave to the contrary. If there is a match, Junos OS returns a FALSE result. If there is no match, Junos OS returns a TRUE result.
- **members community-ids**—One or more community members. If you specify more than one member, you must enclose all members in brackets.

The format for **community-ids** is:

```
as-number:community-value
```

- **as-number** is the AS number and can be a value in the range from 0 through 65,535.
- **community-value** is the community identifier and can be a number in the range from 0 through 65,535.

You also can specify **community-ids** for communities as one of the following well-known community names, which are defined in RFC 1997, BGP Communities Attribute:

- **no-export**—Routes containing this community name are not advertised outside a BGP confederation boundary.
- **no-advertise**—Routes containing this community name are not advertised to other BGP peers.
- **no-export-subconfed**—Routes containing this community name are not advertised to external BGP peers, including peers in other members' ASs inside a BGP confederation.
You can explicitly exclude BGP community information with a static route using the `none` option. Include `none` when configuring an individual route in the `route` portion of the `static` statement to override a `community` option specified in the `defaults` portion of the statement.

The format for extended `community-ids` is the following:

```
type:administrator:assigned-number
```

`type` is the type of extended community and can be either a `bandwidth`, `target`, `origin`, `domain-id`, `src-as`, or `rt-import` community or a 16-bit number that identifies a specific BGP extended community. The `target` community identifies the destination to which the route is going. The `origin` community identifies where the route originated. The `domain-id` community identifies the OSPF domain from which the route originated. The `src-as` community identifies the autonomous system from which the route originated. The `rt-import` community identifies the route to install in the routing table.

**NOTE:** For `src-as`, you can specify only an AS number and not an IP address. For `rt-import`, you can specify only an IP address and not an AS number.

`administrator` is the administrator. It is either an AS number or an IPv4 address prefix, depending on the type of extended community.

`assigned-number` identifies the local provider.

The format for linking a bandwidth with an AS number is:

```
bandwidth:as-number:bandwidth
```

`as-number` specifies the AS number and `bandwidth` specifies the bandwidth in bytes per second.

**NOTE:** In Junos OS Release 9.1 and later, you can specify 4-byte AS numbers as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*, as well as the 2-byte AS numbers that are supported in earlier releases of the Junos OS. In plain-number format, you can configure a value in the range from 1 through 4,294,967,295. To configure a target or origin extended community that includes a 4-byte AS number in the plain-number format, append the letter “L” to the end of number. For example, a target community with the 4-byte AS number 334,324 and an assigned number of 132 is represented as `target:334324L:132`.

In Junos OS Release 9.2 and later, you can also use AS-dot notation when defining a 4-byte AS number for the target and origin extended communities. Specify two integers joined by a period: `16-bit high-order value in decimal.16-bit low-order value in decimal`. For example, the 4-byte AS number represented in plain-number format as 65546 is represented in AS-dot notation as `1.10`.

---

**Copyright © 2013, Juniper Networks, Inc.**

4231
Required Privilege
Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related
Documentation

• Understanding BGP Communities and Extended Communities as Routing Policy Match Conditions
• Understanding How to Define BGP Communities and Extended Communities
• dynamic-db on page 4235
**condition**

**Syntax**

```
condition condition-name {
  dynamic-db;
  if-route-exists{
    address;
    address-family {
      inet {
        address;
        table table-name;
      }
      ccc {
        interface-name;
        standby;
        peer-unit unit-number;
        table table-name;
      }
    }
    table table-name;
  }
}
```

**Hierarchy Level**

[edit dynamic policy-options],
[edit logical-systems logical-system-name policy-options],
[edit policy-options]

**Release Information**

Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
Support for the address families introduced in Junos OS Release 13.2.

**Description**

Define a policy condition based on the existence of routes in specific tables for use in BGP export policies.

**Options**

`condition-name`—Name of the condition.

The remaining statements are explained separately.

**Required Privilege Level**

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**

- Understanding Conditional Installation of Prefixes in a Routing Table
- Example: Configuring Pseudowire Redundancy for Mobile Backhaul Scenarios
- dynamic-db on page 4235
damping (Policy Options)

Syntax

damping name {
    disable;
    half-life minutes;
    max-suppress minutes;
    reuse number;
    suppress number;
}

Hierarchy Level
[edit logical-systems logical-system-name policy-options],
[edit policy-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Define route flap damping properties to set on BGP routes.

Options

disable—Disable damping on a per-prefix basis. Any damping state that is present in the
routing table for a prefix is deleted if damping is disabled.

half-life minutes—Decay half-life. minutes is the interval after which the accumulated
figure-of-merit value is reduced by half if the route remains stable.
Range: 1 through 45
Default: 15 minutes

NOTE: For the half-life, configure a value that is less than the max-suppress. If you do not, the configuration is rejected.

max-suppress minutes—Maximum hold-down time. minutes is the maximum time that
a route can be suppressed no matter how unstable it has been.
Range: 1 through 720
Default: 60 minutes

NOTE: For the max-suppress, configure a value that is greater than the
half-life. If you do not, the configuration is rejected.

name—Name that identifies the set of damping parameters. The name can contain letters,
numbers, and hyphens (-) and can be up to 255 characters long. To include spaces
in the name, enclose it in quotation marks (" ").

reuse number—Reuse threshold. number is the figure-of-merit value below which a
suppressed route can be used again.
Range: 1 through 20,000
Default: 750 (unitless)
**suppress number**—Cutoff (suppression) threshold. `number` is the figure-of-merit value above which a route is suppressed for use or inclusion in advertisements.

**Range:** 1 through 20,000  
**Default:** 3000 (unitless)

**Required Privilege**  
`routing`—To view this statement in the configuration.  
`routing-control`—To add this statement to the configuration.

**Related Documentation**  
- [Configuring BGP Flap Damping Parameters](#)  
- [Example: Configuring Damping Parameters](#)  
- [Example: Configuring BGP Route Flap Damping Based on the MBGP MVPN Address Family](#)

---

**dynamic-db**

**Syntax**

```
dynamic-db;
```

**Hierarchy Level**  
- `[edit logical-systems logical-system-name policy-options as-path path-name]`  
- `[edit logical-systems logical-system-name policy-options as-path-group group-name]`  
- `[edit logical-systems logical-system-name policy-options community community-name]`  
- `[edit logical-systems logical-system-name policy-options condition condition-name]`  
- `[edit logical-systems logical-system-name policy-options policy-statement policy-statement-name]`  
- `[edit logical-systems logical-system-name policy-options prefix-list prefix-list-name]`  
- `[edit policy-options as-path path-name]`  
- `[edit policy-options as-path-group group-name]`  
- `[edit policy-options community community-name]`  
- `[edit policy-options condition condition-name]`  
- `[edit policy-options policy-statement policy-statement-name]`  
- `[edit policy-options prefix-list prefix-list-name]`

**Release Information**  
Statement introduced in Junos OS Release 9.5.  
Statement introduced in Junos OS Release 9.5 for EX Series switches.

**Description**  
Define routing policies and policy objects that reference policies configured in the dynamic database at the `[edit dynamic]` hierarchy level.

**Required Privilege**  
`routing`—To view this statement in the configuration.  
`routing-control-level`—To add this statement to the configuration.

**Related Documentation**  
- [Example: Configuring Dynamic Routing Policies](#)
excess-burst-size

**Syntax**  
excess-burst-size bytes;

**Hierarchy Level**  
[edit firewall three-color-policer policer-name single-rate]

**Release Information**  
Statement introduced in Junos OS Release 11.2 for EX Series switches.

**Description**  
Configure the maximum number of bytes allowed for incoming packets to burst above the committed information rate and still be marked with medium-high packet loss priority (yellow). Packets that exceed the excess burst size (EBS) are marked with high packet loss priority (red).

---

**NOTE:** When you include the excess-burst-size statement in the configuration, you must also include the committed-burst-size and committed-information-rate statements at the same hierarchy level.

---

**Options**

- **bytes**—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).
  
**Range:** 1500 through 100,000,000,000 bytes

**Required Privilege Level**

- firewall—To view this statement in the configuration.
- firewall-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Tricolor Marking Policers on page 4215
family (Firewall Filter)

Syntax

family family-name {
  filter filter-name {
    interface-specific;
    term term-name {
      from {
        match-conditions;
      }
      then {
        action;
        action-modifiers;
      }
    }
  }
}

Hierarchy Level
[edit firewall]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Option interface-specific introduced in Junos OS Release 9.5 for EX Series switches.

Description
Configure a firewall filter for IP version 4 or IP version 6.

Options

family-name—Version or type of addressing protocol:
  • any—Filter packets based on protocol-independent match conditions.
  • ethernet-switching—Filter Layer 2 (Ethernet) packets and Layer 3 (IP) packets.
  • inet—Filter IPv4 packets.
  • inet6—Filter IPv6 packets.

The remaining statements are explained separately.

Required Privilege
interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
  • Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
  • Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
  • Configuring Firewall Filters (CLI Procedure) on page 4192
  • Configuring Firewall Filters (J-Web Procedure) on page 4201
  • Firewall Filters for EX Series Switches Overview on page 4088
**filter (Firewall Filters)**

**Syntax**

```plaintext
filter filter-name {
    interface-specific;
    term term-name {
        from {
            match-conditions;
        }
        then {
            action;
            action-modifiers;
        }
    }
}
```

**Hierarchy Level**

```
[edit firewall family family-name]
```

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Option `interface-specific` introduced in Junos OS Release 9.5 for EX Series switches.

**Description**

Configure firewall filters.

**Options**

`filter-name`—Name that identifies the filter. The name can contain letters, numbers, and hyphens (`-`), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks.

The remaining statements are explained separately.

**Required Privilege**

- firewall—To view this statement in the configuration.
- firewall-control—To add this statement to the configuration.

**Related Documentation**

- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Firewall Filters for EX Series Switches Overview on page 4088
filter (VLANs)

Syntax
filter (input | output) filter-name;

Hierarchy Level [edit vlans vlan-name]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Apply a firewall filter to traffic coming into or exiting from the VLAN.

Default All incoming traffic is accepted unmodified to the VLAN, and all outgoing traffic is sent unmodified from the VLAN.

Options
- filter-name —Name of a firewall filter defined in a filter statement.
  - input—Apply a firewall filter to VLAN ingress traffic.
  - output—Apply a firewall filter to VLAN egress traffic.

Required Privilege
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Firewall Filters for EX Series Switches Overview on page 4088
- Configuring VLANs for EX Series Switches (CLI Procedure) on page 2119
### filter-specific

<table>
<thead>
<tr>
<th><strong>Syntax</strong></th>
<th>filter-specific;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hierarchy Level</strong></td>
<td>[edit firewall policer policer-name]</td>
</tr>
<tr>
<td><strong>Release Information</strong></td>
<td>Statement introduced in Junos OS Release 9.5 for EX Series switches.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Configure a policer to act as a filter-specific policer. If you do not specify the <code>filter-specific</code> statement, the policer acts as a term-specific policer by default.</td>
</tr>
<tr>
<td><strong>Required Privilege Level</strong></td>
<td>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration</td>
</tr>
</tbody>
</table>
| **Related Documentation** | - Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161  
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206  
- Understanding the Use of Policers in Firewall Filters on page 4155 |
firewall

Syntax

```
firewall {  
  family family-name {  
    filter filter-name {  
      interface-specific;  
      term term-name {  
        from {  
          match-conditions;  
        }  
        then {  
          action;  
          action-modifiers;  
        }  
      }  
    }  
  }  
  policer policer-name {  
    filter-specific;  
    if-exceeding {  
      bandwidth-limit bps;  
      burst-size-limit bytes;  
    }  
    then {  
      policer-action;  
    }  
  }  
}  
```

three-color-policer policer-name {  
  action {  
    loss-priority high then discard;  
  }  
  single-rate {  
    (color-aware | color-blind);  
    committed-information-rate bps;  
    committed-burst-size bytes;  
    excess-burst-size bytes;  
  }  
  two-rate {  
    (color-aware | color-blind);  
    committed-information-rate bps;  
    committed-burst-size bytes;  
    peak-information-rate bps;  
    peak-burst-size bytes;  
  }  
}

Hierarchy Level [edit]

Configure firewall filters and policers.

The remaining statements are explained separately.

**Required Privilege**
- firewall—to view this statement in the configuration.
- firewall-control—to add this statement to the configuration.

**Related Documentation**
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Firewall Filters for EX Series Switches Overview on page 4088

**Syntax**
```plaintext
from {
    match-conditions;
}
```

**Hierarchy Level**
```
[edit firewall family family-name filter filter-name term term-name]
```

**Description**
Match packet fields to values specified in a match condition. If the `from` statement is not included in a firewall filter configuration, all packets are considered to match and the actions and action modifiers in the `then` statement are taken.

**Options**
- `match-conditions`—Conditions that define the values or fields that the incoming or outgoing packets must contain for a match. You can specify one or more match conditions. If you specify more than one, they all must match for a match to occur and for the action in the `then` statement to be taken.

**Required Privilege**
- firewall—to view this statement in the configuration.
- firewall-control—to add this statement to the configuration.

**Related Documentation**
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Understanding Firewall Filter Match Conditions on page 4151
if-exceeding

Syntax

if-exceeding {
bandwidth-limit bps;
bandwidth-percent percent
burst-size-limit bytes;
}

Hierarchy Level
[edit firewall policer policer-name]
[edit logical-systems logical-system-name firewall policer policer-name]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Logical systems support introduced in Junos OS Release 9.3.

Description
Configure policer rate limits.

The bandwidth-percent statement is supported on routers only.

The remaining statements are explained separately.

Required Privilege Level
- firewall—To view this statement in the configuration.
- firewall-control—To add this statement to the configuration.

Related Documentation
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Understanding the Use of Policers in Firewall Filters on page 4155
- Basic Single-Rate Two-Color Policers
### interface-specific

**Syntax**  
interface-specific;

**Hierarchy Level**  
[edit firewall family *family-name* filter *filter-name*]

**Release Information**  
Statement introduced in Junos OS Release 9.5 for EX Series switches.

**Description**  
Configure firewall counters that are interface-specific. You can configure an interface-specific firewall filter only on a port or a Layer 3 interface as an interface-specific firewall filter is not supported for a VLAN.

**Required Privilege Level**  
- *interface*—To view this statement in the configuration.
- *interface-control*—To add this statement to the configuration.

**Related Documentation**  
- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Firewall Filters for EX Series Switches Overview on page 4088

### loss-priority high then discard (Three-Color Policier)

**Syntax**  
loss-priority high then discard;

**Hierarchy Level**  
[edit firewall three-color-policer *policer-name* action]

**Release Information**  
Statement introduced in Junos OS Release 11.2 for EX Series switches.

**Description**  
For packets with high loss priority, discard the packets. The loss priority setting is implicit and cannot be configured. Include this statement if you do not want the local switch to forward packets that have high packet loss priority.

For single-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the committed information rate and the excess burst size.

For two-rate three-color policers, Junos OS assigns high loss priority to packets that exceed the peak information rate and the peak burst size.

**Required Privilege Level**  
- *firewall*—To view this statement in the configuration.
- *firewall-control*—To add this statement to the configuration.

**Related Documentation**  
- Configuring Tricolor Marking Policers on page 4215
peak-burst-size

Syntax  peak-burst-size bytes;

Hierarchy Level  [edit firewall three-color-policer policer-name two-rate]

Release Information  Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description  Configure the maximum number of bytes allowed for incoming packets to burst above the peak information rate (PIR) and still be marked with medium-high packet loss priority (yellow). Packets that exceed the peak burst size (PBS) are marked with high packet loss priority (red).

NOTE: When you include the peak-burst-size statement in the configuration, you must also include the committed-burst-size and peak-information-rate statements at the same hierarchy level.

Options  bytes—Number of bytes. You can specify a value in bytes either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).
Range: 1500 through 100,000,000,000 bytes

Required Privilege Level  firewall—To view this statement in the configuration.
firewall-control—To add this statement to the configuration.

Related Documentation  • Configuring Tricolor Marking Policers on page 4215
The `policer` command in Junos OS is used to configure policer rate limits and actions. To activate a policer, you must include the `policer` action modifier in the `then` statement in a firewall filter term. For EX8200 switches, configure a policer and associate it with a global management counter using the `counter` option.

### Syntax
```
policer policer-name {
  counter {
    counter-id counter-index;
  }
  filter-specific;
  if-exceeding {
    bandwidth-limit bps;
    bandwidth-percent percent
    burst-size-limit bytes;
  }
  then {
    policer-action;
  }
}
```

### Hierarchy Level
```
[edit firewall],
[edit logical-systems logical-system-name firewall]
```

### Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Logical systems support introduced in Junos OS Release 9.3.

### Description
Configure policer rate limits and actions. To activate a policer, you must include the `policer` action modifier in the `then` statement in a firewall filter term. Except for EX8200 switches, each policer that you configure includes an implicit counter. To obtain term-specific packet counts, configure a policer for each term in the filter that requires policing. For EX8200 switches, configure a policer and associate it with a global management counter using the `counter` option.

### Options
- `policer-name`: Name that identifies the policer. The name can include letters, numbers, hyphens (-), and can contain up to 64 characters.

The remaining statements are explained separately.

### Required Privilege Level
- `firewall`: To view this statement in the configuration.
- `firewall-control`: To add this statement to the configuration.

### Related Documentation
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Configuring CoS on EX Series Switches on page 1895
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Configuring MPLS on Provider Edge Switches Using Circuit Cross-Connect (CLI Procedure)
- Configuring MPLS on Provider Edge Switches Using IP Over MPLS (CLI Procedure)
- Understanding the Use of Policers in Firewall Filters on page 4155
- Basic Single-Rate Two-Color Policers
policy-statement

Syntax

```
policy-statement policy-name {
  term term-name {
    from {
      family family-name;
      match-conditions;
      policy subroutine-policy-name;
      prefix-list prefix-list-name;
      prefix-list-filter prefix-list-name match-type <actions>;
      route-filter destination-prefix match-type <actions>;
      source-address-filter source-prefix match-type <actions>;
    }
    to {
      match-conditions;
      policy subroutine-policy-name;
    }
    then actions;
  }
}
```

Hierarchy Level

[edit dynamic policy-options],
[edit logical-systems logical-system-name policy-options],
[edit policy-options]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
inet-mdt option introduced in Junos OS Release 10.0R2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
route-target option introduced in Junos OS Release 12.2.

Description

Define a routing policy, including subroutine policies.

A term is a named structure in which match conditions and actions are defined. Routing policies are made up of one or more terms. Each routing policy term is identified by a term name. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose the entire name in double quotation marks.

Each term contains a set of match conditions and a set of actions:

- Match conditions are criteria that a route must match before the actions can be applied. If a route matches all criteria, one or more actions are applied to the route.
- Actions specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

Generally, a router compares a route against the match conditions of each term in a routing policy, starting with the first and moving through the terms in the order in which they are defined, until a match is made and an explicitly configured or default action of
accept or reject is taken. If none of the terms in the policy match the route, the router compares the route against the next policy, and so on, until either an action is taken or the default policy is evaluated.

If none of the match conditions of each term evaluates to true, the final action is executed. The final action is defined in an unnamed term. Additionally, you can define a default action (either accept or reject) that overrides any action intrinsic to the protocol.

The order of match conditions in a term is not relevant, because a route must match all match conditions in a term for an action to be taken.

To list the routing policies under the [edit policy-options] hierarchy level by policy-statement policy-name in alphabetical order, enter the show policy-options configuration command.
Options  

**actions**—(Optional) One or more actions to take if the conditions match. The actions are described in Configuring Flow Control Actions.

**family family-name**—(Optional) Specify an address family protocol. Specify **inet** for IPv4. Specify **inet6** for 128-bit IPv6, and to enable interpretation of IPv6 router filter addresses. For IS-IS traffic, specify **iso**. For IPv4 multicast VPN traffic, specify **inet-mvpn**. For IPv6 multicast VPN traffic, specify **inet6-mvpn**. For multicast-distribution-tree (MDT) IPv4 traffic, specify **inet-mdt**. For BGP route target VPN traffic, specify **route-target**.

---

**NOTE:** When family is not specified, the routing device or routing instance uses the address family or families carried by BGP. If multiprotocol BGP (MP-BGP) is enabled, the policy defaults to the protocol family or families carried in the network layer reachability information (NLRI) as configured in the family statement for BGP. If MP-BGP is not enabled, the policy uses the default BGP address family unicast IPv4.

**from**—(Optional) Match a route based on its source address.

**match-conditions**—(Optional in from statement; required in to statement) One or more conditions to use to make a match. The qualifiers are described in Routing Policy Match Conditions.

**policy subroutine-policy-name**—Use another policy as a match condition within this policy. The name identifying the subroutine policy can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" "). Policy names cannot take the form __.*-internal__, as this form is reserved. For information about how to configure subroutines, see Understanding Policy Subroutines in Routing Policy Match Conditions.

**policy-name**—Name that identifies the policy. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose it in quotation marks (" ").

**prefix-list prefix-list-name** —Name of a list of IPv4 or IPv6 prefixes.

**prefix-list-filter prefix-list-name**—Name of a prefix list to evaluate using qualifiers; **match-type** is the type of match (see Configuring Prefix List Filters), and **actions** is the action to take if the prefixes match.

**route-filter destination-prefix match-type <actions>**—(Optional) List of routes on which to perform an immediate match; **destination-prefix** is the IPv4 or IPv6 route prefix to match, **match-type** is the type of match (see Configuring Route Lists), and **actions** is the action to take if the destination-prefix matches.

**source-address-filter source-prefix match-type <actions>**—(Optional) Unicast source addresses in multiprotocol BGP (MBGP) and Multicast Source Discovery Protocol (MSDP) environments on which to perform an immediate match. **source-prefix** is
the IPv4 or IPv6 route prefix to match, **match-type** is the type of match (see Configuring Route Lists), and **actions** is the action to take if the **source-prefix** matches.

**term term-name**—Name that identifies the term. The term name must be unique in the policy. It can contain letters, numbers, and hyphens ( - ) and can be up to 64 characters long. To include spaces in the name, enclose the entire name in quotation marks (" "). A policy statement can include multiple terms. We recommend that you name all terms. However, you do have the option to include an unnamed term which must be the final term in the policy. To configure an unnamed term, omit the **term** statement when defining match conditions and actions.

to—(Optional) Match a route based on its destination address or the protocols into which the route is being advertised.

then—(Optional) Actions to take on matching routes. The actions are described in Configuring Flow Control Actions and Configuring Actions That Manipulate Route Characteristics.

**Required Privilege**  
**Level**  
*routing*—To view this statement in the configuration.  
*routing-control*—To add this statement to the configuration.

**Related Documentation**  
- [dynamic-db on page 4235](#)
prefix-list

Syntax
prefix-list name {
  ip-addresses;
  apply-path path;
}

Hierarchy Level
[edit dynamic policy-options],
[edit logical-systems logical-system-name policy-options],
[edit policy-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5.
Support for configuration in the dynamic database introduced in Junos OS Release 9.5 for EX Series switches.
Support for the vpls protocol family introduced in Junos OS Release 10.2.
Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description
Define a list of IPv4 or IPv6 address prefixes for use in a routing policy statement or firewall filter statement.

You can configure up to 85,325 prefixes in each prefix list. To configure more than 85,325 prefixes, configure multiple prefix lists and apply them to multiple firewall filter terms.

Options
name—Name that identifies the list of IPv4 or IPv6 address prefixes.

ip-addresses—List of IPv4 or IPv6 address prefixes, one IP address per line in the configuration.

The remaining statement is explained separately.

Required Privilege Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
• Understanding Prefix Lists for Use in Routing Policy Match Conditions
• Firewall Filter Match Conditions Based on Address Fields
• Example: Configuring Routing Policy Prefix Lists
• Example: Configuring a Filter to Limit TCP Access to a Port Based On a Prefix List
routing-instance

Syntax  routing-instance routing-instance-name:

Hierarchy Level  [edit firewall family inet filter filter-name term term-name then]

Release Information  Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description  Specify a specific virtual routing instance to which the switch sends matched packets.

Options  routing-instance-name—Name of a virtual routing instance.

Required Privilege  firewall—To view this statement in the configuration.

Level  firewall-control—To add this statement to the configuration.

Related Documentation
  • Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183
  • Configuring Virtual Routing Instances (CLI Procedure) on page 2125
  • Understanding Filter-Based Forwarding for EX Series Switches on page 4158
## single-rate

**Syntax**

```
single-rate {
  (color-aware | color-blind);
  committed-burst-size bytes;
  committed-information-rate bps;
  excess-burst-size bytes;
}
```

**Hierarchy Level**

[edit firewall three-color-policer policer-name]

**Release Information**

Statement introduced in Junos OS Release 11.2 for EX Series switches.

**Description**

Configure a single-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), and excess burst size (EBS).

Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the CIR and the CBS but do not exceed the EBS are assigned medium-high loss priority (yellow). Packets that exceed the EBS are assigned high loss priority (red).

Green and yellow packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.

The remaining statements are explained separately.

**Required Privilege Level**

- firewall—To view this statement in the configuration.
- firewall-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Tricolor Marking Policers on page 4215
term

Syntax

```
term term-name {
    from {
        match-conditions;
    }
    then {
        action;
        action-modifiers;
    }
}
```

Hierarchy Level
[edit firewall family family-name filter filter-name]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
Define a firewall filter term.

Options

*term-name*—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks.

The remaining statements are explained separately.

Required Privilege

- **Level**
  - firewall—To view this statement in the configuration.
  - firewall-control—To add this statement to the configuration.

Related Documentation

- [Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches](page 4096)
- [Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches](page 4161)
- [Configuring Firewall Filters (CLI Procedure)](page 4192)
- [Configuring Firewall Filters (J-Web Procedure)](page 4201)
- [Firewall Filters for EX Series Switches Overview](page 4088)
then (Firewall Filters)

Syntax

```
then {
  action;
  action-modifiers;
}
```

Hierarchy Level

```
[edit firewall family family-name filter filter-name term term-name]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure a filter action.

Options

- `action`—Action to accept, discard, or forward packets that match all match conditions specified in a filter term.
- `action-modifiers`—Additional actions to analyze, classify, count, or police packets that match all conditions specified in a filter term.

Required Privilege

- `firewall`—To view this statement in the configuration.
- `firewall-control`—To add this statement to the configuration.

Related Documentation

- Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches on page 4096
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Example: Using Filter-Based Forwarding to Route Application Traffic to a Security Device on EX Series Switches on page 4183
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Understanding Firewall Filter Match Conditions on page 4151
**then (Policer Action)**

**Syntax**
```
then {
  policer-action;
}
```

**Hierarchy Level**
```
[edit firewall policer policer-name]
[edit logical-systems logical-system-name firewall policer policer-name]
```

**Release Information**
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure a policer action.

**Options**
`policer-action`—Actions to take are:
- `discard`—Discard traffic that exceeds the rate limits defined by the policer.
- `forwarding-class class-name`—For routers only, classify traffic that exceeds the rate limits defined by the policer.
- `loss-priority`—Set the loss priority for traffic that exceeds the rate limits defined by the policer.

**Required Privilege**
- `firewall`—To view this statement in the configuration.
- `firewall-control`—To add this statement to the configuration.

**Related Documentation**
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Understanding the Use of Policers in Firewall Filters on page 4155
- Example: Configuring CoS for a PBB Network on MX Series Routers
- Basic Single-Rate Two-Color Policers
three-color-policer (Configuring)

Syntax

three-color-policer {policer-name} {
  action {
    loss-priority high then discard;
  }
  single-rate {
    (color-aware | color-blind);
    committed-burst-size bytes;
    committed-information-rate bps;
    excess-burst-size bytes;
  }
  two-rate {
    (color-aware | color-blind);
    committed-burst-size bytes;
    committed-information-rate bps;
    peak-burst-size bytes;
    peak-information-rate bps;
  }
}

Hierarchy Level  [edit firewall]

Release Information  Statement introduced in Junos OS Release 11.2 for EX Series switches.

Description  Configure a three-color policer.

Options  

policer-name—Name of the three-color policer. Reference this name when you apply the policer to an interface.

The remaining statements are explained separately.

Required Privilege Level

firewall—To view this statement in the configuration.

firewall-control—To add this statement to the configuration.

Related Documentation

• Configuring Tricolor Marking Policers on page 4215
**two-rate**

**Syntax**
```
two-rate {
    (color-aware | color-blind);
    committed-burst-size bytes;
    committed-information-rate bps;
    peak-burst-size bytes;
    peak-information-rate bps;
}
```

**Hierarchy Level**
```
[edit firewall three-color-policer policer-name].
```

**Release Information**
Statement introduced in Junos OS Release 11.2 for EX Series switches.

**Description**
Configure a two-rate three-color policer in which marking is based on the committed information rate (CIR), committed burst size (CBS), peak information rate (PIR), and peak burst size (PBS).

Packets that conform to the CIR or the CBS are assigned low loss priority (green). Packets that exceed the PIR and the PBS are assigned high loss priority (red).

Green packets are always forwarded; this action is not configurable. You can configure red packets to be discarded. By default, red packets are forwarded.

The remaining statements are explained separately.

**Required Privilege**
- firewall—To view this statement in the configuration.
- firewall-control—To add this statement to the configuration.

**Related Documentation**
- Configuring Tricolor Marking Policers on page 4215
CHAPTER 79
Administration

- Routine Monitoring on page 4259
- Operational Commands on page 4262

Routine Monitoring

- Verifying That Firewall Filters Are Operational on page 4259
- Verifying That Policers Are Operational on page 4260
- Monitoring Firewall Filter Traffic on page 4261

Verifying That Firewall Filters Are Operational

**Purpose**
After you configure and apply firewall filters to ports, VLANs, or Layer 3 interfaces, you can perform the following task to verify that the firewall filters configured on EX Series switches are working properly.

**Action**
Use the operational mode command to verify that the firewall filters on the switch are working properly:

```
user@switch> show firewall
```

<table>
<thead>
<tr>
<th>Filter: egress-vlan-watch-employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counters:</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>counter-employee-web</td>
</tr>
</tbody>
</table>

```
Filter: ingress-port-voip-class-limit-tcp-icmp
```

| Counters:                         |
| Name                              | Bytes | Packets |
| icmp-counter                      | 0     | 0        |

**Policers:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-connection-policer</td>
<td>0</td>
</tr>
<tr>
<td>tcp-connection-policer</td>
<td>0</td>
</tr>
</tbody>
</table>

```
Filter: ingress-vlan-rogue-block
```

**Meaning**
The `show firewall` command displays the names of all firewall filters, policers, and counters that are configured on the switch. For each counter that is specified in a filter configuration, the output field shows the byte count and packet count for the term in which the counter is specified. For each policer that is specified in a filter configuration, the output field shows the packet count for packets that exceed the specified rate limits.
Verifying That Policers Are Operational

Purpose: After you configure policers and include them in firewall filter configurations, you can perform the following tasks to verify that the policers configured on EX Series switches are working properly.

Action: Use the operational mode command to verify that the policers on the switch are working properly:

```
user@switch> show policer
Filter: egress-vlan-watch-employee
Filter: ingress-port-filter
Filter: ingress-port-voip-class-limit-tcp-icmp
Policers:
Name                                              Packets
icmp-connection-policer                                 0
tcp-connection-policer                                  0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

Meaning: The `show policer` command displays the names of all firewall filters and policers that are configured on the switch. For each policer that is specified in a filter configuration, the output field shows the current packet count for all packets that exceed the specified rate limits.

Related Documentation:
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Monitoring Firewall Filter Traffic on page 4261
Monitoring Firewall Filter Traffic

You can monitor firewall filter traffic on EX Series switches.

- Monitoring Traffic for All Firewall Filters and Policers That Are Configured on the Switch on page 4261
- Monitoring Traffic for a Specific Firewall Filter on page 4261
- Monitoring Traffic for a Specific Policer on page 4262

**Monitoring Traffic for All Firewall Filters and Policers That Are Configured on the Switch**

**Purpose**
Perform the following task to monitor the number of packets and bytes that matched the firewall filters and monitor the number of packets that exceeded policer rate limits:

**Action**
Use the operational mode command:

```
user@switch> show firewall
```

```
Filter: egress-vlan-watch-employee
Counters:
  Name                                                  Bytes              Packets
  counter-employee-web                                 3348                   27
Filter: ingress-port-voip-class-limit-tcp-icmp
Counters:
  Name                                                  Bytes              Packets
  icmp-counter                                         4100                   49
Policers:
  Name                                              Packets
  icmp-connection-policer                                 0
  tcp-connection-policer                                  0
Filter: ingress-vlan-rogue-block
Filter: ingress-vlan-limit-guest
```

**Meaning**
The `show firewall` command displays the names of all firewall filters, policers, and counters that are configured on the switch. The output fields show byte and packet counts for counters and packet count for policers.

**Monitoring Traffic for a Specific Firewall Filter**

**Purpose**
Perform the following task to monitor the number of packets and bytes that matched a firewall filter and monitor the number of packets that exceeded the policer rate limits:

**Action**
Use the operational mode command:

```
user@switch> show firewallfilter ingress-vlan-rogue-block
```

```
Filter: ingress-vlan-rogue-block
Counters:
  Name                                                  Bytes              Packets
  rogue-counter                                        2308                   20
```

**Meaning**
The `show firewall filter filter-name` command displays the name of the firewall filter, the packet and byte count for all counters configured with the filter, and the packet count for all policers configured with the filter.
Monitoring Traffic for a Specific Policer

**Purpose**
Perform the following task to monitor the number of packets that exceeded policer rate limits:

**Action**
Use the operational mode command:

```
user@switch> show policer tcp-connection-policer
Filter: ingress-port-voip-class-limit-tcp-icmp
Policers:
  Name                          Packets
  tcp-connection-policer        0
```

**Meaning**
The `show policer policer-name` command displays the name of the firewall filter that specifies the policer-action and displays the number of packets that exceeded rate limits for the specified filter.

**Related Documentation**
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
- Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Verifying That Firewall Filters Are Operational on page 4259

**Operational Commands**
clear firewall

Syntax

```
clear firewall
<all>
<counter counter-name>
<filter filter-name>
<policer counter <all | counter-id counter-index>>
```

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Clear statistics about configured firewall filters.

When you clear the counters of a filter, this not only impacts the counters shown by the CLI, but also the ones tracked by SNMP 2.

Options

- **none**—Clear the packet and byte counts for all firewall filter counters and clear the packet counts for all policer counters.
- **all**—(Optional) Clear the packet and byte counts for all firewall filter counters and clear the packet counts for all policer counters.
- **counter counter-name** —(Optional) Clear the packet and byte counts for the specified firewall filter counter.
- **filter filter-name** —(Optional) Clear the packet and byte counts for the specified firewall filter.
- **policer counter <all | counter-id counter-index>**—(EX8200 switches only) (Optional) Clear policers associated with a specific counter ID. You can also use **policer counter all** to clear all counters. The value of **counter-index** can be 0, 1, or 2.

Required Privilege
Level
```
clear
```

Related Documentation
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Verifying That Firewall Filters Are Operational on page 4259
- Verifying That Policers Are Operational on page 4260
- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding the Use of Policers in Firewall Filters on page 4155

Sample Output
```
clear firewall (all)

user@switch> clear firewall all

clear firewall (counter counter-name)

user@switch> clear firewall counter port-filter-counter
```
clear firewall (filter filter-name)
    user@switch> clear firewall filter ingress-port-filter

clear firewall (policer counter all)
    user@switch# clear firewall policer counter all

clear firewall (policer counter counter-id counter-index)
    user@switch# clear firewall policer counter counter-id 0
clear firewall

Syntax

clear firewall (all | counter counter-name | filter filter-name | log (all | logical-system-name) | logical-system logical-system-name)

Syntax (EX Series Switches)
clear firewall (all | counter counter-name | filter filter-name | log (all | logical-system-name) | policer counter (all | counter-id counter-index))

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
logical-system option introduced in Junos OS Release 9.3.
log option introduced before Junos OS Release 11.4.

Description

Clear statistics about configured firewall filters.

When you clear the counters of a filter, this impacts not only the counters shown by the CLI, but also the ones tracked by SNMP2.

NOTE: The clear firewall command cannot be used to clear the Routing Engine filter counters on a backup Routing Engine that is enabled for graceful Routing Engine switchover (GRES).

If you clear statistics for firewall filters that are applied to Trio-based DPCs and that also use the prefix-action action on matched packets, wait at least 5 seconds before you enter the show firewall prefix-action-stats command. A 5-second pause between issuing the clear firewall and show firewall prefix-action-stats commands avoids a possible timeout of the show firewall prefix-action-stats command.

Options

clear firewall (all | counter counter-name | filter filter-name | log (all | logical-system-name) | logical-system logical-system-name) | logical-system logical-system-name | policer counter (all | counter-id counter-index))

all—Clear the packet and byte counts for all filters. On EX Series switches, this option also clears the packet counts for all policer counters.

counter counter-name—Clear the packet and byte counts for a filter counter that has been configured with the counter firewall filter action.

filter filter-name—Clear the packet and byte counts for the specified firewall filter.

log (all | logical-system-name)—Clear log entries for IPv4 firewall filters that have then log as an action. Use log_all to clear all log entries or log logical-system-name to clear log entries for the specified logical system.

logical-system logical-system-name—Clear the packet and byte counts for the specified logical system.

policer counter (all | counter-id counter-index)—(EX8200 switches only) Clear all policer counters using the policer counter all command, or clear a specific policer counter using the policer counter counter-id counter-index command. The value of counter-index can be 0, 1, or 2.
Required Privilege
Level  clear

Related Documentation
  • show firewall on page 4272

List of Sample Output
  clear firewall all on page 4266
  clear firewall (counter counter-name) on page 4266
  clear firewall (filter filter-name) on page 4266
  clear firewall (policer counter all) (EX8200 Switch) on page 4266
  clear firewall (policer counter counter-id counter-index) (EX8200 Switch) on page 4266

Sample Output
  clear firewall all
    user@host> clear firewall all

  clear firewall (counter counter-name)
    user@host> clear firewall counter port-filter-counter

  clear firewall (filter filter-name)
    user@host> clear firewall filter ingress-port-filter

  clear firewall (policer counter all) (EX8200 Switch)
    user@switch> clear firewall policer counter all

  clear firewall (policer counter counter-id counter-index) (EX8200 Switch)
    user@switch> clear firewall policer counter counter-id 0
show firewall

Syntax

show firewall
<counter counter-name>
<filter filter-name>
<log (detail | interface interface-name)>
<policer counters (<(detail) | counter-id counter-index <detail>)>>
terse

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Option policer counters introduced in Junos OS Release 12.2 for EX Series switches.

Description

Display statistics about configured firewall filters.

Options

none—Display statistics about all configured firewall filters, counters, and policers.

counter counter-name—(Optional) Display statistics about a particular firewall filter counter.

filter filter-name—(Optional) Display statistics about a particular firewall filter.

log (detail | interface interface-name)—(Optional) Display detailed log entries of firewall activity or log information about a specific interface.

policer counters (<detail) | counter-id counter-index <detail>)—(EX8200 switches only)
(Original) Display policer counter statistics in brief or in detail.

terse—(Optional) Display firewall filter names only.

Required Privilege Level

view

Related Documentation

• Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161

• Configuring Policers to Control Traffic Rates (CLI Procedure) on page 4206

• Verifying That Firewall Filters Are Operational on page 4259

• Verifying That Policers Are Operational on page 4260

• Firewall Filters for EX Series Switches Overview on page 4088

• Understanding the Use of Policers in Firewall Filters on page 4155

List of Sample Output

show firewall on page 4269
show firewall (filter filter-name) on page 4269
show firewall (counter counter-name) on page 4269
show firewall log on page 4269
show firewall policer counters (EX8200 Switches Only) on page 4270
show firewall policer counters (detail) (EX8200 Switches Only) on page 4270
show firewall policer counters (counter-id counter-index) (EX8200 Switches only) on page 4270
**Output Fields**

Table 528 on page 4268 lists the output fields for the `show firewall` command. Output fields are listed in the approximate order in which they appear.

### Table 528: `show firewall` Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Filter</strong></td>
<td>Name of the filter that is configured with the <code>filter</code> statement at the <code>[edit firewall]</code> hierarchy level.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Counters</strong></td>
<td>Display filter counter information:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Name—Name of a filter counter that has been configured with the <code>counter</code> firewall filter action</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bytes—Number of bytes that match the filter term where the <code>counter</code> action was specified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packets—Number of packets that matched the filter term where the <code>counter</code> action was specified.</td>
<td></td>
</tr>
<tr>
<td><strong>Policers</strong></td>
<td>Display policer information:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Name—Name of policer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Packets—Number of packets that matched the filter term where the <code>policer</code> action was specified. This is the number of packets that exceed the rate limits that the policer specifies.</td>
<td></td>
</tr>
<tr>
<td><strong>Policer Counters</strong></td>
<td>(EX Series switch only) Global management counter ID. The counter ID value (<code>counter index</code>) can be 0, 1, or 2.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Green</strong></td>
<td>(EX Series switch only) Number of packets within the limits. The number of packets is smaller than the committed information rate (CIR).</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Yellow</strong></td>
<td>(EX Series switch only) Number of packets partially within the limits. The number of packets is greater than the CIR but the burst size is within the excess burst size (EBS) limit.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>discard</strong></td>
<td>(EX Series switch only) Number of discarded packets.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Bytes</strong></td>
<td>(EX Series switch only) Number of green, yellow, red, or discarded packets in bytes.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Packets</strong></td>
<td>(EX Series switch only) Number of green, yellow, red, or discarded packets.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Filter name</strong></td>
<td>(EX Series switch only) Name of the filter with a term associated to a policer.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Term name</strong></td>
<td>(EX Series switch only) Name of the term associated with a policer.</td>
<td>detail</td>
</tr>
<tr>
<td><strong>Policer name</strong></td>
<td>(EX Series switch only) Name of the policer that is associated with a global management counter.</td>
<td>detail</td>
</tr>
</tbody>
</table>
Sample Output

show firewall

```
user@switch> show firewall
Filter: egress-vlan-filter
Counters:
Name Bytes Packets
employee-web-counter 0 0
```

```
Filter: ingress-port-filter
Counters:
Name Bytes Packets
ingress-port-counter 0 0
```

```
Filter: ingress-port-voip-class-filter
Counters:
Name Bytes Packets
icmp-counter 0 0
```

```
Policers:
Name Packets
icmp-connection-policer 0
tcp-connection-policer 0
```

show firewall (filter filter-name)

```
user@switch> show firewall filter egress-vlan-filter
Filter: egress-vlan-filter
Counters:
Name Bytes Packets
employee-web-counter 0 0
```

show firewall (counter counter-name)

```
user@switch> show firewall counter icmp-counter
Filter: ingress-port-voip-class-filter
Counters:
Name Bytes Packets
icmp-counter 0 0
```

show firewall log

```
user@switch> show firewall log
Log :
```
```
Time Filter Action Interface Protocol Src Addr
08:00:53 pfe R ge-1/0/1.0 ICMP 192.168.3.5
08:00:52 pfe R ge-1/0/1.0 ICMP 192.168.3.5
08:00:51 pfe R ge-1/0/1.0 ICMP 192.168.3.5
08:00:50 pfe R ge-1/0/1.0 ICMP 192.168.3.5
08:00:49 pfe R ge-1/0/1.0 ICMP 192.168.3.5
08:00:48 pfe R ge-1/0/1.0 ICMP 192.168.3.5
08:00:47 pfe R ge-1/0/1.0 ICMP 192.168.3.5
```
```
show firewall policer counters (EX8200 Switches Only)

user@switch> show firewall policer counters
Policer Counter Index 0:

Bytes         Packets
Green:        73            15914
Yellow:       9             1962
Discard:      119           25942

Policer Counter Index 1:

Bytes         Packets
Green:        0             0
Yellow:       0             0
Discard:      0             0

Policer Counter Index 2:

Bytes         Packets
Green:        0             0
Yellow:       0             0
Discard:      0             0

show firewall policer counters (detail) (EX8200 Switches Only)

user@switch> show firewall policer counters detail
Policer Counter Index 0:

Bytes         Packets
Green:        73            15914
Yellow:       9             1962
Discard:      119           25942

Filter name    Term name     Policer name
myfilter       polcr-term-1  myfilter-polcr-1
inet-filter-ae ae-snmp       policer-1
inet-filter-ae ae-ssh        policer-2

Policer Counter Index 1:

Bytes         Packets
Green:        0             0
Yellow:       0             0
Discard:      0             0

Filter name    Term name     Policer name

Policer Counter Index 2:

Bytes         Packets
Green:        0             0
Yellow:       0             0
Discard:      0             0

show firewall policer counters (counter-id counter-index) (EX8200 Switches only)

user@switch> show firewall policer counters counter-id 0
Policer Counter Index 0:

Bytes         Packets
Green:        73            15914
Yellow:       9             1962
Discard:      119           25942
show firewall policer counters (counter-id counter-index detail) (EX2800 Switches only)

```
user@switch> show firewall policer counters counter-id 0 detail
Policer Counter Index 0:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green:</td>
<td>73</td>
<td>15914</td>
</tr>
<tr>
<td>Yellow:</td>
<td>9</td>
<td>1962</td>
</tr>
<tr>
<td>Discard:</td>
<td>119</td>
<td>25942</td>
</tr>
</tbody>
</table>

Filter name        Term name       Policer name
myfilter            polcr-term-1    myfilter-polcr-1
inet-filter-ae      ae-snmp         policer-1
inet-filter-ae      ae-ssh          policer-2
```
show firewall

**Syntax**
```
show firewall
<counter counter-name>
<filter filter-name>
<log>
<logical-system (all | logical-system-name)>
<terse>
```

**Syntax (EX Series Switches)**
```
show firewall
<counter counter-name>
<detail>
<filter filter-name>
<log <(detail | interface interface-name)>
<policer counters <(detail | counter-id counter-index <detail>)>
<terse>
```

**Release Information**
- Command introduced before Junos OS Release 7.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- logical-system option introduced in Junos OS Release 9.3.
- terse option introduced in Junos OS Release 9.4.
- policer counters option introduced in Junos OS Release 12.2 for EX Series switches.
- detail option introduced in Junos OS Release 12.3.

**Description**
Display statistics about configured firewall filters.

**Options**
- **none**—(Optional) Display statistics about all configured firewall filters and counters. For EX Series switches, this command also displays statistics about all configured policers.

- **counter counter-name**—(Optional) Name of a filter counter.

- **detail**—(EX Series switches only) (Optional) Display firewall filter statistics with enhanced policer.

- **filter filter-name**—(Optional) Name of a configured filter.

- **logical-system (all | logical-system-name)**—(Optional) Perform this operation on all logical systems or on a particular logical system.

- **log**—(Optional) Display log entries for firewall filters.

- **log <(detail | interface interface-name)>**—(EX Series switches only) (Optional) Display detailed log entries of firewall activity or log information about a specific interface.

- **policer counters <(detail | counter-id counter-index <detail>)>**—(EX8200 switches only) (Optional) Display policer counter statistics in brief or in detail.

- **terse**—(Optional) Display firewall filter names only.

**Required Privilege**
- **Level** view
Related Documentation

- clear firewall on page 4265
- show firewall log on page 4279
- Verifying That Firewall Filters Are Operational on page 4259
- Verifying That Policers Are Operational on page 4260

List of Sample Output

- show firewall filter (MX Series Router and EX Series Switch) on page 4275
- show firewall filter (non MX Series Router and EX Series Switch) on page 4275
- show firewall filter (Hierarchical Policer, MX Series with MPC) on page 4275
- show firewall filter (Dynamic Input Filter) on page 4275
- show firewall (Logical Systems) on page 4275
- show firewall (counter counter-name) on page 4276
- show firewall log on page 4276
- show firewall policer counters (EX8200 Switch) on page 4276
- show firewall policer counters (detail) (EX8200 Switch) on page 4277
- show firewall policer counters (counter-id counter-index) (EX8200 Switch) on page 4277
- show firewall policer counters (counter-id counter-index detail) (EX8200 Switch) on page 4277
- show firewall detail on page 4278

Output Fields

Table 529: show firewall Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Name of a filter that has been configured with the <code>filter</code> statement at the <code>[edit firewall]</code> hierarchy level.</td>
</tr>
<tr>
<td></td>
<td>Except on EX Series switches:</td>
</tr>
<tr>
<td></td>
<td>• When an interface-specific filter is displayed, the name of the filter is followed by the full interface name and by either <code>-i</code> for an input filter or <code>-o</code> for an output filter.</td>
</tr>
<tr>
<td></td>
<td>• When dynamic filters are displayed, the name of the filter is followed by the full interface name and by either <code>-in</code> for an input filter or <code>-out</code> for an output filter. When a logical system–specific filter is displayed, the name of the filter is prefixed with two underscore (<code>_</code>) characters and the name of the logical system (for example, <code>__ls1/filter1</code>).</td>
</tr>
<tr>
<td></td>
<td>• When a service filter is displayed that uses a service set, the separator between the service-set name and the service-filter name is a semicolon (<code>;</code>).</td>
</tr>
<tr>
<td>Counters</td>
<td>Display filter counter information:</td>
</tr>
<tr>
<td></td>
<td>• Name—Name of a filter counter that has been configured with the <code>counter</code> firewall filter action.</td>
</tr>
<tr>
<td></td>
<td>• Bytes—Number of bytes that match the filter term under which the <code>counter</code> action is specified.</td>
</tr>
<tr>
<td></td>
<td>• Packets—Number of packets that matched the filter term under which the <code>counter</code> action is specified.</td>
</tr>
</tbody>
</table>

NOTE: On M and T Series routers, firewall filters cannot count IP-Options packets on a per option type and per interface basis. A limited work around is to use the `show pfe statistics ip options` command to see IP-Options statistics on a per Packet Forwarding Engine (PFE) basis. See `show pfe statistics ip` for sample output.
Display policer information:

- **Name**—Name of policer.
- **Bytes**—(For two-color policers on MX Series routers and EX Series switches, and for hierarchical policers on MS-DPC, MIC, and MPC interfaces on MX Series routers) Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer.
  
  For other combinations of policer type, device, and line card type, this field is blank.
- **Packets**—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policers</td>
<td>Display policer information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—Name of policer.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Bytes</strong>—(For two-color policers on MX Series routers and EX Series switches, and for hierarchical policers on MS-DPC, MIC, and MPC interfaces on MX Series routers) Number of bytes that match the filter term under which the policer action is specified. This is only the number out-of-specification (out-of-spec) byte counts, not all the bytes in all packets policed by the policer. For other combinations of policer type, device, and line card type, this field is blank.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Packets</strong>—Number of packets that matched the filter term under which the policer action is specified. This is only the number of out-of-specification (out-of-spec) packet counts, not all packets policed by the policer.</td>
</tr>
<tr>
<td>Policer Counter Index</td>
<td>(EXB200 switch only) Global management counter ID. The counter ID value (counter-index) can be 0, 1, or 2.</td>
</tr>
<tr>
<td>Green</td>
<td>(EXB200 switch only) Number of packets within the limits. The number of packets is smaller than the committed information rate (CIR).</td>
</tr>
<tr>
<td>Yellow</td>
<td>(EXB200 switch only) Number of packets partially within the limits. The number of packets is greater than the CIR, but the burst size is within the excess burst size (EBS) limit.</td>
</tr>
<tr>
<td>Discard</td>
<td>(EXB200 switch only) Number of discarded packets.</td>
</tr>
<tr>
<td>Bytes</td>
<td>(EXB200 switch only) Number of green, yellow, red, or discarded packets in bytes.</td>
</tr>
<tr>
<td>Packets</td>
<td>(EXB200 switch only) Number of green, yellow, red, or discarded packets.</td>
</tr>
<tr>
<td>Filter name</td>
<td>(EXB200 switch only) Name of the filter with a term associated to a policer.</td>
</tr>
<tr>
<td>Term name</td>
<td>(EXB200 switch only) Name of the term associated with a policer.</td>
</tr>
<tr>
<td>Policer name</td>
<td>(EXB200 switch only) Name of the policer that is associated with a global management counter.</td>
</tr>
</tbody>
</table>
Sample Output

show firewall filter (MX Series Router and EX Series Switch)

```
user@host> show firewall filter test
Filter: test
Counters:
Name                            Bytes             Packets
Counter-1                           0                   0
Counter-2                           0                   0
Policers:
Name                            Bytes             Packets
Policer-1                        2770                  70
```

show firewall filter (non MX Series Router and EX Series Switch)

```
user@host> show firewall filter test
Filter: test
Counters:
Name                            Bytes             Packets
Counter-1                           0                   0
Counter-2                           0                   0
Policers:
Name                            Bytes             Packets
Policer-1                                              70
```

show firewall filter (Hierarchical Policer, MX Series with MPC)

```
user@host> show firewall filter
FL_V4_PHY-HP-EF-AWARE-Gold=400k-MCAST=200k-Total=1M-ds-10/0/0:2:1-i
Filter: FL_V4_PHY-HP-EF-AWARE-Gold=400k-MCAST=200k-Total=1M-ds-10/0/0:2:1-i
Counters:
Name                                                Bytes              Packets
AF1x_counter-ds-10/0/0:2:1-i                            0                    0
AF2x_counter-ds-10/0/0:2:1-i                  25529445976             24500428
AF3x_counter-ds-10/0/0:2:1-i                      2182022                39482
AF4x_counter-ds-10/0/0:2:1-i                            0                    0
BE_counter-ds-10/0/0:2:1-i                              0                    0
EF_counter-ds-10/0/0:2:1-i                    14817044120             12265765
STD_counter-ds-10/0/0:2:1-i                             0                    0
Policers:
Name                                                Bytes              Packets
POL_CE-PE_M=200k-filter-ds-10/0/0:2:1-i        5948099658              5708349
POL_CE-PE_G=400K_R=1M-filter-ds-10/0/0:2:1-i ?????????????              ????????
```

show firewall filter (Dynamic Input Filter)

```
user@host> show firewall filter dfwd-ge-5/0/0.1-in
Filter: dfwd-ge-5/0/0.1-in
Counters:
Name                                                Bytes              Packets
c1-ge-5/0/0.1-in                                        0                    0
```

show firewall (Logical Systems)

```
user@host> show firewall
```
Filter: __lr1/test
Counters:
Name                  Bytes        Packets
icmp                  420          5

Filter: __default_bpdu_filter__
Filter: __lr1/inet_filter1
Counters:
Name                  Bytes        Packets
inet_tcp_count        0            0
inet_udp_count        0            0

Filter: __lr1/inet_filter2
Counters:
Name                  Bytes        Packets
inet_icmp_count       0            0
inet_pim_count        0            0

Filter: __lr2/inet_filter1
Counters:
Name                  Bytes        Packets
inet_tcp_count        0            0
inet_udp_count        0            0

show firewall (counter counter-name)

user@host> show firewall counter icmp-counter
Filter: ingress-port-voip-class-filter
Counters:
Name                  Bytes        Packets
icmp-counter          0            0

show firewall log

user@host> show firewall log
Log:
Time      Filter  Action Interface     Protocol        Src Addr          Dest Addr
08:00:53  pfe     R      ge-1/0/1.0    ICMP            192.168.3.5     192.168.3.4
08:00:52  pfe     R      ge-1/0/1.0    ICMP            192.168.3.5     192.168.3.4
08:00:51  pfe     R      ge-1/0/1.0    ICMP            192.168.3.5     192.168.3.4
08:00:50  pfe     R      ge-1/0/1.0    ICMP            192.168.3.5     192.168.3.4
08:00:49  pfe     R      ge-1/0/1.0    ICMP            192.168.3.5     192.168.3.4
08:00:48  pfe     R      ge-1/0/1.0    ICMP            192.168.3.5     192.168.3.4
08:00:47  pfe     R      ge-1/0/1.0    ICMP            192.168.3.5     192.168.3.4

show firewall policer counters (EX8200 Switch)

user@switch> show firewall policer counters
Policer Counter Index 0:
Green:          Bytes    Packets
                73        15914
Yellow:         9          1962
Discard:        119       25942
Policer Counter Index 1:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Discard</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Policer Counter Index 2:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Discard</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show firewall policer counters (detail) (EX8200 Switch)

```
user@switch> show firewall policer counters detail
Policer Counter Index 0:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>73</td>
<td>15914</td>
</tr>
<tr>
<td>Yellow</td>
<td>9</td>
<td>1962</td>
</tr>
<tr>
<td>Discard</td>
<td>119</td>
<td>25942</td>
</tr>
</tbody>
</table>

Filter name | Term name | Policer name
-------------|-----------|---------------
myfilter     | polcr-term-1 | myfilter-polcr-1
inet-filter-ae | ae-snmp       | policer-1
inet-filter-ae | ae-ssh        | policer-2
```

Policer Counter Index 1:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Discard</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Policer Counter Index 2:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Yellow</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Discard</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show firewall policer counters (counter-id counter-index) (EX8200 Switch)

```
user@switch> show firewall policer counters counter-id 0
Policer Counter Index 0:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>73</td>
<td>15914</td>
</tr>
<tr>
<td>Yellow</td>
<td>9</td>
<td>1962</td>
</tr>
<tr>
<td>Discard</td>
<td>119</td>
<td>25942</td>
</tr>
</tbody>
</table>
```

show firewall policer counters (counter-id counter-index detail) (EX8200 Switch)

```
user@switch> show firewall policer counters counter-id 0 detail
Policer Counter Index 0:

<table>
<thead>
<tr>
<th></th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>73</td>
<td>15914</td>
</tr>
<tr>
<td>Yellow</td>
<td>9</td>
<td>1962</td>
</tr>
<tr>
<td>Discard</td>
<td>119</td>
<td>25942</td>
</tr>
</tbody>
</table>
```

Copyright © 2013, Juniper Networks, Inc.
show firewall detail

user@host> show firewall detail
Filter: __default_bpdu_filter__

Filter: foo
Counters:
Name        Bytes    Packets
cl          17652140  160474

Policers:
Name        Bytes    Packets
P1-t1
  OOS         0        18286
  Offered    0 18446744073709376546
  Transmitted 0 18446744073709358260
**show firewall log**

**Syntax**

```
show firewall log
<detail>
<interface interface-name>
<logical-system (logical-system-name | all)>
```

**Syntax (EX Series Switches)**

```
show firewall log
<detail>
<interface interface-name>
```

**Release Information**

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
logical-system option introduced in Junos OS Release 9.3.

**Description**

Display log information about firewall filters.

**Options**

- `none`—Display log information about firewall filters.
- `detail`—(Optional) Display detailed information.
- `interface interface-name`—(Optional) Display log information about a specific interface.
- `logical-system (logical-system-name | all)`—(Optional) Perform this operation on all logical systems or on a particular system.

**Required Privilege**

view

**List of Sample Output**

- show firewall log on page 4280
- show firewall log detail on page 4280

**Output Fields**

Table 530 on page 4279 lists the output fields for the `show firewall log` command. Output fields are listed in the approximate order in which they appear.

**Table 530: show firewall log Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of Log</td>
<td>Time that the event occurred.</td>
</tr>
<tr>
<td>Filter</td>
<td>• Displays the name of a configured firewall filter or service filter only if the packet hit the filter’s log action in a kernel filter (in the control plane). For any traffic that reaches the Routing Engine, the packets hit the log action in the kernel.</td>
</tr>
<tr>
<td></td>
<td>• For all other logged packets (packet hit the filter’s log action in the Packet Forwarding Engine), this field displays pfe instead of a configured filter name.</td>
</tr>
</tbody>
</table>
### Table 530: show firewall log Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Action</td>
<td>Filter action:</td>
</tr>
<tr>
<td></td>
<td>• A—Accept</td>
</tr>
<tr>
<td></td>
<td>• D—Discard</td>
</tr>
<tr>
<td></td>
<td>• R—Reject</td>
</tr>
<tr>
<td>Name of Interface</td>
<td>• Displays a physical interface name if the packet arrived at a port on a line card.</td>
</tr>
<tr>
<td></td>
<td>• Displays local if the packet was generated by the device's internal Ethernet interface, em1 or fpx1, which connects the Routing Engine with the router’s packet-forwarding components.</td>
</tr>
<tr>
<td>Name of protocol</td>
<td>Packet’s protocol name: egp, gre, icmp, ipip, ospf, pim, rsvp, tcp, or udp.</td>
</tr>
<tr>
<td>Packet length</td>
<td>Length of the packet.</td>
</tr>
<tr>
<td>Source address</td>
<td>Packet’s source address.</td>
</tr>
<tr>
<td>Destination address</td>
<td>Packet’s destination address and port.</td>
</tr>
</tbody>
</table>

### Sample Output

**show firewall log**

```
user@host> show firewall log
Time      Filter    Action Interface     Protocol  Src Addr      Dest Addr
13:10:12  pfe       D      rlsq0.902     ICMP      180.1.177.2   180.1.177.1
13:10:11  pfe       D      rlsq0.902     ICMP      180.1.177.2   180.1.177.1
```

**show firewall log detail**

```
user@host> show firewall log detail
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fpx0.0
Name of protocol: TCP, Packet Length: 50824, Source address: 172.17.22.108, Destination address: 192.168.70.66
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fpx0.0
Name of protocol: TCP, Packet Length: 50824, Source address: 172.17.22.108, Destination address: 192.168.70.66
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fpx0.0
Name of protocol: TCP, Packet Length: 1020, Source address: 172.17.22.108, Destination address: 192.168.70.66
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fpx0.0
Name of protocol: TCP, Packet Length: 1020, Source address: 172.17.22.108, Destination address: 192.168.70.66
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fpx0.0
Name of protocol: TCP, Packet Length: 1020, Source address: 172.17.22.108, Destination address: 192.168.70.66
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fpx0.0
```
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829, Destination address: 192.168.70.66:513
Time of Log: 2004-10-13 10:37:17 PDT, Filter: f, Filter action: accept, Name of interface: fxp0.0
Name of protocol: TCP, Packet Length: 49245, Source address: 172.17.22.108:829, Destination address: 192.168.70.66:513
....
show policer

**Syntax**
```
show policer
<policer-name>
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display statistics about configured policers.

**Options**
- **none**—Display the count of policed packets for all configured policers in the system.
- **policer-name**—(Optional) Display the count of policed packets for the specified policer.

**Required Privilege**
view

**Related Documentation**
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Verifying That Firewall Filters Are Operational on page 4259
- Verifying That Policers Are Operational on page 4260
- Firewall Filters for EX Series Switches Overview on page 4088
- Understanding the Use of Policers in Firewall Filters on page 4155

**List of Sample Output**
- `show policer` on page 4282
- `show policer (policer-name)` on page 4283

**Output Fields**
Table 531 on page 4282 lists the output fields for the `show policer` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Name of filter that is configured with the <code>filter</code> statement at the <code>[edit firewall]</code> hierarchy level.</td>
<td>All levels</td>
</tr>
<tr>
<td>Policers</td>
<td>Display policer information:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>- Filter—Name of filter that specifies the policer action.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Name—Name of policer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Packets—Number of packets that matched the filter term where the policer action is specified. This is the number of packets that exceed the rate limits that the policer specifies.</td>
<td></td>
</tr>
</tbody>
</table>

**Sample Output**
```
show policer
```
```
user@host> show policer
```
Filter: egress-vlan-filter
Filter: ingress-port-filter

Policers:

<table>
<thead>
<tr>
<th>Name</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>icmp-connection-policer</td>
<td>0</td>
</tr>
<tr>
<td>tcp-connection-policer</td>
<td>0</td>
</tr>
</tbody>
</table>

Filter: ingress-vlan-rogue-block

**show policer (policer-name)**

```
user@host> show policer tcp-connection-policer
Filter: ingress-port-filter
Policers:

<table>
<thead>
<tr>
<th>Name</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp-connection-policer</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show policy

Syntax
show policy
<logical-system (all | logical-system-name)>
<policy-name>

Syntax (EX Series Switches)
show policy
<policy-name>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display information about configured routing policies.

Options
none—List the names of all configured routing policies.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

policy-name—(Optional) Show the contents of the specified policy.

Required Privilege
view

Related Documentation
• show policy damping on page 2685

List of Sample Output
show policy on page 4284
show policy policy-name on page 4285
show policy (Multicast Scoping) on page 4285

Output Fields
Table 532 on page 4284 lists the output fields for the show policy command. Output fields are listed in the approximate order in which they appear.

Table 532: show policy Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-name</td>
<td>Name of the policy listed.</td>
</tr>
<tr>
<td>term</td>
<td>Policy term listed.</td>
</tr>
<tr>
<td>from</td>
<td>Match condition for the policy.</td>
</tr>
<tr>
<td>then</td>
<td>Action for the policy.</td>
</tr>
</tbody>
</table>

Sample Output

show policy

user@host> show policy
Configured policies:
__vrf-export-red-internal__
__vrf-import-red-internal__
red-export
all_routes

show policy policy-name

user@host> show policy test-statics
Policy test-statics:
  from
    3.0.0.0/8  accept
    3.1.0.0/16  accept
  then reject

show policy (Multicast Scoping)

user@host> show policy test-statics
Policy test-statics:
  from
    multicast-scoping == 8
show policy conditions

Syntax

show policy conditions
<condition-name>
<detail>
<dynamic>
<logical-system (all | logical-system-name)>

Syntax (EX Series Switches)

show policy conditions
<condition-name>
<detail>
<dynamic>

Release Information

Command introduced in Junos OS Release 9.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display all the configured conditions as well as the routing tables with which the configuration manager is interacting. If the detail keyword is included, the output also displays dependent routes for each condition.

Options

none—Display all configured conditions and associated routing tables.

condition-name—(Optional) Display information about the specified condition only.

detail—(Optional) Display the specified level of output.

dynamic—(Optional) Display information about the conditions in the dynamic database.

logical-system (all | logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege

view

List of Sample Output

show policy conditions detail on page 4287

Output Fields

Table 533 on page 4286 lists the output fields for the show policy conditions command. Output fields are listed in the approximate order in which they appear.

Table 533: show policy conditions Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>Name of configured condition.</td>
<td>All levels</td>
</tr>
<tr>
<td>event</td>
<td>Condition type. If the if-route-exists option is configured, the event type is:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Existence of a route in a specific routing table.</td>
<td>All levels</td>
</tr>
<tr>
<td>Dependent routes</td>
<td>List of routes dependent on the condition, along with the latest generation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>number.</td>
<td>detail</td>
</tr>
<tr>
<td>Condition tables</td>
<td>List of routing tables associated with the condition, along with the latest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>generation number and number of dependencies.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 533: show policy conditions Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>If-route-exists</td>
<td>List of conditions configured to look for a route in the specified table.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

Sample Output

show policy conditions detail

```
user@host> show policy conditions detail
Configured conditions:
Condition primary (static), event: Existence of a route in a specific routing table
Dependent routes:
8.41.0.0/24, generation 18

Condition standby (static), event: Existence of a route in a specific routing table
Dependent routes:
8.41.0.0/24, generation 18

Condition tables:
Table mpls.0, generation 0, dependencies 0, If-route-exists conditions: primary (static) standby (static)
Table l3vpn.inet.0, generation 633, dependencies 2
```
test policy

Syntax

```
test policy policy-name prefix
```

Release Information

Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Test a policy configuration to determine which prefixes match routes in the routing table.

NOTE: If you are using the test policy command on a logical system, you must first set the CLI to the logical system context. For example, if you want to test a routing policy that is configured on logical system R2, first run the set cli logical-system R2 command.

Options

- `policy-name`—Name of a policy.
- `prefix`—Destination prefix to match.

Additional Information

All prefixes in the default unicast routing table (inet.0) that match prefixes that are the same as or longer than the specific prefix are processed by the `from` clause in the specified policy. All prefixes accepted by the policy are displayed. The `test policy` command evaluates a policy differently from the BGP import process. When testing a policy that contains an `interface` match condition in the `from` clause, the `test policy` command uses the match condition. In contrast, BGP does not use the `interface` match condition when evaluating the policy against routes learned from internal BGP (IBGP) or external BGP (EGBP) multihop peers.

Required Privilege

- View

Related Documentation

- Understanding Routing Policy Tests
- Example: Testing a Routing Policy with Complex Regular Expressions

List of Sample Output

`test policy` on page 4288

Output Fields

For information about output fields, see the output field tables for the `show route` command, the `show route detail` command, the `show route extensive` command, or the `show route terse` command.

Sample Output

test policy

```
user@host> test policy test-statics 3.0.0.1/8
inet.0: 44 destinations, 44 routes (44 active, 0 holddown, 0 hidden)
Prefixes passing policy:
```
3.0.0.0/8  *[BGP/170] 16:22:46, localpref 100, from 10.255.255.41
     AS Path: 50888 I
            > to 10.11.4.32 via en0.2, label-switched-path l2
3.3.3.1/32  *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
            > to 10.0.4.7 via fxp0.0
3.3.3.2/32  *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
            > to 10.0.4.7 via fxp0.0
3.3.3.3/32  *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
            > to 10.0.4.7 via fxp0.0
3.3.3.4/32  *[IS-IS/18] 2d 00:21:46, metric 0, tag 2
            > to 10.0.4.7 via fxp0.0
Policy test-statics: 5 prefixes accepted, 0 prefixes rejected
CHAPTER 80

Troubleshooting Procedures

- Troubleshooting Firewall Filters on page 4291

Troubleshooting Firewall Filters

Troubleshooting issues with firewall filters on EX Series switches:

1. A Firewall Filter Configuration Returns a “No Space Available in TCAM” Message on page 4291

A Firewall Filter Configuration Returns a “No Space Available in TCAM” Message

**Problem** When a firewall filter configuration exceeds the amount of available ternary content addressable memory (TCAM) space, the switch returns the following system log (syslogd) message:

No space available in tcam.
Rules for filter filter-name will not be installed.

The switch returns this error message during the commit operation in the following instances:

- If the firewall filter that you have applied to a port, VLAN, or Layer 3 interface requires more than the amount of available TCAM space.

- If you delete and add large firewall filters in the same commit operation. In this case, the large firewall filter might not be deleted from the TCAM space, because of which there will be no TCAM space freed up for the new firewall filter to be added to it. In addition to the syslogd message, the following error message is displayed in the CLI:

  fpc<device-id> dfw_grph_merge_dfw_bind: rules for filter filter-name will not be installed

However, in both these instances, the commit operation for the firewall filter configuration is completed in the CLI.

**Solution** When a firewall filter configuration exceeds the amount of available TCAM table space, you must configure a new firewall filter with fewer filter terms or, if you had deleted and created a firewall filter with a large number of terms (on the order of 1000 or more), you must delete and add the large firewall filters in separate commit operations.
The first procedure (set of steps) in this Solution section tells you how to delete a firewall filter and its bind point and associate a new firewall filter with that existing bind point.

The second procedure in this Solution section tells you how to create a new firewall filter with fewer terms (without deleting the bind point) and bind the new firewall filter with the existing bind point, when you want to create a firewall filter with fewer terms. Do not use the second procedure if you need to replace one large firewall filter with another large firewall filter—you must delete the original large firewall filter and commit that delete operation, and then add the new large firewall filter.

To delete the firewall filter and its bind point and apply a new firewall filter to the same bind point:

1. Delete the firewall filter configuration and its bind points to ports, VLANs, or Layer 3 interfaces—for example:
   ```
   [edit]
   user@switch# delete firewall family ethernet-switching filter mini-filter-ingress-vlan
   user@switch# delete vlans voice-vlan description "filter to block rogue devices on voice-vlan"
   user@switch# delete vlans voice-vlan filter input mini-filter-ingress-vlan
   ```

2. Commit the operation:
   ```
   [edit]
   user@switch# commit
   ```

   **NOTE:** Use separate commit operations for deleting and adding large firewall filters.

3. Configure a firewall filter with fewer terms (if the error message appeared when you tried to create a new filter) or configure a large filter (if the error message appeared when you tried to delete and add large firewall filters)—for example:
   ```
   [edit]
   user@switch# set firewall family ethernet-switching filter new-filter-ingress-vlan ...
   ```

   **NOTE:** See “Firewall Filters for EX Series Switches Overview” on page 4088 to ascertain the maximum number of terms allowed for various firewall filters on EX Series switches.

4. Apply (bind) the new firewall filter to a port, VLAN, or Layer 3 interface—for example:
   ```
   [edit]
   user@switch# set vlans voice-vlan description "filter to block rogue devices on voice-vlan"
   user@switch# set vlans voice-vlan filter input new-filter-ingress-vlan
   ```

5. Commit the operation:
   ```
   [edit]
   user@switch# commit
   ```

To create a new firewall filter and attach it to the existing bind point:

1. Configure a firewall filter with fewer terms than the original filter:
[edit]
user@switch# set firewall family ethernet-switching filter new-filter-ingress-vlan

2. Apply the firewall filter to the port, VLAN, or Layer 3 interfaces to overwrite the bind points of the original filter—for example:

[edit]
user@switch# set vlans voice-vlan description "smaller filter to block rogue devices on voice-vlan"
user@switch# set vlans voice-vlan filter input new-filter-ingress-vlan

As a bind point can be attached to only one firewall filter, this configuration detaches the bind point from the previous firewall filter that contained many terms and attaches the bind point to the new firewall filter.

3. Commit the operation:

[edit]
user@switch# commit

Related Documentation
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches on page 4161
- Verifying That Firewall Filters Are Operational on page 4259
- Configuring Firewall Filters (CLI Procedure) on page 4192
- Configuring Firewall Filters (J-Web Procedure) on page 4201
PART 26

Spanning-Tree Protocols

• Overview on page 4297  
• Configuration on page 4313  
• Administration on page 4421
CHAPTER 81

Overview

- Spanning Trees Overview on page 4297

Spanning Trees Overview

- Understanding MSTP for EX Series Switches on page 4298
- Understanding RSTP for EX Series Switches on page 4300
- Understanding STP for EX Series Switches on page 4304
- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 4306
- Understanding VSTP for EX Series Switches on page 4306
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series
  Switches on page 4308
- Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series
  Switches on page 4310
- Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series
  Switches on page 4311
Understanding MSTP for EX Series Switches

Ethernet networks are susceptible to broadcast storms if loops are introduced. However, an Ethernet network should always include loops because they provide redundant paths in case of a link failure. Spanning-tree protocols address both of these issues because they provide link redundancy while simultaneously preventing undesirable loops.

Spanning-tree protocols intelligently avoid loops in a network by creating a tree topology (spanning-tree) of the entire bridged network with only one available path between the tree root and a leaf. All other paths are forced into a standby state. The tree root is a switch within the network elected by the STA (spanning-tree algorithm) to use when computing the best path between bridges throughout the network and the root bridge. Frames travel through the network to their destination—a leaf such as an end-user PC—along branches. A tree branch is a network segment, or link, between bridges. Switches that forward frames through an STP spanning-tree are called designated bridges.

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning-Tree Protocol (STP), Rapid Spanning-Tree Protocol (RSTP), Multiple Spanning-Tree Protocol (MSTP), and VLAN Spanning-Tree Protocol (VSTP). This topic explains MSTP.

This topic describes:

- MSTP Maps Multiple VLANs on page 4298
- Configuring MSTP Regions on page 4299
- Selecting a Spanning-Tree Protocol on page 4299

MSTP Maps Multiple VLANs

MSTP is an extension of RSTP that maps multiple independent spanning-tree instances onto one physical topology. Each spanning-tree instance (STI) includes one or more VLANs. Unlike in STP and RSTP configurations, a port may belong to multiple VLANs and be dynamically blocked in one spanning-tree instance but forwarding in another. This behavior significantly improves network resource utilization by load-balancing across the network and maintaining switch CPU loads at moderate levels. MSTP also leverages the fast re-convergence time of RSTP when a network, switch, or port failure occurs within a spanning-tree instance.

MSTP creates a Common and Internal Spanning-Tree (CIST) to interconnect and manage all MSTP regions and even individual devices that run RSTP or STP, which are recognized as distinct spanning-tree regions by MSTP. The CIST views each MSTP region as a virtual bridge, regardless of the actual number of devices participating in the MSTP region, and enables MSTIs to link to other regions. The CIST is a single topology that connects all switches (STP, RSTP, and MSTP devices) through an active topology, ensuring connectivity between LANs and devices within a bridged network. This functionality provided by MSTP enables you to better utilize network resources while remaining backward-compatible with older network devices.
Configuring MSTP Regions

When enabling MSTP, you define one or more MSTP regions. An MSTP region defines a logical domain where MSTIs can be administered independently of MSTIs in other regions, setting the boundary for Bridge Protocol Data Units (BPDUs) sent by one MSTI. An MSTP region is a group of switches that is defined by three parameters:

- Region name—User-defined alphanumeric name for the region.
- Revision level—User-defined value that identifies the region.

An MSTP region can support up to 64 MST instances, and each MSTI can support from 1 to 4094 VLANs. When you define a region, MSTP automatically creates an internal spanning-tree instance (IST instance 0) that provides the root switch for the region and includes all currently configured VLANs that are not specifically assigned to a user-defined Multiple Spanning-Tree Instance (MSTI). An MSTI includes all static VLANs that you specifically add to it. The switch places any dynamically created VLANs in the IST instance by default, unless you explicitly map them to another MSTI. Once you assign a VLAN to a user-defined MSTI, the switch removes the VLAN from the IST instance.

Selecting a Spanning-Tree Protocol

The default factory configuration for EX Series switches is RSTP, a faster version of STP. To determine which spanning-tree protocol is best for your situation, see Table 534 on page 4299 below.

Table 534: Selecting a Spanning-Tree Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSTP</td>
<td>• Rapid Spanning-Tree Protocol is the default switch configuration and is recommended for most network configurations because it converges more quickly than STP after a failure.</td>
<td>• RSTP does not work with 802.1D 1998 bridges.</td>
</tr>
<tr>
<td></td>
<td>• Voice and video work better with RSTP than they do with STP.</td>
<td>• RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic.</td>
</tr>
<tr>
<td></td>
<td>• RSTP is backward compatible with STP so switches do not all have to run RSTP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RSTP supports more ports than MSTP or VSTP</td>
<td></td>
</tr>
<tr>
<td>STP</td>
<td>• Spanning-Tree Protocol works with 802.1D 1998 bridges.</td>
<td>• STP is slower than RSTP.</td>
</tr>
<tr>
<td></td>
<td>• RSTP is backward compatible with STP so switches do not all have to run STP.</td>
<td>• STP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic.</td>
</tr>
<tr>
<td>MSTP</td>
<td>• Multiple Spanning-Tree Protocol works with most VLANs.</td>
<td>• Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP.</td>
</tr>
<tr>
<td></td>
<td>• RSTP and STP are recognized as distinct spanning-tree regions by MSTP.</td>
<td>• MSTP supports a limited number of ports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MSTP uses more CPU than RSTP and does not converge as fast as RSTP.</td>
</tr>
</tbody>
</table>
Table 534: Selecting a Spanning-Tree Protocol (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| VSTP     | • VLAN Spanning-Tree Protocol works with VLANs that require device compatibility.  
          • VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch. | • With VSTP there can be only STP instance per VLAN, whereas MSTP lets you combine multiple VLANs in one instance.  
          • VSTP supports a limited number of ports compared to RSTP.  
          • VSTP uses more CPU than RSTP and does not converge as fast as RSTP.  
          • Having a large number of VSTP and RSTP instances can cause continuous changes in the topology. As a workaround, reduce the number of VSTP instances to fewer than 190. |

Related Documentation
- Understanding STP for EX Series Switches on page 4304
- Understanding RSTP for EX Series Switches on page 4300
- Understanding VSTP for EX Series Switches on page 4306
- Understanding Layer 2 Protocol Tunneling on EX Series Switches
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330

Understanding RSTP for EX Series Switches

Ethernet networks are susceptible to broadcast storms if loops are introduced. However, an Ethernet network should always include loops because they provide redundant paths in case of a link failure. Spanning tree protocols address both of these issues because they provide link redundancy while simultaneously preventing undesirable loops. Rapid Spanning-Tree Protocol (RSTP) is the default spanning-tree protocol for preventing loops on Ethernet networks.

This topic describes:
- Spanning-Tree Protocols Help Prevent Broadcast Storms on page 4300
- RSTP is an Enhancement of the Original STP on page 4301
- Port Roles Determine Participation in The Spanning-Tree on page 4301
- Port States Determine How a Port Processes a Frame on page 4301
- Edge Ports Connect to Devices That Cannot Be Part of a Spanning-Tree on page 4302
- BPDUs Maintain the Spanning-Tree on page 4302
- When an RSTP Root Bridge Fails on page 4303
- Switches Must Relearn MAC Addresses After a Link Failure on page 4303
- Selecting a Spanning-Tree Protocol on page 4303

Spanning-Tree Protocols Help Prevent Broadcast Storms

Spanning tree protocols intelligently avoid loops in a network by creating a tree topology (spanning-tree) of the entire bridged network with only one available path between the
tree root and a leaf. All other paths are forced into a standby state. The tree root is a switch within the network elected by the STA (spanning-tree algorithm) to use when computing the best path between bridges throughout the network and the root bridge. Frames travel through the network to their destination—a leaf such as an end-user PC—along branches. A tree branch is a network segment, or link, between bridges. Switches that forward frames through an STP spanning-tree are called designated bridges.

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning-Tree Protocol (STP), Rapid Spanning-Tree Protocol (RSTP), Multiple Spanning-Tree Protocol (MSTP), and VLAN Spanning-Tree Protocol (VSTP). This topic explains the spanning-tree default RSTP.

**RSTP is an Enhancement of the Original STP**

RSTP evolved from the original STP IEEE 802.1D protocol to provide faster spanning-tree re-convergence after a switch port, switch, or LAN failure. Where STP took up to 50 seconds to respond to topology changes, RSTP responds to changes within the timeframe of three hello BPDUs (bridge protocol data units), or 6 seconds. This is the primary reason that RSTP is the default configuration on EX Series switches. In addition, note that EX Series switches configured to use STP actually run RSTP force version 0, which is compatible with STP.

**Port Roles Determine Participation in The Spanning-Tree**

Each port has both a state and a role. A port’s role determines how it participates in the spanning-tree. The five port roles used in RSTP are:

- **Root port**—The port closest to the root bridge (has the lowest path cost from a bridge). This is the only port that receives frames from and forwards frames to the root bridge.

- **Designated port**—The port that forwards traffic away from the root bridge toward a leaf. A designated bridge has one designated port for every link connection it serves. A root bridge forwards frames from all of its ports, which serve as designated ports.

- **Alternate port**—A port that provides an alternate path toward the root bridge if the root port fails and is placed in the discarding state. This port is not part of the active spanning-tree, but if the root port fails, the alternate port immediately takes over.

- **Backup port**—A port that provides a backup path toward the leaves of the spanning-tree if a designated port fails and is placed in the discarding state. A backup port can only exist where two or more bridge ports connect to the same LAN for which the bridge serves as the designated bridge. A backup port for a designated port immediately takes over if the port fails.

- **Disabled port**—The port is not part of the active spanning-tree.

**Port States Determine How a Port Processes a Frame**

Each port has both a state and a role. A port’s state determines how it processes a frame. RSTP places each port of a designated bridge in one of three states:

- **Discarding**—The port discards all BPDUs. A port in this state discards all frames it receives and does not learn MAC addresses.
- **Learning**—The port prepares to forward traffic by examining received frames for location information in order to build its MAC address table.

- **Forwarding**—The port filters and forwards frames. A port in the forwarding state is part of the active spanning-tree.

### Edge Ports Connect to Devices That Cannot Be Part of a Spanning-Tree

RSTP also defines the concept of an *edge port*, which is a designated port that connects to non-STP-capable devices, such as PCs, servers, routers, or hubs that are not connected to other switches. Because edge ports connect directly to end stations, they cannot create network loops and can transition to the forwarding state immediately. You can manually configure edge ports, and a switch can also detect edge ports by noting the absence of communication from the end stations.

The edge ports themselves do send BPDUs to the spanning-tree. If you have a good understanding of the implications on your network and want to modify RSTP on the edge port interface, see *Configuring RSTP (CLI Procedure)*.

### BPDUs Maintain the Spanning-Tree

Spanning-tree protocols use frames called bridge protocol data units (BPDUs) to create and maintain the spanning-tree. A BPDU frame is a message sent from one switch to another to communicate information about itself, such as its bridge ID, root path costs, and port MAC addresses. The initial exchange of BPDUs between switches determines the root bridge. Simultaneously, BPDUs are used to communicate the cost of each link between branch devices, which is based upon port speed or user configuration. RSTP uses this path cost to determine the ideal route for data frames to travel from one leaf to another leaf and then blocks all other routes. If an edge port receives a BPDU, it automatically transitions to a regular RSTP port.

When the network is in a steady state, the spanning-tree converges when the spanning-tree algorithm (STA) identifies both the root and designated bridges and all ports are in either a forwarding or blocking state. To maintain the tree, the root bridge continues to send BPDUs at a “hello time” interval (default 2 seconds). These BPDUs continue to communicate the current tree topology. When a port receives a hello BPDU, it compares the information to that already stored for the receiving port. One of three actions takes place when a switch receives a BPDU:

- If the BPDU data matches the existing entry in the MAC address table, the port resets a timer called “max age” to zero and then forwards a new BPDU with the current active topology information to the next port in the spanning-tree.

- If the topology in the BPDU has been changed, the information is updated in the MAC address table, “max age” is again set to zero, and a new BPDU is forwarded with the current active topology information to the next port in the spanning-tree.

- When an RSTP port does not receive a BPDU for three hello times, it reacts one of two ways. If the port is the root port, a complete rework of the spanning-tree occurs—see *When an RSTP Root Bridge Fails*. If the bridge is any non-root bridge, RSTP detects that the connected device cannot send BPDUs and converts that port to an edge port.
When an RSTP Root Bridge Fails

When a link to the root port goes down, a flag called a topology change notification (TCN) is added to the BPDU. When this BPDU reaches the next port in the VLAN, the MAC address table is flushed and the BPDU is sent to the next bridge. Eventually, all ports in the VLAN have flushed their MAC address tables. Then, RSTP configures a new root port.

After a root port or a designated port fails, the alternate or backup port takes over after an exchange of BPDU's called the proposal-agreement handshake. RSTP propagates this handshake over point-to-point links, which are dedicated links between two network nodes, or switches, that connect one port to another. If a local port becomes a new root or designated port, it negotiates a rapid transition with the receiving port on the nearest neighboring switch by using the proposal-agreement handshake to ensure a loop-free topology.

Switches Must Relearn MAC Addresses After a Link Failure

Because a link failure causes all associated ports to flush their MAC address table, the network may be slower as it floods to relearn the MAC addresses. There is a way to speed up this relearning process. During TCN propagation, the Layer 2 forwarding table of switches is flushed, resulting in a flood of data packets. The ARP feature causes the switch to proactively send ARP requests for IP addresses in the ARP cache (present because of Layer 3 VLAN interface). With ARP on STP enabled, as the reply comes through, the switches builds up the Layer 2 forwarding table, thus limiting the flooding later. Enabling ARP on STP is most useful to prevent excessive flooding in large Layer 2 networks using RVIs.

Selecting a Spanning-Tree Protocol

The default factory configuration for EX Series switches is RSTP, a faster version of the original STP. To determine which spanning-tree protocol is best for your situation, see Table 535 on page 4303 below.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| RSTP     | - Rapid Spanning-Tree Protocol is the default switch configuration and is recommended for most network configurations because it converges more quickly than STP after a failure.  
- Voice and video work better with RSTP than they do with STP.  
- RSTP is backward compatible with STP so switches do not all have to run RSTP.  
- RSTP supports more ports than MSTP or VSTP  | - RSTP does not work with 802.1D 1998 bridges.  
- RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic. |
| STP      | - Spanning-Tree Protocol works with 802.1D 1998 bridges.  
- RSTP is backward compatible with STP so switches do not all have to run STP.  | - STP is slower than RSTP.  
- STP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic. |
Table 535: Selecting a Spanning-Tree Protocol (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| MSTP     | • Multiple Spanning-Tree Protocol works with most VLANs.  
          • RSTP and STP are recognized as distinct spanning-tree regions by MSTP. | • Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP.  
          • MSTP supports a limited number of ports.  
          • MSTP uses more CPU than RSTP and does not converge as fast as RSTP. |
| VSTP     | • VLAN Spanning-Tree Protocol works with VLANs that require device compatibility.  
          • VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch. | • With VSTP there can be only STP instance per VLAN, whereas MSTP lets you combine multiple VLANs in one instance.  
          • VSTP supports a limited number of ports compared to RSTP.  
          • VSTP uses more CPU than RSTP and does not converge as fast as RSTP.  
          • Having a large number of VSTP and RSTP instances can cause continuous changes in the topology. As a workaround, reduce the number of VSTP instances to fewer than 190. |

Related Documentation

- Understanding STP for EX Series Switches on page 4304
- Understanding MSTP for EX Series Switches on page 4298
- Understanding VSTP for EX Series Switches on page 4306
- Understanding Layer 2 Protocol Tunneling on EX Series Switches
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313

Understanding STP for EX Series Switches

Ethernet networks are susceptible to broadcast storms if loops are introduced. However, an Ethernet network should always include loops because they provide redundant paths in case of a link failure. Spanning-tree protocols address both of these issues because they provide link redundancy while simultaneously preventing undesirable loops.

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning–Tree Protocol (STP), Rapid Spanning–Tree Protocol (RSTP), Multiple Spanning–Tree Protocol (MSTP), and VLAN Spanning–Tree Protocol (VSTP). Configure STP when you need to support older 802.1D 1998 bridges. However, note that EX Series switches configured to use STP actually run RSTP force version 0, which is compatible with STP. For an explanation of RSTP, see “Understanding RSTP for EX Series Switches” on page 4300

This topic describes:

- Selecting a Spanning-Tree Protocol on page 4305
Selecting a Spanning-Tree Protocol

The default factory configuration for EX Series switches is RSTP, a faster version of STP. To determine which spanning-tree protocol is best for your situation, see Table 536 on page 4305 below.

Table 536: Selecting a Spanning-Tree Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSTP</td>
<td>• Rapid Spanning-Tree Protocol is the default switch configuration and is recommended for most network configurations because it converges more quickly than STP after a failure. • Voice and video work better with RSTP than they do with STP. • RSTP is backward compatible with STP so switches do not all have to run RSTP. • RSTP supports more ports than MSTP or VSTP</td>
<td>• RSTP does not work with 802.1D 1998 bridges. • RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic.</td>
</tr>
<tr>
<td>STP</td>
<td>• Spanning-Tree Protocol works with 802.1D 1998 bridges. • RSTP is backward compatible with STP so switches do not all have to run STP.</td>
<td>• STP is slower than RSTP. • STP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic.</td>
</tr>
<tr>
<td>MSTP</td>
<td>• Multiple Spanning-Tree Protocol works with most VLANs. • RSTP and STP are recognized as distinct spanning-tree regions by MSTP.</td>
<td>• Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP. • MSTP supports a limited number of ports. • MSTP uses more CPU than RSTP and does not converge as fast as RSTP.</td>
</tr>
<tr>
<td>VSTP</td>
<td>• VLAN Spanning-Tree Protocol works with VLANs that require device compatibility. • VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch.</td>
<td>• With VSTP there can be only STP instance per VLAN, whereas MSTP lets you combine multiple VLANs in one instance. • VSTP supports a limited number of ports compared to RSTP. • VSTP uses more CPU than RSTP and does not converge as fast as RSTP. • Having a large number of VSTP and RSTP instances can cause continuous changes in the topology. As a workaround, reduce the number of VSTP instances to fewer than 190.</td>
</tr>
</tbody>
</table>

Related Documentation

- Configuring STP (CLI Procedure)
- Understanding RSTP for EX Series Switches on page 4300
- Understanding MSTP for EX Series Switches on page 4298
- Understanding VSTP for EX Series Switches on page 4306
- Understanding Layer 2 Protocol Tunneling on EX Series Switches
RSTP or VSTP Forced to Run as IEEE 802.1D STP

On MX Series routers and EX Series switches in a Layer 2 environment, you can force the configured Rapid Spanning Tree Protocol (RSTP) or VLAN Spanning Tree Protocol (VSTP) to run as the original IEEE 802.1D Spanning Tree Protocol (STP) version. Configure original IEEE.802.1D STP for compatibility with older bridges that do not support RSTP or VSTP.

Keep the following limitations in mind when RSTP or VSTP are forced to run as the original STP version:

- If you configure an instance interface as an edge port, the configuration statement is ignored.
- If you configure point-to-point link mode for an instance interface, the configuration statement is ignored.

Related Documentation

- Spanning-Tree Protocols Supported
- Configuring Rapid Spanning-Tree Protocol
- Configuring VLAN Spanning-Tree Protocol
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 4381
- Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure) on page 4372
- force-version on page 4394

Understanding VSTP for EX Series Switches

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). The default factory configuration for EX Series switches uses RSTP. If you use VLANs, however, we recommend that you enable MSTP unless your network requires the device compatibility provided by VSTP. Switches configured to run VSTP automatically assign each VLAN to one spanning-tree instance that runs RSTP. While this approach is useful to optimize network usage in small networks with a limited number of VLANs, a VSTP configuration in a network with several hundred VLANs can overload switch CPUs. MSTP ensures that your network is not slowed down by the increased network traffic caused by hundreds of VLANs, each with its own spanning-tree instance.

When using VSTP, you can selectively configure up to 253 VLANs per switch—additional VLANs use RSTP. (VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch.)

NOTE: When you configure VSTP, we recommend that you enable VSTP on all VLANs that can receive VSTP bridge protocol data units (BPDUs).
NOTE: When you configure VSTP with the set protocol vstp vlan all command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration on your switch, you must set it separately with the set protocol vstp vlan 1 command.

NOTE: Option vlan all is not supported in Junos OS Release 13.2X50.

Selecting a Spanning-Tree Protocol

The default factory configuration for EX Series switches is RSTP, a faster version of STP. To determine which spanning-tree protocol is best for your situation, see Table 537 on page 4307.

Table 537: Selecting a Spanning-Tree Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| RSTP     | • Rapid Spanning Tree Protocol is the default switch configuration and is recommended for most network configurations because it converges more quickly than STP after a failure.  
• Voice and video work better with RSTP than they do with STP.  
• RSTP is backward compatible with STP so switches do not all have to run RSTP.  
• RSTP supports more ports than MSTP or VSTP. | • RSTP does not work with 802.1D 1998 bridges.  
• RSTP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning tree. This limits the number of forwarding paths for data traffic. |
| STP      | • Spanning Tree Protocol works with 802.1D 1998 bridges.  
• RSTP is backward compatible with STP so switches do not all have to run STP. | • STP is slower than RSTP.  
• STP is not recommended for multiple VLAN networks because it is not VLAN-aware—as a result, all VLANs within a LAN share the same spanning-tree. This limits the number of forwarding paths for data traffic. |
| MSTP     | • Multiple Spanning Tree Protocol works with most VLANs.  
• RSTP and STP are recognized as distinct Spanning Tree regions by MSTP. | • Some protocols require compatibility that is not provided by MSTP. In this case, use VSTP.  
• MSTP supports a limited number of ports.  
• MSTP uses more CPU than RSTP and does not converge as fast as RSTP. |
| VSTP     | • VLAN Spanning Tree Protocol works with VLANs that require device compatibility.  
• VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on a switch. | • With VSTP there can be only STP instance per VLAN, whereas MSTP lets you combine multiple VLANs in one instance.  
• VSTP supports a limited number of ports compared to RSTP.  
• VSTP uses more CPU than RSTP and does not converge as fast as RSTP. |
Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches

Networks frequently use multiple protocols simultaneously to achieve different goals and in some cases those protocols might conflict with each other. One such case is when spanning-tree protocols are active on the network, where a special type of switching frame called a bridge protocol data unit (BPDU) can conflict with BPDUs generated on other devices such as PCs. The different kinds of BPDUs are not compatible but they can still be recognized by other devices that use BPDUs and cause network outages. You need to protect any device that recognizes BPDUs from picking up incompatible BPDUs.

Different Kinds of BPDUs

Spanning-tree protocols such as Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), and Multiple Spanning Tree Protocol (MSTP) generate their own BPDUs. These peer STP applications use their BPDUs to communicate, and ultimately, the exchange of BPDUs determines which interfaces block traffic and which interfaces become root ports and forward traffic.

User bridge applications running on a PC can also generate BPDUs. If these BPDUs are picked up by STP applications running on the switch, they can trigger STP miscalculations, and those miscalculations can lead to network outages. Similarly, BPDUs generated by STP protocols can cause problems if they are picked up by devices like PCs that are not using STP. Some mechanism for BPDU protection must be implemented in these cases.

Protecting Switches From Incompatible BPDUs

To protect the state of spanning-tree protocols on switches from outside BPDUs, enable BPDU protection on the interfaces of a switch on which spanning-tree protocols are configured and are connected to user devices (such as PCs)—for example, on edge ports connected to PCs. Use the same strategy when a device on which STP is not configured is connected to a switch through a trunk interface that could be forwarding BPDUs generated by spanning-tree protocols. In this case, you would protect the device from BPDUs generated by the STP on the switch.

To configure BPDU protection on a switch on which spanning-tree protocols are configured, include the `bpdu-block-on-edge` statement at the `[edit protocols (stp | mstp | rstp)]` hierarchy level. To prevent such a switch from forwarding BPDUs generated by spanning-tree protocols to devices, include the `bpdu-block` statement at the `[edit ethernet-switching-options]` hierarchy level.
NOTE: You can configure the drop option under the `bpdu-block` statement only on interfaces on which no spanning-tree protocol is configured.

When an interface configured with BPDU protection encounters an incompatible BPDU, it drops that BPDU and then, either shuts down or continues to receive packets other than spanning-tree protocol BPDUs (for STP, MSTP, and RSTP) depending on the configuration defined in the `bpdu-block` statement. If the interface continues to be open after dropping all incompatible BPDUs, all traffic except incompatible BPDUs continues to ingress and egress through the interface.

If the interface shuts down after dropping all BPDUs, there are two ways to re-enable the interface:

- Include the `disable-timeout` statement in the BPDU configuration so that the interface automatically returns to service after the timer expires.
- Issue the operational mode command `clear ethernet-switching bpdu-error` on the switch. This command will only re-enable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.

NOTE: You can also configure BPDU drop protection on a switch without spanning trees—typically, you do this when such a switch is connected to a switch with spanning trees through a trunk interface.

Related Documentation
- Configuring BPDU Protection on an Interface (CLI Procedure)
- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357
- Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 4310
- Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 4311
- Understanding STP for EX Series Switches on page 4304
Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), and Multiple Spanning Tree Protocol (MSTP). Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing ports from moving into a forwarding state that would result in a loop opening up in the network.

A loop-free network in spanning-tree topologies is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDUs to communicate. Ultimately, the exchange of BPDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

However, a blocking interface can transition to the forwarding state in error if the interface stops receiving BPDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor.

When loop protection is enabled, the spanning-tree topology detects root ports and blocked ports and makes sure both keep receiving BPDUs. If a loop-protection-enabled interface stops receiving BPDUs from its designated port, it reacts as it would react to a problem with the physical connection on this interface. It doesn't transition the interface to a forwarding state, but instead transitions it to a loop-inconsistent state. The interface recovers and then it transitions back to the spanning-tree blocking state as soon as it receives a BPDU.

We recommend that you enable loop protection on all switch interfaces that have a chance of becoming root or designated ports. Loop protection is most effective when enabled in the entire switched network. When you enable loop protection, you must configure at least one action (log, block, or both).

Note that an interface can be configured for either loop protection or root protection, but not for both.

Related Documentation

- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
- Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 4311
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 4308
- Understanding MSTP for EX Series Switches on page 4298
- Understanding RSTP for EX Series Switches on page 4300
- Understanding STP for EX Series Switches on page 4304
- Understanding VSTP for EX Series Switches on page 4306
Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches

Juniper Networks EX Series Ethernet Switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), and Multiple Spanning Tree Protocol (MSTP). A loop-free network is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPDDUs to communicate. Ultimately, the exchange of BPDDUs determines which interfaces block traffic and which interfaces become root ports and forward traffic.

However, a root port elected through this process has the possibility of being wrongly elected. A user bridge application running on a PC can generate BPDDUs, too, and interfere with root port election. Root protection allows network administrators to manually enforce the root bridge placement in the network.

Enable root protection on interfaces that should not receive superior BPDDUs from the root bridge and should not be elected as the root port. These interfaces become designated ports and are typically located on an administrative boundary. If the bridge receives superior STP BPDDUs on a port that has root protection enabled, that port transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge that should not be the root bridge from being elected the root bridge. After the bridge stops receiving superior STP BPDDUs on the interface with root protection, the interface returns to a listening state, followed by a learning state, and ultimately back to a forwarding state. Recovery back to the forwarding state is automatic.

When root protection is enabled on an interface, it is enabled for all the STP instances on that interface. The interface is blocked only for instances for which it receives superior BPDDUs. Otherwise, it participates in the spanning-tree topology.

An interface can be configured for either root protection or loop protection, but not for both.

Related Documentation

• Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches on page 4367
• Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
• Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
• Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357
• Understanding MSTP for EX Series Switches on page 4298
• Understanding RSTP for EX Series Switches on page 4300
• Understanding STP for EX Series Switches on page 4304
• Understanding VSTP for EX Series Switches on page 4306
CHAPTER 82

Configuration

- Configuration Examples on page 4313
- Configuration Tasks on page 4372
- Operational Tasks on page 4380
- Configuration Statements on page 4381

Configuration Examples

- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
- Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches on page 4367

Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches

EX Series switches use Rapid Spanning Tree Protocol (RSTP) by default to provide a loop-free topology.

When switches that support redundant Routing Engines use RSTP, it is important to keep RSTP synchronized on both Routing Engines so that no loss of service occurs after a Routing Engine switchover. Nonstop bridging protocol keeps Routing Engines synchronized.

This example describes how to configure RSTP and NSB on four EX Series switches:

- Requirements on page 4314
- Overview and Topology on page 4314
- Configuring RSTP and Nonstop Bridging on Switch 1 on page 4316
- Configuring RSTP and Nonstop Bridging on Switch 2 on page 4319
• Configuring RSTP and Nonstop Bridging on Switch 3 on page 4322
• Configuring RSTP and Nonstop Bridging on Switch 4 on page 4325
• Verification on page 4328

Requirements

This example uses the following hardware and software components:

• Junos OS Release 11.3 or later for EX Series switches
• Four EX Series switches

Before you configure the switches for RSTP, be sure you have:

• Installed the four switches. See Connecting and Configuring an EX Series Switch (J-Web Procedure).
• Performed the initial software configuration on all switches. See Installing and Connecting an EX3200 Switch.

Overview and Topology

RSTP works by identifying certain links as point to point links and blocking other possible paths. When one of the point-to-point links fails, a designated alternate link transitions to the forwarding state and take over. Configuring nonstop bridging (NSB) on a switch with redundant Routing Engines keeps RSTP synchronized on both Routing Engines. This way, RSTP remains active immediately after a switchover because it is already synchronized to the backup Routing Engine. RSTP does not have to reconverge after a Routing Engine switchover when NSB is enabled because the neighbor devices do not detect an RSTP change on the switch. In this example, four EX Series switches are connected in the topology displayed in Figure 65 on page 4315 to create a loop-free topology with NSB applied to switches with dual Routing Engines.
Table 538 on page 4315 shows the components of the topology for this example.

NOTE: You can configure RSTP on logical or physical interfaces. This example shows RSTP configured on logical interfaces.

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch 1</strong></td>
<td>The following interfaces on Switch 1 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/9</code> is connected to Switch 2</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/13</code> is connected to Switch 4</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/11</code> is connected to Switch 3</td>
</tr>
<tr>
<td><strong>Switch 2</strong></td>
<td>The following interfaces on Switch 2 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/14</code> is connected to Switch 1</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/18</code> is connected to Switch 3</td>
</tr>
<tr>
<td><strong>Switch 3</strong></td>
<td>The following interfaces on Switch 3 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/26</code> is connected to Switch 1</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/28</code> is connected to Switch 2</td>
</tr>
<tr>
<td></td>
<td>- <code>ge-0/0/24</code> is connected to Switch 4</td>
</tr>
</tbody>
</table>
Table 538: Components of the Topology for Configuring RSTP (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 4</td>
<td>The following interfaces on Switch 4 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/19 is connected to Switch 1</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/23 is connected to Switch 3</td>
</tr>
</tbody>
</table>
| VLAN names and tag IDs | voice-vlan, tag 10  
|                  | employee-vlan, tag 20  
|                  | guest-vlan, tag 30  
|                  | camera-vlan, tag 40                                                                                                                    |

This configuration example creates a loop-free topology between four EX Series switches using RSTP.

An RSTP topology contains ports that have specific roles:

- The root port is responsible for forwarding data to the root bridge.
- The alternate port is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The designated port forwards data to the downstream network segment or device.
- The backup port is a backup port for the designated port. When a designated port goes down, the backup port becomes the active designated port and starts forwarding data.

**NOTE:** You also can create a loop-free topology between the aggregation layer and the distribution layer using redundant trunk links. For more information about configuring redundant trunk links, see *Example: Configuring Redundant Trunk Links for Faster Recovery.*

### Configuring RSTP and Nonstop Bridging on Switch 1

**CLI Quick Configuration**

To quickly configure RSTP and nonstop bridging on Switch 1, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/11 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/13 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/9 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
```
set protocols rstp bridge-priority 16k
set protocols rstp interface ge-0/0/13.0 cost 1000
set protocols rstp interface ge-0/0/13.0 mode point-to-point
set protocols rstp interface ge-0/0/9.0 cost 1000
set protocols rstp interface ge-0/0/9.0 mode point-to-point
set protocols rstp interface ge-0/0/11.0 cost 1000
set protocols rstp interface ge-0/0/11.0 mode point-to-point

If Switch 1 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 1, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful switchover
set system commit synchronize
set ethernet-switching-options nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 1:

1. Configure the VLANs voice-vlan, employee-vlan, guest-vlan, and camera-vlan:

   [edit vlans]
   user@switch1# set voice-vlan description “Voice VLAN”
   user@switch1# set voice-vlan vlan-id 10
   user@switch1# set employee-vlan description “Employee VLAN”
   user@switch1# set employee-vlan vlan-id 20
   user@switch1# set guest-vlan description “Guest VLAN”
   user@switch1# set guest-vlan vlan-id 30
   user@switch1# set camera-vlan description “Camera VLAN”
   user@switch1# set camera-vlan vlan-id 40

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

   [edit interfaces]
   user@switch1# set ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch1# set ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch1# set ge-0/0/11 unit 0 family ethernet-switching vlan members [10 20 30 40]

3. Configure the port mode for the interfaces:

   [edit interfaces]
   user@switch1# set ge-0/0/13 unit 0 family ethernet-switching port-mode trunk
   user@switch1# set ge-0/0/9 unit 0 family ethernet-switching port-mode trunk
   user@switch1# set ge-0/0/11 unit 0 family ethernet-switching port-mode trunk

4. Configure RSTP on the switch:

   [edit protocols]
   user@switch1# rstp bridge-priority 16k
   user@switch1# rstp interface ge-0/0/13.0 cost 1000
   user@switch1# rstp interface ge-0/0/13.0 mode point-to-point
   user@switch1# rstp interface ge-0/0/9.0 cost 1000
   user@switch1# rstp interface ge-0/0/9.0 mode point-to-point
   user@switch1# rstp interface ge-0/0/11.0 cost 1000
   user@switch1# rstp interface ge-0/0/11.0 mode point-to-point

Step-by-Step Procedure

If Switch 1 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 1:

1. Enable graceful Routing Engine switchover (GRES):
2. Configure the switch to always synchronize configuration changes between the Routing Engines:

```
[edit system]
user@switch1# set commit synchronize
```

If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

```
[edit ethernet-switching-options]
user@switch1# set nonstop-bridging
```

**NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

**Results** Check the results of the configuration:

```
user@switch1> show configuration
interfaces {
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/9 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/11 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
}
```
Configuring RSTP and Nonstop Bridging on Switch 2

CLI Quick Configuration

To quickly configure RSTP and nonstop bridging on Switch 2, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description “Voice VLAN”
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description “Employee VLAN”
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description “Guest VLAN”
set vlans guest-vlan vlan-id 30
```
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/18 unit 0 family ethernet-switching port-mode trunk
set protocols rstp bridge-priority 32k
set protocols rstp interface ge-0/0/14.0 cost 1000
set protocols rstp interface ge-0/0/14.0 mode point-to-point
set protocols rstp interface ge-0/0/18.0 cost 1000
set protocols rstp interface ge-0/0/18.0 mode point-to-point

If Switch 2 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 2, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful switchover
set system commit synchronize
set ethernet-switching-options nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 2:

1. Configure the VLANs voice-vlan, employee-vlan, guest-vlan, and camera-vlan:

   [edit vlans]
   user@switch2# set voice-vlan description "Voice VLAN"
   user@switch2# set voice-vlan vlan-id 10
   user@switch2# set employee-vlan description "Employee VLAN"
   user@switch2# set employee-vlan vlan-id 20
   user@switch2# set guest-vlan description "Guest VLAN"
   user@switch2# set guest-vlan vlan-id 30
   user@switch2# set camera-vlan vlan-description "Camera VLAN"
   user@switch2# set camera-vlan vlan-id 40

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

   [edit interfaces]
   user@switch2# set ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch2# set ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]

3. Configure the port mode for the interfaces:

   [edit interfaces]
   user@switch2# set ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
   user@switch2# set ge-0/0/18 unit 0 family ethernet-switching port-mode trunk

4. Configure RSTP on the switch:

   [edit protocols]
   user@switch2# rstp bridge-priority 32k
   user@switch2# rstp interface ge-0/0/14.0 cost 1000
   user@switch2# rstp interface ge-0/0/14.0 mode point-to-point
   user@switch2# rstp interface ge-0/0/18.0 cost 1000
   user@switch2# rstp interface ge-0/0/18.0 mode point-to-point

Step-by-Step Procedure

If Switch 2 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 2:

1. Enable graceful Routing Engine switchover (GRES):

   [edit chassis redundancy]
user@switch2# set graceful-switchover

2. Configure the switch to always synchronize configuration changes between the Routing Engines:

[edit system]
user@switch2# set commit synchronize

If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

[edit ethernet-switching-options]
user@switch2# set nonstop-bridging

NOTE: This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results

Check the results of the configuration:

user@switch2> show configuration

interfaces {
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
    ge-0/0/18 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members [10 20 30 40];
                }
            }
        }
    }
}
protocols {
    rstp {
        bridge-priority 32k;
        interface ge-0/0/14.0 {
            cost 1000;
            mode point-to-point;
        }
        interface ge-0/0/18.0 {
            cost 1000;
            mode point-to-point;
        }
    }
}
To quickly configure RSTP and nonstop bridging on Switch 3, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/26 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/28 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/24 unit 0 family ethernet-switching port-mode trunk
set protocols rstp bridge-priority 8k
set protocols rstp interface ge-0/0/26.0 cost 1000
set protocols rstp interface ge-0/0/26.0 mode point-to-point
set protocols rstp interface ge-0/0/28.0 cost 1000
set protocols rstp interface ge-0/0/28.0 mode point-to-point
set protocols rstp interface ge-0/0/24.0 cost 1000
set protocols rstp interface ge-0/0/24.0 mode point-to-point
```
If Switch 3 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 3, copy the following commands and paste them into the switch terminal window:

```plaintext
set chassis redundancy graceful switchover
set system commit synchronize
set ethernet-switching-options nonstop-bridging
```

### Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 3:

1. Configure the VLANs `voice-vlan`, `employee-vlan`, `guest-vlan`, and `camera-vlan`:
   ```plaintext
   [edit vlans]
   user@switch3# set voice-vlan description "Voice VLAN"
   user@switch3# set voice-vlan vlan-id 10
   user@switch3# set employee-vlan description "Employee VLAN"
   user@switch3# set employee-vlan vlan-id 20
   user@switch3# set guest-vlan description "Guest VLAN"
   user@switch3# set guest-vlan vlan-id 30
   user@switch3# set camera-vlan description "Camera VLAN"
   user@switch3# set camera-vlan vlan-id 40
   ``

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:
   ```plaintext
   [edit interfaces]
   user@switch3# set ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch3# set ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch3# set ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]
   ``

3. Configure the port mode for the interfaces:
   ```plaintext
   [edit interfaces]
   user@switch3# set ge-0/0/26 unit 0 family ethernet-switching port-mode trunk
   user@switch3# set ge-0/0/28 unit 0 family ethernet-switching port-mode trunk
   user@switch3# set ge-0/0/24 unit 0 family ethernet-switching port-mode trunk
   ``

4. Configure RSTP on the switch:
   ```plaintext
   [edit protocols]
   user@switch3# rstp bridge-priority 8k
   user@switch3# rstp interface ge-0/0/26 cost 1000
   user@switch3# rstp interface ge-0/0/26 mode point-to-point
   user@switch3# rstp interface ge-0/0/28 cost 1000
   user@switch3# rstp interface ge-0/0/28 mode point-to-point
   user@switch3# rstp interface ge-0/0/24 cost 1000
   user@switch3# rstp interface ge-0/0/24 mode point-to-point
   ```

### Step-by-Step Procedure

If Switch 3 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 3:

1. Enable graceful Routing Engine switchover (GRES):
   ```plaintext
   [edit chassis redundancy]
   user@switch3# set graceful-switchover
   ``

2. Configure the switch to always synchronize configuration changes between the Routing Engines:
   ```plaintext
   [edit system]
   user@switch3# set commit synchronize
   ```
If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

   ```plaintext
   [edit ethernet-switching-options]
   user@switch3# set nonstop-bridging
   ```

   **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results  Check the results of the configuration:

   ```plaintext
   user@switch3> show configuration
   interfaces {
     ge-0/0/26 {
       unit 0 {
         family ethernet-switching {
           port-mode trunk;
           vlan { members [10 20 30 40]; }
         }
       }
     }
     ge-0/0/28 {
       unit 0 {
         family ethernet-switching {
           port-mode trunk;
           vlan { members [10 20 30 40]; }
         }
       }
     }
     ge-0/0/24 {
       unit 0 {
         family ethernet-switching {
           port-mode trunk;
           vlan { members [10 20 30 40]; }
         }
       }
     }
   }
   }
   protocols {
     rstp {
       bridge-priority 8k;
       interface ge-0/0/26.0 {
         cost 1000;
     ```
mode point-to-point;
}
interface ge-0/0/28.0 {
  cost 1000;
  mode point-to-point;
}
interface ge-0/0/24.0 {
  cost 1000;
  mode point-to-point;
}
}
bridge-priority 8k;
}

vlans {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}

system {
  commit synchronize;
}

chassis {
  redundancy {
    graceful-switchover;
  }
  ethernet-switching-options {
    nonstop-bridging;
  }
}

**Configuring RSTP and Nonstop Bridging on Switch 4**

**CLI Quick Configuration**

To quickly configure RSTP and nonstop bridging on Switch 4, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]
```
set interfaces ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/23 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/19 unit 0 family ethernet-switching port-mode trunk
set protocols rstp bridge-priority 16k
set protocols rstp interface ge-0/0/23.0 cost 1000
set protocols rstp interface ge-0/0/23.0 mode point-to-point
set protocols rstp interface ge-0/0/19.0 cost 1000
set protocols rstp interface ge-0/0/19.0 mode point-to-point

If Switch 4 includes dual Routing Engines, configure NSB. To quickly configure nonstop bridging on Switch 4, copy the following commands and paste them into the switch terminal window:

set chassis redundancy graceful switchover
set system commit synchronize
set ethernet-switching-options nonstop-bridging

Step-by-Step Procedure

To configure RSTP and nonstop bridging on Switch 4:

1. Configure the VLANs voice-vlan, employee-vlan, guest-vlan, and camera-vlan:

   [edit vlans]
   user@switch4# set voice-vlan description "Voice VLAN"
   user@switch4# set voice-vlan vlan-id 10
   user@switch4# set employee-vlan description "Employee VLAN"
   user@switch4# set employee-vlan vlan-id 20
   user@switch4# set guest-vlan description "Guest VLAN"
   user@switch4# set guest-vlan vlan-id 30
   user@switch4# set camera-vlan description "Camera VLAN"
   user@switch4# set camera-vlan vlan-id 40

2. Configure the VLANs on the interfaces, including support for the Ethernet switching protocol:

   [edit interfaces]
   user@switch4# set ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch4# set ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]

3. Configure the port mode for the interfaces:

   [edit interfaces]
   user@switch4# set ge-0/0/23 unit 0 family ethernet-switching port-mode trunk
   user@switch4# set ge-0/0/19 unit 0 family ethernet-switching port-mode trunk

4. Configure RSTP on the switch:

   [edit protocols]
   user@switch4# rstp bridge-priority 16k
   user@switch4# rstp interface all cost 1000
   user@switch4# rstp interface ge-0/0/23.0 cost 1000
   user@switch4# rstp interface ge-0/0/23.0 mode point-to-point
   user@switch4# rstp interface ge-0/0/19.0 cost 1000
   user@switch4# rstp interface ge-0/0/19.0 mode point-to-point

Step-by-Step Procedure

If Switch 4 includes dual Routing Engines, configure nonstop bridging. To configure NSB on Switch 4:

1. Enable graceful Routing Engine switchover (GRES):

   [edit chassis redundancy]
   user@switch4# set graceful-switchover
2. Configure the switch to always synchronize configuration changes between the Routing Engines:

   [edit system]
   user@switch4# set commit synchronize

   If you try to commit a configuration in which nonstop bridging is configured but synchronization of configuration changes is not configured, the configuration is not committed.

3. Enable nonstop bridging:

   [edit ethernet-switching-options]
   user@switch4# set nonstop-bridging

   **NOTE:** This process enables NSB for all NSB-supported Layer 2 protocols on the switch, including RSTP.

Results  Check the results of the configuration:

   user@switch4> show configuration
   interfaces {
     ge-0/0/23 {
       unit 0 {
         family ethernet-switching {
           port-mode trunk;
           vlan {
             members [10 20 30 40];
           }
         }
       }
     }
     ge-0/0/19 {
       unit 0 {
         family ethernet-switching {
           port-mode trunk;
           vlan {
             members [10 20 30 40];
           }
         }
       }
     }
   }
   protocols {
     rstp {
       bridge-priority 16k;
       interface ge-0/0/23.0 {
         cost 1000;
         mode point-to-point;
       }
       interface ge-0/0/19.0 {
         cost 1000;
         mode point-to-point;
       }
     }
   }
Verifying RSTP Configuration on Switch 1

Purpose

Verify the RSTP configuration on Switch 1.

Verification

To confirm that the configuration is working properly, perform these tasks on both Routing Engines:

- Verifying RSTP Configuration on Switch 1 on page 4328
- Verifying RSTP Configuration on Switch 2 on page 4329
- Verifying RSTP Configuration on Switch 3 on page 4329
- Verifying RSTP Configuration on Switch 4 on page 4330
**Action**  Use the operational mode command:

```
user@switch1> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/13.0</td>
<td>128:526</td>
<td>128:526</td>
<td>16384.0019e25040e0</td>
<td>1000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/9.0</td>
<td>128:522</td>
<td>128:522</td>
<td>32768.0019e2503d20</td>
<td>1000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>128:524</td>
<td>128:524</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
</tbody>
</table>

**Meaning**  Refer to the topology in Figure 65 on page 4315. The operational mode command `show spanning-tree interface` shows that `ge-0/0/13.0` is in a forwarding state. The other interfaces on Switch 1 are blocking.

**Verifying RSTP Configuration on Switch 2**

**Purpose**  Use this procedure to verify the RSTP configuration on both Switch 2 Routing Engines.

**Action**  Use the operational mode command:

```
user@switch2> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/14.0</td>
<td>128:527</td>
<td>128:527</td>
<td>32768.0019e2503d20</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
<td>128:529</td>
<td>128:529</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
</tbody>
</table>

**Meaning**  Refer to the topology in Figure 65 on page 4315. The operational mode command `show spanning-tree interface` shows that `ge-0/0/18.0` is in a forwarding state and is the root port.

**Verifying RSTP Configuration on Switch 3**

**Purpose**  Use this procedure to verify the RSTP configuration on both Switch 3 Routing Engines.
Action

Use the operational mode commands:

```
user@switch3> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/26.0</td>
<td>128:539</td>
<td>128:539</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/28.0</td>
<td>128:541</td>
<td>128:541</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/24.0</td>
<td>128:537</td>
<td>128:537</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Meaning

Refer to the topology in Figure 65 on page 4315. The operational mode command `show spanning-tree interface` shows that no interface is the root interface.

**Verifying RSTP Configuration on Switch 4**

Purpose

Use this procedure to verify the RSTP configuration on both Switch 4 Routing Engines.

Action

Use the operational mode commands:

```
user@switch4> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/23.0</td>
<td>128:536</td>
<td>128:536</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/19.0</td>
<td>128:532</td>
<td>128:532</td>
<td>16384.0019e25040e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Meaning

Refer to the topology in Figure 65 on page 4315. The operational mode command `show spanning-tree interface` shows that interface `ge-0/0/23.0` is the root interface and forwarding.

**Related Documentation**

- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Understanding RSTP for EX Series Switches on page 4300

**Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches**

Multiple Spanning Tree Protocol (MSTP) is used to create a loop-free topology in networks using multiple spanning tree regions, each region containing multiple spanning-tree instances (MSTIs). MSTIs provide different paths for different VLANs. This functionality facilitates better load sharing across redundant links.

Up to 64 MSTI instances can be created for an EX Series switch, and each MSTI can support up to 4094 VLANs.
This example describes how to configure MSTP on four EX Series switches:

- Requirements on page 4331
- Overview and Topology on page 4331
- Configuring MSTP on Switch 1 on page 4334
- Configuring MSTP on Switch 2 on page 4336
- Configuring MSTP on Switch 3 on page 4339
- Configuring MSTP on Switch 4 on page 4342
- Verification on page 4344

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.0 or later for EX Series switches
- Four EX Series switches

Before you configure the switches for MSTP, be sure you have:

- Installed the four switches. See Connecting and Configuring an EX Series Switch (J-Web Procedure).
- Performed the initial software configuration on all switches. See Installing and Connecting an EX3200 Switch.

Overview and Topology

When the number of VLANs grows in a network, MSTP provides a more efficient way of creating a loop-free topology using MSTIs. Each MSTI in the spanning tree domain maintains its own tree. Each tree can be mapped to different links, utilizing bandwidth that would be unavailable to a single tree. MSTIs reduce demand on system resources.
Figure 66: Network Topology for MSTP

NOTE: You can configure MSTP on logical or physical interfaces. This example shows MSTP configured on logical interfaces.

Table 539: Components of the Topology for Configuring MSTP on EX Series Switches

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch 1</strong></td>
<td>The following ports on Switch 1 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/9 is connected to Switch 2</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/13 is connected to Switch 4</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/11 is connected to Switch 3</td>
</tr>
<tr>
<td><strong>Switch 2</strong></td>
<td>The following ports on Switch 2 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/14 is connected to Switch 1</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/18 is connected to Switch 3</td>
</tr>
</tbody>
</table>
Table 539: Components of the Topology for Configuring MSTP on EX Series Switches (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 3</td>
<td>The following ports on Switch 3 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/26 is connected to Switch 1</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/28 is connected to Switch 2</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/24 is connected to Switch 4</td>
</tr>
<tr>
<td>Switch 4</td>
<td>The following ports on Switch 4 are connected in this way:</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/19 is connected to Switch 1</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/23 is connected to Switch 3</td>
</tr>
</tbody>
</table>
| VLAN names and tag IDs | voice-vlan, tag 10  
|                    | employee-vlan, tag 20  
|                    | guest-vlan, tag 30  
|                    | camera-vlan, tag 40                                                                 |
| MSTIs             | 1  
|                   | 2                                                                 |

The topology in Figure 66 on page 4332 shows a Common Internal Spanning Tree (CIST). The CIST is a single spanning tree connecting all devices in the network. The switch with the highest priority is elected as the root bridge of the CIST.

Also in an MSTP topology are ports that have specific roles:

- The root port is responsible for forwarding data to the root bridge.
- The alternate port is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The designated port forwards data to the downstream network segment or device.
- The backup port is a backup port for the designated port. When a designated port goes down, the backup port becomes the active designated port and starts forwarding data.

In this example, one MSTP region, **region1**, contains Switch 1, Switch 2, Switch 3, and Switch 4. Within the region, four VLANs are created:

- The voice-vlan supports voice traffic and has a VLAN tag identifier of 10.
- The employee-vlan supports data traffic and has a VLAN tag identifier of 20.
- The guest-vlan supports guest VLAN traffic (for supplicants that fail 802-1X authentication) and has a VLAN tag identifier of 30.
- The camera-vlan supports video traffic and has a VLAN tag identifier of 40.

The VLANs are associated with specific interfaces on each of the four switches. Two MSTIs, 1 and 2, are then associated with the VLAN tag identifiers, and some MSTP parameters, such as cost, are configured on each switch.
### Configuring MSTP on Switch 1

**CLI Quick Configuration**

To quickly configure interfaces and MSTP on Switch 1, copy the following commands and paste them into the switch terminal window:

```plaintext
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/11 unit 0 family ethernet-switching port-mode trunk
set protocols mstp configuration-name region1
set protocols mstp bridge-priority 16k
set protocols mstp interface ge-0/0/13.0 cost 1000
set protocols mstp interface ge-0/0/13.0 mode point-to-point
set protocols mstp interface ge-0/0/9.0 cost 1000
set protocols mstp interface ge-0/0/9.0 mode point-to-point
set protocols mstp interface ge-0/0/11.0 cost 1000
set protocols mstp interface ge-0/0/11.0 mode point-to-point
set protocols msti 1 bridge-priority 16k
set protocols msti 1 vlan [10 20]
set protocols mstp msti 1 link 0/0/11 cost 4000
set protocols mstp msti 2 bridge-priority 8k
set protocols mstp msti 2 vlan [30 40]
```

**Step-by-Step Procedure**

To configure interfaces and MSTP on Switch 1:

1. **Configure the VLANs** `voice-vlan`, `employee-vlan`, `guest-vlan`, and `camera-vlan`:
   ```plaintext
   [edit vlans]
   user@switch1# set voice-vlan description "Voice VLAN"
   user@switch1# set voice-vlan vlan-id 10
   user@switch1# set employee-vlan description "Employee VLAN"
   user@switch1# set employee-vlan vlan-id 20
   user@switch1# set guest-vlan description "Guest VLAN"
   user@switch1# set guest-vlan vlan-id 30
   user@switch1# set camera-vlan description "Camera VLAN"
   user@switch1# set guest-vlan vlan-id 40
   ```

2. **Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol**:
   ```plaintext
   [edit interfaces]
   user@switch1# set ge-0/0/13 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch1# set ge-0/0/9 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch1# set ge-0/0/11 unit 0 family ethernet-switching vlan members [10 20 30 40]
   ```

3. **Configure the port mode for the interfaces**:
   ```plaintext
   [edit interfaces]
   ```
4. Configure MSTP on the switch, including the two MSTIs:

```
[edit protocols]
user@switch1# mstp configuration-name region1
user@switch1# mstp bridge-priority 16k
user@switch1# mstp interface ge-0/0/13.0 cost 1000
user@switch1# mstp interface ge-0/0/13.0 mode point-to-point
user@switch1# mstp interface ge-0/0/9.0 cost 1000
user@switch1# mstp interface ge-0/0/9.0 mode point-to-point
user@switch1# mstp interface ge-0/0/11.0 cost 4000
user@switch1# mstp interface ge-0/0/11.0 mode point-to-point
user@switch1# mstp msti1 bridge-priority 16k
user@switch1# mstp msti1 vlan [10 20]
user@switch1# mstp msti1 interface ge-0/0/11.0 cost 4000
user@switch1# mstp msti2 bridge-priority 8k
user@switch1# mstp msti2 vlan [30 40]
```

**Results**  
Check the results of the configuration:

```
user@switch1> show configuration
interfaces {
  ge-0/0/13 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/9 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
        }
      }
    }
  }
  ge-0/0/11 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
```
members 30;
members 40;
}
}
}
}
}
}
}
}
}
protocols {
mstp {
   configuration-name region1;
   bridge-priority 16k;
   interface ge-0/0/13.0 {
      cost 1000;
      mode point-to-point;
   }
   interface ge-0/0/9.0 {
      cost 1000;
      mode point-to-point;
   }
   interface ge-0/0/11.0 {
      cost 4000;
      mode point-to-point;
   }
   msti1 {
      bridge-priority 16k;
      vlan [ 10 20 ];
      interface ge-0/0/11.0 {
         cost 4000;
      }
   }
   msti2 {
      bridge-priority 8k;
      vlan [ 30 40 ];
   }
}
vlans {
   voice-vlan {
      vlan-id 10;
   }
   employee-vlan {
      vlan-id 20;
   }
   guest-vlan {
      vlan-id 30;
   }
   camera-vlan {
      vlan-id 40;
   }
}

Configuring MSTP on Switch 2

To quickly configure interfaces and MSTP on Switch 2, copy the following commands and paste them into the switch terminal window:
[edit]
To configure interfaces and MSTP on Switch 2:

1. Configure the VLANs `voice-vlan`, `employee-vlan`, `guest-vlan`, and `camera-vlan`:

   ```
   [edit vlans]
   user@switch2# set voice-vlan description "Voice VLAN"
   user@switch2# set voice-vlan vlan-id 10
   user@switch2# set employee-vlan description "Employee VLAN"
   user@switch2# set employee-vlan vlan-id 20
   user@switch2# set guest-vlan description "Guest VLAN"
   user@switch2# set guest-vlan vlan-id 30
   user@switch2# set camera-vlan description "Camera VLAN"
   user@switch2# set camera-vlan vlan-id 40
   ```

2. Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol:

   ```
   [edit interfaces]
   user@switch2# set ge-0/0/14 unit 0 family ethernet-switching vlan members [10 20 30 40]
   user@switch2# set ge-0/0/18 unit 0 family ethernet-switching vlan members [10 20 30 40]
   ```

3. Configure the port mode for the interfaces:

   ```
   [edit interfaces]
   user@switch2# set ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
   user@switch2# set ge-0/0/18 unit 0 family ethernet-switching port-mode trunk
   ```

4. Configure MSTP on the switch, including the two MSTIs:

   ```
   [edit protocols]
   user@switch2# mstp configuration-name region1
   user@switch2# mstp bridge-priority 32k
   user@switch2# mstp interface ge-0/0/14 unit 0 family ethernet-switching port-mode trunk
   user@switch2# mstp interface ge-0/0/18 unit 0 family ethernet-switching port-mode trunk
   ```
user@switch2# mstp msti 2 bridge-priority 4k
user@switch2# mstp msti 2 vlan [30 40]

Results
Check the results of the configuration:

user@switch2> show configuration
interfaces {
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
    ge-0/0/18 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
}
protocols {
    mstp {
        configuration-name region1;
        bridge-priority 32k;
        interface ge-0/0/14.0 {
            cost 1000;
            mode point-to-point;
        }
        interface ge-0/0/18.0 {
            cost 1000;
            mode point-to-point;
        }
        msti 1 {
            bridge-priority 32k;
            vlan [10 20];
        }
        msti 2 {
            bridge-priority 4k;
            vlan [30 40];
        }
    }
}
vlans {
    voice-vlan {
        vlan-id 10;
    }
    employee-vlan {
        vlan-id 20;
    }
    guest-vlan {
        vlan-id 30;
    }
    camera-vlan {
        vlan-id 40;
    }
}

Configuring MSTP on Switch 3

To quickly configure interfaces and MSTP on Switch 3, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/26 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/28 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/24 unit 0 family ethernet-switching port-mode trunk
set protocols mstp configuration-name region1
set protocols mstp bridge-priority 8k
set protocols mstp interface ge-0/0/26.0 cost 1000
set protocols mstp interface ge-0/0/26.0 mode point-to-point
set protocols mstp interface ge-0/0/28.0 cost 1000
set protocols mstp interface ge-0/0/28.0 mode point-to-point
set protocols mstp interface ge-0/0/24.0 cost 1000
set protocols mstp interface ge-0/0/24.0 mode point-to-point
set protocols mstp msti 1 bridge-priority 4k
set protocols mstp msti 1 vlan [10 20]
set protocols mstp msti 2 bridge-priority 16k
set protocols mstp msti 2 vlan [30 40]
```
To configure interfaces and MSTP on Switch 3:

1. Configure the VLANs voice-vlan, employee-vlan, guest-vlan, and camera-vlan:

```plaintext
[edit vlans]
user@switch3# set voice-vlan description "Voice VLAN"
user@switch3# set voice-vlan vlan-id 10
user@switch3# set employee-vlan description "Employee VLAN"
user@switch3# set employee-vlan vlan-id 20
user@switch3# set guest-vlan description "Guest VLAN"
user@switch3# set guest-vlan vlan-id 30
user@switch3# set camera-vlan description "Camera VLAN"
user@switch3# set guest-vlan vlan-id 40
```

2. Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol:

```plaintext
[edit interfaces]
user@switch3# set ge-0/0/26 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set ge-0/0/28 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch3# set ge-0/0/24 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```plaintext
[edit interfaces]
user@switch3# set ge-0/0/26 unit 0 family ethernet-switching port-mode trunk
user@switch3# set ge-0/0/28 unit 0 family ethernet-switching port-mode trunk
user@switch3# set ge-0/0/24 unit 0 family ethernet-switching port-mode trunk
```

4. Configure MSTP on the switch, including the two MSTIs:

```plaintext
[edit protocols]
user@switch3# mstp configuration-name region1
user@switch3# mstp bridge-priority 8k
user@switch3# mstp interface ge-0/0/26.0 cost 1000
user@switch3# mstp interface ge-0/0/26.0 mode point-to-point
user@switch3# mstp interface ge-0/0/28.0 cost 1000
user@switch3# mstp interface ge-0/0/28.0 mode point-to-point
user@switch3# mstp interface ge-0/0/24.0 cost 1000
user@switch3# mstp interface ge-0/0/24.0 mode point-to-point
user@switch3# mstp interface all cost 1000
user@switch3# mstp msti1 bridge-priority 4k
user@switch3# mstp msti1 vlan [10 20]
user@switch3# mstp msti2 bridge-priority 16k
user@switch3# mstp msti2 vlan [30 40]
```

Results

Check the results of the configuration:

```plaintext
user@switch3> show configuration
interfaces {
  ge-0/0/26 {
    unit 0 {
      family ethernet-switching {
        port-mode trunk;
        vlan {
          members 10;
          members 20;
          members 30;
          members 40;
```


```plaintext
ge-0/0/28 {
  unit 0 {
    family ethernet-switching {
      port-mode trunk;
      vlan {
        members 10;
        members 20;
        members 30;
        members 40;
      }
    }
  }
}

ge-0/0/24 {
  unit 0 {
    family ethernet-switching {
      port-mode trunk;
      vlan {
        members 10;
        members 20;
        members 30;
        members 40;
      }
    }
  }
}

protocols {
    mstp {
      configuration-name region1;
      bridge-priority 8k;
      interface ge-0/0/26.0 {
        cost 1000;
        mode point-to-point;
      }
      interface ge-0/0/28.0 {
        cost 1000;
        mode point-to-point;
      }
      interface ge-0/0/24.0 {
        cost 1000;
        mode point-to-point;
      }
      msti 1 {
        bridge-priority 4k;
        vlan [ 10 20 ];
      }
      msti 2 {
        bridge-priority 16k;
        vlan [ 30 40 ];
      }
    }
  }
```
Configuring MSTP on Switch 4

CLI Quick Configuration

To quickly configure interfaces and MSTP on Switch 4, copy the following commands and paste them into the switch terminal window:

```
[edit]
set vlans voice-vlan description "Voice VLAN"
set vlans voice-vlan vlan-id 10
set vlans employee-vlan description "Employee VLAN"
set vlans employee-vlan vlan-id 20
set vlans guest-vlan description "Guest VLAN"
set vlans guest-vlan vlan-id 30
set vlans camera-vlan description "Camera VLAN"
set vlans camera-vlan vlan-id 40
set interfaces ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]
set interfaces ge-0/0/23 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/0/19 unit 0 family ethernet-switching port-mode trunk
set protocols mstp configuration-name region1
set protocols mstp bridge-priority 16k
set protocols mstp interface ge-0/0/23.0 cost 1000
set protocols mstp interface ge-0/0/23.0 mode point-to-point
set protocols mstp interface ge-0/0/19.0 cost 1000
set protocols mstp interface ge-0/0/19.0 mode point-to-point
set protocols mstp msti 1 bridge-priority 16k
set protocols mstp msti 1 vlan [10 20]
set protocols mstp msti 2 bridge-priority 32k
set protocols mstp msti 2 vlan [30 40]
```

Step-by-Step Procedure

To configure interfaces and MSTP on Switch 4:

1. Configure the VLANs voice-vlan, employee-vlan, guest-vlan, and camera-vlan:

```
[edit vlans]
user@switch4# set voice-vlan description "Voice VLAN"
user@switch4# set voice-vlan vlan-id 10
user@switch4# set employee-vlan description "Employee VLAN"
user@switch4# set employee-vlan vlan-id 20
user@switch4# set guest-vlan description "Guest VLAN"
user@switch4# set guest-vlan vlan-id 30
user@switch4# set camera-vlan description "Camera VLAN"
user@switch4# set guest-vlan vlan-id 40
```
2. Configure the VLANs on the interfaces, including support for the Ethernet Switching protocol:

```
[edit interfaces]
user@switch4# set ge-0/0/23 unit 0 family ethernet-switching vlan members [10 20 30 40]
user@switch4# set ge-0/0/19 unit 0 family ethernet-switching vlan members [10 20 30 40]
```

3. Configure the port mode for the interfaces:

```
[edit interfaces]
user@switch4# set ge-0/0/23 unit 0 family ethernet-switching port-mode trunk
user@switch4# set ge-0/0/19 unit 0 family ethernet-switching port-mode trunk
```

4. Configure MSTP on the switch, including the two MSTIs:

```
[edit protocols]
user@switch4# mstp configuration-name region1
user@switch4# mstp bridge-priority 16k
user@switch4# mstp interface all cost 1000
user@switch4# mstp interface ge-0/0/23.0 cost 1000
user@switch4# mstp interface ge-0/0/23.0 mode point-to-point
user@switch4# mstp interface ge-0/0/19.0 cost 1000
user@switch4# mstp interface ge-0/0/19.0 mode point-to-point
user@switch4# mstp msti 1 bridge-priority 16k
user@switch4# mstp msti 1 vlan [10 20]
user@switch4# mstp msti 2 bridge-priority 32k
user@switch4# mstp msti 2 vlan [30 40]
```

**Results**

Check the results of the configuration:

```
user@switch4> show configuration
interfaces {
    ge-0/0/23 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
    ge-0/0/19 {
        unit 0 {
            family ethernet-switching {
                port-mode trunk;
                vlan {
                    members 10;
                    members 20;
                    members 30;
                    members 40;
                }
            }
        }
    }
}
```

*/
protocols {
  mstp {
    configuration-name region1;
    bridge-priority 16k;
    interface ge-0/0/23.0 {
      cost 1000;
      mode point-to-point;
    }
    interface ge-0/0/19.0 {
      cost 1000;
      mode point-to-point;
    }
    msti 1 {
      bridge-priority 16k;
      vlan [ 10 20 ];
    }
    msti 2 {
      bridge-priority 32k;
      vlan [ 30 40 ];
    }
  }
}
vlans {
  voice-vlan {
    vlan-id 10;
  }
  employee-vlan {
    vlan-id 20;
  }
  guest-vlan {
    vlan-id 30;
  }
  camera-vlan {
    vlan-id 40;
  }
}

Verification
To confirm that the configuration is working properly, perform these tasks:

- Verifying MSTP Configuration on Switch 1 on page 4344
- Verifying MSTP Configuration on Switch 2 on page 4346
- Verifying MSTP Configuration on Switch 3 on page 4348
- Verifying MSTP Configuration on Switch 4 on page 4350

Verifying MSTP Configuration on Switch 1

Purpose Verify the MSTP configuration on Switch 1.
Action

Use the operational mode commands:

```
user@switch1> show spanning-tree interface
Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/13.0</td>
<td>128:527</td>
<td>128:525</td>
<td>16384.0019e25040e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/9.0</td>
<td>128:529</td>
<td>128:513</td>
<td>32768.0019e2503d20</td>
<td>1000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>128:531</td>
<td>128:513</td>
<td>8192.0019e25051e0</td>
<td>4000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/13.0</td>
<td>128:527</td>
<td>128:525</td>
<td>16385.0019e25040e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/9.0</td>
<td>128:529</td>
<td>128:513</td>
<td>32769.0019e2503d20</td>
<td>1000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>128:531</td>
<td>128:513</td>
<td>4097.0019e25051e0</td>
<td>4000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/13.0</td>
<td>128:527</td>
<td>128:527</td>
<td>8194.0019e25044e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/9.0</td>
<td>128:529</td>
<td>128:513</td>
<td>4098.0019e2503d20</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/11.0</td>
<td>128:531</td>
<td>128:531</td>
<td>8194.0019e25044e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

user@switch1> show spanning-tree bridge
STP bridge parameters
Context ID : 0
Enabled protocol : MSTP

STP bridge parameters for CIST
Root ID : 8192.00:19:e2:50:51:e0
Root cost : 0
Root port : ge-0/0/13.0
CIST regional root : 8192.00:19:e2:50:51:e0
CIST internal root cost : 2000
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 18
Message age : 0
Number of topology changes : 3
Time since last topology change : 921 seconds
Local parameters
Bridge ID : 16384.00:19:e2:50:44:e0
Extended system ID : 0
Internal instance ID : 0

STP bridge parameters for MST1 1
MSTI regional root : 4097.00:19:e2:50:51:e0
Root cost : 2000
Root port : ge-0/0/13.0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 18
Local parameters
Bridge ID : 16385.00:19:e2:50:44:e0
Extended system ID : 0
Internal instance ID : 1

STP bridge parameters for MSTI 2
MSTI regional root : 4098.00:19:e2:50:3d:20
Root cost : 1000
Root port : ge-0/0/9.0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 19

Local parameters
Bridge ID : 8194.00:19:e2:50:44:e0
Extended system ID : 0
Internal instance ID : 2

Meaning The operational mode command `show spanning-tree interface` displays spanning-tree domain information such as the designated port and the port roles.

The operational mode command `show spanning-tree bridge` displays the spanning-tree domain information at either the bridge level or interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

**Verifying MSTP Configuration on Switch 2**

**Purpose** Verify the MSTP configuration on Switch 2.
Action

Use the operational mode commands:

```
user@switch2> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/14.0</td>
<td>128:513</td>
<td>32768.0019e2503d20</td>
<td>1000 FWD DESG</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
<td>128:519</td>
<td>8192.0019e25051e0</td>
<td>1000 FWD ROOT</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/14.0</td>
<td>128:513</td>
<td>32769.0019e2503d20</td>
<td>1000 FWD DESG</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
<td>128:519</td>
<td>4097.0019e25051e0</td>
<td>1000 FWD ROOT</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/14.0</td>
<td>128:513</td>
<td>4098.0019e2503d20</td>
<td>1000 FWD DESG</td>
</tr>
<tr>
<td>ge-0/0/18.0</td>
<td>128:519</td>
<td>4098.0019e2503d20</td>
<td>1000 FWD DESG</td>
</tr>
</tbody>
</table>

```
user@switch2> show spanning-tree bridge
```

STP bridge parameters

- Context ID: 0
- Enabled protocol: MSTP

STP bridge parameters for CIST

- Root ID: 8192.00:19:e2:50:51:e0
- Root cost: 0
- Root port: ge-0/0/18.0
- CIST regional root: 8192.00:19:e2:50:51:e0
- CIST internal root cost: 1000
- Hello time: 2 seconds
- Maximum age: 20 seconds
- Forward delay: 15 seconds
- Hop count: 19
- Message age: 0
- Number of topology changes: 1
- Time since last topology change: 782 seconds

Local parameters

- Bridge ID: 32768.00:19:e2:50:3d:20
- Extended system ID: 0
- Internal instance ID: 0

STP bridge parameters for MSTI 1

- MSTI regional root: 4097.00:19:e2:50:51:e0
- Root cost: 1000
- Root port: ge-0/0/18.0
- Hello time: 2 seconds
- Maximum age: 20 seconds
- Forward delay: 15 seconds
- Hop count: 19

Local parameters

- Bridge ID: 32769.00:19:e2:50:3d:20
Meaning  The operational mode command `show spanning-tree interface` displays spanning-tree domain information such as the designated port and the port roles.

The operational mode command `show spanning-tree bridge` displays the spanning-tree domain information at either the bridge level or interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

**Verifying MSTP Configuration on Switch 3**

**Purpose**  Verify the MSTP configuration on Switch 3.
**Action**

Use the operational mode commands:

```
user@switch3> show spanning-tree interface
```

---

**Spanning tree interface parameters for instance 0**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/26.0</td>
<td>128:513</td>
<td>128:513</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/28.0</td>
<td>128:515</td>
<td>128:515</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/24.0</td>
<td>128:517</td>
<td>128:517</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

---

**Spanning tree interface parameters for instance 1**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/26.0</td>
<td>128:513</td>
<td>128:513</td>
<td>4097.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/28.0</td>
<td>128:515</td>
<td>128:515</td>
<td>4097.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/24.0</td>
<td>128:517</td>
<td>128:517</td>
<td>4097.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

---

**Spanning tree interface parameters for instance 2**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/26.0</td>
<td>128:513</td>
<td>128:531</td>
<td>8194.0019e25044e0</td>
<td>1000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/28.0</td>
<td>128:515</td>
<td>128:519</td>
<td>4098.0019e2503d20</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/24.0</td>
<td>128:517</td>
<td>128:517</td>
<td>16386.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

---

```
user@switch3> show spanning-tree bridge
```

**STP bridge parameters**

Context ID : 0
Enabled protocol : MSTP

**STP bridge parameters for CIST**

- Root ID : 8192.00:19:e2:50:51:e0
- CIST regional root : 8192.00:19:e2:50:51:e0
- CIST internal root cost : 0
- Hello time : 2 seconds
- Maximum age : 20 seconds
- Forward delay : 15 seconds
- Number of topology changes : 3
- Time since last topology change : 843 seconds

**Local parameters**

- Bridge ID : 8192.00:19:e2:50:51:e0
- Extended system ID : 0
- Internal instance ID : 0

**STP bridge parameters for MSTI 1**

- MSTI regional root : 4097.00:19:e2:50:51:e0
- Hello time : 2 seconds
- Maximum age : 20 seconds
- Forward delay : 15 seconds

**Local parameters**

- Bridge ID : 4097.00:19:e2:50:51:e0
- Extended system ID : 0
- Internal instance ID : 1

**STP bridge parameters for MSTI 2**

- MSTI regional root : 4098.00:19:e2:50:3d:20
Meaning  The operational mode command `show spanning-tree interface` displays spanning-tree domain information such as the designated port and the port roles.

The operational mode command `show spanning-tree bridge` displays the spanning-tree domain information at either the bridge level or interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

**Verifying MSTP Configuration on Switch 4**

**Purpose**  Verify the MSTP configuration on Switch 4.
Action  Use the operational mode commands:

```
user@switch4> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/23.0</td>
<td>128:523</td>
<td>128:517</td>
<td>8192.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/19.0</td>
<td>128:525</td>
<td>128:525</td>
<td>16384.0019e25040e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/23.0</td>
<td>128:523</td>
<td>128:517</td>
<td>4097.0019e25051e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/19.0</td>
<td>128:525</td>
<td>128:525</td>
<td>16385.0019e25040e0</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/23.0</td>
<td>128:523</td>
<td>128:517</td>
<td>16386.0019e25051e0</td>
<td>1000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/19.0</td>
<td>128:525</td>
<td>128:527</td>
<td>8194.0019e25040e0</td>
<td>1000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
</tbody>
</table>

```
user@switch4> show spanning-tree bridge
```

STP bridge parameters

- Context ID: 0
- Enabled protocol: MSTP

STP bridge parameters for CIST

- Root ID: 8192.00:19:e2:50:51:e0
- Root cost: 0
- Root port: ge-0/0/23.0
- CIST regional root: 8192.00:19:e2:50:51:e0
- CIST internal root cost: 1000
- Hello time: 2 seconds
- Maximum age: 20 seconds
- Forward delay: 15 seconds
- Hop count: 19
- Message age: 0
- Number of topology changes: 4
- Time since last topology change: 887 seconds

Local parameters

- Bridge ID: 16384.00:19:e2:50:40:e0
- Extended system ID: 0
- Internal instance ID: 0

STP bridge parameters for MSTI 1

- MSTI regional root: 4097.00:19:e2:50:51:e0
- Root cost: 1000
- Root port: ge-0/0/23.0
- Hello time: 2 seconds
- Maximum age: 20 seconds
- Forward delay: 15 seconds
- Hop count: 19

Local parameters

- Bridge ID: 16385.00:19:e2:50:40:e0
- Extended system ID: 0
### STP bridge parameters for MSTI 2

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSTI regional root</td>
<td>4098.00:19:e2:50:3d:20</td>
</tr>
<tr>
<td>Root cost</td>
<td>2000</td>
</tr>
<tr>
<td>Root port</td>
<td>ge-0/0/19.0</td>
</tr>
<tr>
<td>Hello time</td>
<td>2 seconds</td>
</tr>
<tr>
<td>Maximum age</td>
<td>20 seconds</td>
</tr>
<tr>
<td>Forward delay</td>
<td>15 seconds</td>
</tr>
<tr>
<td>Hop count</td>
<td>18</td>
</tr>
<tr>
<td>Local parameters</td>
<td></td>
</tr>
<tr>
<td>Bridge ID</td>
<td>32770.00:19:e2:50:40:e0</td>
</tr>
<tr>
<td>Extended system ID</td>
<td>0</td>
</tr>
<tr>
<td>Internal instance ID</td>
<td>2</td>
</tr>
</tbody>
</table>

### Meaning

The operational mode command `show spanning-tree interface` displays spanning-tree domain information such as the designated port and the port roles.

The operational mode command `show spanning-tree bridge` displays the spanning-tree domain information at either the bridge level or interface level. If the optional interface name is omitted, all interfaces in the spanning-tree domain are displayed.

### Related Documentation

- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding MSTP for EX Series Switches on page 4298

### Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). All spanning-tree protocols use a special type of frame called a bridge protocol data unit (BPDU) to communicate. Other devices—PC bridging applications, for example, also use BPDUs and generate their own BPDUs. These different BPDUs are not compatible. When BPDUs generated by spanning-tree protocols are transmitted to a device that uses another type of BPDU, they can cause problems on the device. Similarly, if switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of STP miscalculations.

This example configures BPDU protection on an EX Series switch that uses RSTP. The upstream configuration is done on the edge interfaces, where outside BPDUs are often received from other devices:

- Requirements on page 4353
- Overview and Topology on page 4353
- Configuration on page 4354
- Verification on page 4355
Requirements

This example uses the following hardware and software components:

- Two EX Series switches in an RSTP topology
- Junos OS Release 9.1 or later for EX Series switches

Before you configure the interfaces on Switch 2 for BPDU protection, be sure you have:

- RSTP enabled on the switches.

NOTE: By default, RSTP is enabled on all EX Series switches.

Overview and Topology

The switches, being in an RSTP topology, support a loop-free network through the exchange of BPDUs. Receipt of outside BPDUs in an STP, RSTP, or MSTP topology, however, can lead to network outages by triggering an STP misconfiguration. To prevent such outages, enable BPDU protection on STP interfaces that could receive outside BPDUs. If an outside BPDU is received on a BPDU-protected interface, the interface shuts down to prevent the outside BPDU from accessing the STP interface.

Figure 67 on page 4354 shows the topology for this example. In this example, Switch 1 and Switch 2 are configured for RSTP and create a loop-free topology. The interfaces on Switch 2 are edge access ports—edge access ports frequently receive outside BPDUs generated by PC applications.

This example configures interface ge-0/0/5.0 and interface ge-0/0/6.0 as edge ports on Switch 2, and then configures BPDU protection on those ports. With BPDU protection enabled, these interfaces shut down when they encounter an outside BPDU sent by the PCs connected to Switch 2.
Figure 67: BPDU Protection Topology

Table 540 on page 4354 shows the components that will be configured for BPDU protection.

Table 540: Components of the Topology for Configuring BPDU Protection on EX Series Switches

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 1 (Distribution Layer)</td>
<td>Switch 1 is connected to Switch 2 on a trunk interface.</td>
</tr>
<tr>
<td>Switch 2 (Access Layer)</td>
<td>Switch 2 has these access ports that require BPDU protection:</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/5.0</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/6.0</td>
</tr>
</tbody>
</table>

This configuration example uses RSTP topology. You also can configure BPDU protection for STP or MSTP topologies at the [edit protocols (mstp | stp)] hierarchy level.

Configuration

To configure BPDU protection on two access interfaces:

**CLI Quick Configuration**

Quickly configure RSTP on the two Switch 2 interfaces, and then configure BPDU protection on all edge ports on Switch 2 by copying the following commands and pasting them into the switch terminal window:

```
[edit]
set protocols rstp interface ge-0/0/5.0 edge
set protocols rstp interface ge-0/0/6.0 edge
set protocols rstp bpdublock-on-edge
```
To configure RSTP on the two Switch 2 interfaces, and then configure BPDU protection:

1. Configure RSTP on interface `ge-0/0/5.0` and interface `ge-0/0/6.0`, and configure them as edge ports:

   ```
   [edit protocols rstp]
   user@switch# set interface ge-0/0/5.0 edge
   user@switch# set interface ge-0/0/6.0 edge
   ```

2. Configure BPDU protection on all edge ports on this switch:

   ```
   [edit protocols rstp]
   user@switch# set bpdu-block-on-edge
   ```

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/5.0 [ 
  edge; 
  ]
interface ge-0/0/6.0 [ 
  edge; 
  ]
bpdu-block-on-edge;
```

To confirm that the configuration is working properly:

- Displaying the Interface State Before BPDU Protection Is Triggered on page 4355
- Verifying That BPDU Protection Is Working Correctly on page 4356

### Displaying the Interface State Before BPDU Protection Is Triggered

Before BPDUs can be received from PCs connected to interface `ge-0/0/5.0` and interface `ge-0/0/6.0`, confirm the interface state.

**Action**

Use the operational mode command:

```
user@switch> show spanning-tree interface
```

**Meaning**

The output from the operational mode command `show spanning-tree interface` shows that `ge-0/0/5.0` and interface `ge-0/0/6.0` are ports in a forwarding state.
Verifying That BPDU Protection Is Working Correctly

Purpose
In this example, the PCs connected to Switch 2 start sending BPDUs to interface ge-0/0/5.0 and interface ge-0/0/6.0. Verify that BPDU protection is working on the interfaces.

Action
Use the operational mode command:

```
user@switch> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>128:513</td>
<td>128:513</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>128:514</td>
<td>128:514</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>128:515</td>
<td>128:515</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>128:516</td>
<td>128:516</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>128:517</td>
<td>128:517</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>128:518</td>
<td>128:518</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>128:519</td>
<td>128:519</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/7.0</td>
<td>128:520</td>
<td>128:1</td>
<td>16384.00aabbcc0348</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/8.0</td>
<td>128:521</td>
<td>128:521</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Meaning
When BPDUs are sent from the PCs to interface ge-0/0/5.0 and interface ge-0/0/6.0 on Switch 2, the output from the operational mode command `show spanning-tree interface` shows that the interfaces have transitioned to a BPDU inconsistent state. The BPDU inconsistent state causes the interfaces to shut down.

Disabling the BPDU protection configuration on an interface does not automatically re-enable the interface. However, if the `disable-timeout (Spanning Trees)` statement has been included in the BPDU configuration, the interface does return to service after the timer expires. Otherwise, you must use the operational mode command `clear ethernet-switching bpdu-error` to unblock and re-enable the interface.

If the PCs connected to Switch 2 send BPDUs to the interfaces again, BPDU protection is triggered once more and the interfaces transition back to the BPDU inconsistent state, causing them to shut down. In such cases, you need to find and repair the misconfiguration on the PCs that is sending BPDUs to Switch 2.

Related Documentation
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
Spanning-tree protocols support loop-free network communication through the exchange of a special type of frame called a bridge protocol data unit (BPDU). However, when BPDUs generated by spanning-tree protocols are communicated to devices on which spanning-tree protocols are not configured, these devices recognize the BPDUs, which can lead to network outages. You can, however, enable BPDU protection on switch interfaces to prevent BPDUs generated by spanning-tree protocols from passing through those interfaces. When BPDU protection is enabled, an interface shuts down or drops BPDU packets when any incompatible BPDU is encountered, thereby preventing the BPDUs generated by spanning-tree protocols from reaching the switch. When an interface is configured to drop BPDU packets, all traffic except the incompatible BPDUs can pass through the interface.

NOTE: The BPDU drop feature can be specified only on interfaces on which no spanning-tree protocol is configured.

This example configures BPDU protection on STP switch downstream interfaces that connect to two PCs:

- Requirements on page 4357
- Overview and Topology on page 4358
- Configuration on page 4359
- Verification on page 4361

Requirements

This example uses the following hardware and software components:

- One EX Series switch in an RSTP topology
- One EX Series switch that is not in any spanning-tree topology
- Junos OS Release 9.1 or later for EX Series switches

Before you configure the interfaces on Switch 2 for BPDU protection, be sure you have:

- Ensured that RSTP is operating on Switch 1.
- Disabled or enabled RSTP on Switch 2 (depending on the configuration that you plan to implement.)
If you want to enable the BPDU shutdown feature, then it is optional to disable spanning-tree protocols on the interface.

**NOTE:** By default, RSTP is enabled on all EX Series switches.

**Overview and Topology**

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). All spanning-tree protocols use a special type of frame called a BPDU to communicate. Other devices also use BPDUs—PC bridging applications, for example, generate their own BPDUs. These different BPDUs are not compatible. When BPDUs generated by spanning-tree protocols are transmitted to a device that uses another type of BPDU, they can cause problems on the device. Similarly, if switches within a spanning-tree topology receive BPDUs from other devices, network outages can occur because of the miscalculations caused by the outside BPDUs. Therefore, you must configure BPDU protection on interfaces in a spanning-tree topology to avoid network outages.

This example explains how to block outside BPDUs from reaching a switch interface connected to devices that are not part of the STP topology. This example addresses two scenarios. In the first scenario, an interface is shutdown when it encounters an outside BPDU. In the second scenario, an interface drops only BPDU packets while retaining the status of the interface as up and allowing all other traffic to pass through the interface.

Figure 67 on page 4354 shows the topology for this example. Switch 1 and Switch 2 are connected through a trunk interface. Switch 1 is configured for RSTP while Switch 2 has a spanning-tree protocol configured on it for the first scenario, and does not have a spanning-tree protocol configured on it for the second scenario.

In the first scenario, this example configures downstream BPDU protection on Switch 2 interfaces `ge-0/0/5.0` and `ge-0/0/6.0` when the default spanning-tree protocol (RSTP) is not disabled on these interfaces. When BPDU protection is enabled with the `shutdown` statement, the switch interfaces will shut down if BPDUs generated by the laptops attempt to access Switch 2.

In the second scenario, this example configures downstream BPDU protection on Switch 2 interfaces `ge-0/0/5.0` and `ge-0/0/6.0` when the default spanning-tree protocol (RSTP) is disabled on these interfaces. When BPDU protection is enabled with the `drop` statement, the switch interfaces drop only the BPDUs while allowing remaining traffic to pass through and retaining their status as up if BPDUs generated by the laptops attempt to access Switch 2.

**CAUTION:** When configuring BPDU protection on an interface without spanning trees connected to a switch with spanning trees, be careful that you do not configure BPDU protection on all interfaces. Doing so could prevent
BPDUs being received on switch interfaces (such as a trunk interface) that you intended to have receive BPDUs from a switch with spanning trees.

**Figure 68: BPDU Protection Topology**

Table 541 on page 4359 shows the components that will be configured for BPDU protection.

Table 541: Components of the Topology for Configuring BPDU Protection on EX Series Switches

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 1 (Distribution Layer)</td>
<td>Switch 1 is connected to Switch 2 through a trunk interface. Switch 1 is configured for RSTP.</td>
</tr>
<tr>
<td>Switch 2 (Access Layer)</td>
<td>Switch 2 has two downstream access ports connected to laptops:</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/5.0</td>
</tr>
<tr>
<td></td>
<td>• ge-0/0/6.0</td>
</tr>
</tbody>
</table>

**Configuration**

To configure BPDU protection on the interfaces:

**CLI Quick Configuration**

This is the first scenario that explains configuration for the `shutdown` statement. To quickly configure BPDU protection on Switch 2 for the `shutdown` statement, copy the following commands and paste them into the switch terminal window:

```
[edit]
```
To configure BPDU protection for the `shutdown` statement:

1. Configure the BPDU `shutdown` statement on the downstream interface `ge-0/0/5.0` on Switch 2:
   ```
   [edit ethernet-switching-options]
   user@switch# set bpdu-block interface ge-0/0/5.0 shutdown
   ```
2. Configure the BPDU `shutdown` statement on the downstream interface `ge-0/0/6.0` on Switch 2:
   ```
   [edit ethernet-switching-options]
   user@switch# set bpdu-block interface ge-0/0/6.0 shutdown
   ```

Check the results of the configuration:

```
user@switch> show ethernet-switching-options
bpdu-block {
  interface ge-0/0/5.0 {
    shutdown;
  }
  interface ge-0/0/6.0 {
    shutdown;
  }
}
```

This is the second scenario that explains configuration for the `drop` statement. To quickly configure BPDU protection on Switch 2 for the `drop` statement, copy the following commands and paste them into the switch terminal window:

```
[edit]
user@switch# set protocols rstp interface ge-0/0/5.0 disable
user@switch# set protocols rstp interface ge-0/0/6.0 disable
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/5.0 drop
user@switch# set ethernet-switching-options bpdu-block interface ge-0/0/6.0 drop
```

**NOTE:** You can also disable RSTP globally using the `delete protocols rstp`, the `set protocols rstp disable`, or the `set protocols rstp interface all disable` command.

To configure BPDU protection for the `drop` statement:

1. Disable RSTP on both the interfaces `ge-0/0/5.0` and `ge-0/0/6.0` interfaces:
   ```
   [edit]
   user@switch# set protocols rstp interface ge-0/0/5.0 disable
   user@switch# set protocols rstp interface ge-0/0/6.0 disable
   ```
2. Configure the BPDU `drop` statement on the downstream interface `ge-0/0/5.0` on Switch 2:
   ```
   [edit ethernet-switching-options]
   user@switch# set bpdu-block interface ge-0/0/5.0 drop
   ```
3. Configure the BPDU drop statement on the downstream interface ge-0/0/6.0 on Switch 2:

```
[edit ethernet-switching-options]
user@switch# set bpdu-block interface ge-0/0/6.0 drop
```

### Results
Check the results of the configuration:

```
user@switch> show protocols rstp
interface ge-0/0/5.0 {
   disable;
}
interface ge-0/0/6.0 {
   disable;
}
user@switch> show ethernet-switching-options
bpdu-block {
   interface ge-0/0/5.0 {
      drop;
   }
   interface ge-0/0/6.0 {
      drop;
   }
}
```

### Verification
To confirm that the configuration is working properly, perform these tasks:

- Displaying the Interface State Before BPDU Protection Is Triggered on page 4361
- Verifying That BPDU Shutdown Protection Is Working Correctly on page 4361
- Verifying That BPDU Drop Protection Is Working Correctly on page 4362

#### Displaying the Interface State Before BPDU Protection Is Triggered

**Purpose**
Before any BPDUs can be received on Switch 2 on either interface ge-0/0/5.0 or interface ge-0/0/6.0, confirm the state of those interfaces.

**Action**
Use the operational mode command `show ethernet-switching interfaces`:

```
user@switch> show ethernet-switching interfaces
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Tag</th>
<th>Tagging</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/5.0</td>
<td>up</td>
<td>default</td>
<td>untagged</td>
<td>untagged</td>
<td>unblocked</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>up</td>
<td>default</td>
<td>untagged</td>
<td>untagged</td>
<td>unblocked</td>
</tr>
</tbody>
</table>

**Meaning**
The output from the operational mode command `show ethernet-switching interfaces` shows that ge-0/0/5.0 and interface ge-0/0/6.0 are up and unblocked.

#### Verifying That BPDU Shutdown Protection Is Working Correctly

**Purpose**
Verify that BPDU protection is working correctly in the network by checking to see whether BPDUs have been blocked appropriately.
Action  Issue `show ethernet-switching interfaces` to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on Switch 2:

```
user@switch> show ethernet-switching interfaces
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Tag</th>
<th>Tagging</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/5.0</td>
<td>down</td>
<td>default</td>
<td>untagged</td>
<td>Disabled by bpdu-control</td>
<td></td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>down</td>
<td>default</td>
<td>untagged</td>
<td>Disabled by bpdu-control</td>
<td></td>
</tr>
</tbody>
</table>

Meaning  When the BPDUs sent from laptops reached interfaces `ge-0/0/5.0` and `ge-0/0/6.0` on Switch 2, the interfaces transitioned to a BPDU inconsistent state, shutting down the two interfaces to prevent BPDUs from reaching the laptops.

You need to re-enable the blocked interfaces. There are two ways to do this. If you included the statement `disable-timeout (Spanning Trees)` in the BPDU configuration, the interface returns to service after the timer expires. Otherwise, use the operational mode command `clear ethernet-switching bpdu-error` to unblock and re-enable `ge-0/0/5.0` and `ge-0/0/6.0`. This command will only re-enable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.

If BPDUs reach the downstream interfaces on Switch 2 again, BPDU protection is triggered again and the interfaces shut down. In such cases, you must find and repair the misconfiguration that is sending BPDUs to interfaces `ge-0/0/5.0` and `ge-0/0/6.0`.

**Verifying That BPDU Drop Protection Is Working Correctly**

Purpose  Verify that BPDU drop protection is working correctly in the network by checking to see whether BPDUs have been blocked appropriately.

Action  Issue `show ethernet-switching interfaces` to see what happened when the BPDUs reached the two interfaces configured for BPDU protection on Switch 2:

```
user@switch> show ethernet-switching interfaces
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>VLAN members</th>
<th>Tag</th>
<th>Tagging</th>
<th>Blocking</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/5.0</td>
<td>up</td>
<td>default</td>
<td>untagged</td>
<td>unblocked-xSTP bpdu</td>
<td>filter enabled</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>up</td>
<td>default</td>
<td>untagged</td>
<td>unblocked-xSTP bpdu</td>
<td>filter enabled</td>
</tr>
</tbody>
</table>

Meaning  When the BPDUs sent from laptops reached interfaces `ge-0/0/5.0` and `ge-0/0/6.0` on Switch 2, the interfaces dropped those BPDUs to prevent them from reaching Switch 2, and the state of both the interfaces is `up`.

Related Documentation

- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing interfaces from moving into a forwarding state that would result in a loop opening up in the network.

This example describes how to configure loop protection for an interface on an EX Series switch in an RSTP topology:

**Requirements**

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- Three EX Series switches in an RSTP topology

Before you configure the interface for loop protection, be sure you have:

- RSTP operating on the switches.

**NOTE:** By default, RSTP is enabled on all EX Series switches.

**Overview and Topology**

A loop-free network in spanning-tree topologies is supported through the exchange of a special type of frame called bridge protocol data unit (BPDU). Peer STP applications running on the switch interfaces use BPWDUs to communicate. Ultimately, the exchange of BPWDUs determines which interfaces block traffic (preventing loops) and which interfaces become root ports and forward traffic.

A blocking interface can transition to the forwarding state in error if the interface stops receiving BPWDUs from its designated port on the segment. Such a transition error can occur when there is a hardware error on the switch or software configuration error between the switch and its neighbor. When this happens, a loop opens up in the spanning tree.
Loops in a Layer 2 topology cause broadcast, unicast, and multicast frames to continuously circle the looped network. As a switch processes a flood of frames in a looped network, its resources become depleted and the ultimate result is a network outage.

**CAUTION:** An interface can be configured for either loop protection or root protection, but not for both.

Three EX Series switches are displayed in Figure 69 on page 4364. In this example, they are configured for RSTP and create a loop-free topology. Interface `ge-0/0/6` is blocking traffic between Switch 3 and Switch 1; thus, traffic is forwarded through interface `ge-0/0/7` on Switch 2. BPDUs are being sent from the root bridge on Switch 1 to both of these interfaces.

This example shows how to configure loop protection on interface `ge-0/0/6` to prevent it from transitioning from a blocking state to a forwarding state and creating a loop in the spanning-tree topology.

**Figure 69: Network Topology for Loop Protection**

Table 542 on page 4364 shows the components that will be configured for loop protection.

**Table 542: Components of the Topology for Configuring Loop Protection on EX Series Switches**

<table>
<thead>
<tr>
<th>Property</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 1</td>
<td>Switch 1 is the root bridge.</td>
</tr>
<tr>
<td>Switch 2</td>
<td>Switch 2 has the root port <code>ge-0/0/7</code>.</td>
</tr>
<tr>
<td>Switch 3</td>
<td>Switch 3 is connected to Switch 1 through interface <code>ge-0/0/6</code>.</td>
</tr>
</tbody>
</table>
A spanning-tree topology contains ports that have specific roles:

- The root port is responsible for forwarding data to the root bridge.
- The alternate port is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The designated port forwards data to the downstream network segment or device.

This configuration example uses an RSTP topology. However, you also can configure loop protection for STP or MSTP topologies at the [edit protocols (mstp | stp)] hierarchy level.

**Configuration**

To configure loop protection on an interface:

**CLI Quick Configuration**

To quickly configure loop protection on interface ge-0/0/6:

```plaintext
[edit]
set protocols rstp interface ge-0/0/6 bpdu-timeout-action block
```

**Step-by-Step Procedure**

To configure loop protection:

1. Configure interface ge-0/0/6 on Switch 3:

```plaintext
[edit protocols rstp]
user@switch# set interface ge-0/0/6 bpdu-timeout-action (Spanning Trees) block
```

**Results**

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/6.0 {
    bpdu-timeout-action {
        block;
    }
}
```

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Displaying the Interface State Before Loop Protection Is Triggered on page 4365
- Verifying That Loop Protection Is Working on an Interface on page 4366

**Displaying the Interface State Before Loop Protection Is Triggered**

Before loop protection is triggered on interface ge-0/0/6, confirm that the interface is blocking.
Action  Use the operational mode command:

user@switch> show spanning-tree interface

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>128:513</td>
<td>128:513</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>128:514</td>
<td>128:514</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>128:515</td>
<td>128:515</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>128:516</td>
<td>128:516</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>128:517</td>
<td>128:517</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>128:518</td>
<td>128:518</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>128:519</td>
<td>128:2</td>
<td>16384.00abbbcc0348</td>
<td>20000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
</tbody>
</table>

Meaning  The output from the operational mode command `show spanning-tree interface` shows that `ge-0/0/6.0` is the alternate port and in a blocking state.

Verifying That Loop Protection Is Working on an Interface

Purpose  Verify the loop protection configuration on interface `ge-0/0/6`. RSTP has been disabled on interface `ge-0/0/4` on Switch 1. This will stop BPDUs from being sent to interface `ge-0/0/6` and trigger loop protection on the interface.

Action  Use the operational mode command:

user@switch> show spanning-tree interface

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>128:513</td>
<td>128:513</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>128:514</td>
<td>128:514</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>128:515</td>
<td>128:515</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>128:516</td>
<td>128:516</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>128:517</td>
<td>128:517</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>128:518</td>
<td>128:518</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>128:519</td>
<td>128:2</td>
<td>16384.00abbbcc0348</td>
<td>20000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
</tbody>
</table>

Meaning  The operational mode command `show spanning-tree interface` shows that interface `ge-0/0/6.0` has detected that BPDUs are no longer being forwarded to it and has moved into a loop-inconsistent state. The loop-inconsistent state prevents the interface from transitioning to a forwarding state. The interface recovers and transitions back to its original state as soon as it receives BPDUs.

Related Documentation  •  Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches

EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). Root protection increases the efficiency of STP, RSTP, and MSTP by allowing network administrators to manually enforce the root bridge placement in the network.

This example describes how to configure root protection on an interface on an EX Series switch:

- Requirements on page 4367
- Overview and Topology on page 4367
- Configuration on page 4370
- Verification on page 4370

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.1 or later for EX Series switches
- Four EX Series switches in an RSTP topology

Before you configure the interface for root protection, be sure you have:

- RSTP operating on the switches.

**NOTE:** By default, RSTP is enabled on all EX Series switches.

Overview and Topology

Peer STP applications running on switch interfaces exchange a special type of frame called a bridge protocol data unit (BPDU). Switches communicate interface information using BPDU's to create a loop-free topology that ultimately determines the root bridge and which interfaces block or forward traffic in the spanning tree.
However, a root port elected through this process has the possibility of being wrongly elected. A user bridge application running on a PC can generate BPDUs, too, and interfere with root port election.

To prevent this from happening, enable root protection on interfaces that should not receive superior BPDUs from the root bridge and should not be elected as the root port. These interfaces are typically located on an administrative boundary and are designated ports.

When root protection is enabled on an interface:

- The interface is blocked from becoming the root port.
- Root protection is enabled for all STP instances on that interface.
- The interface is blocked only for instances for which it receives superior BPDUs. Otherwise, it participates in the spanning-tree topology.

![CAUTION: An interface can be configured for either root protection or loop protection, but not for both.]

Four EX Series switches are displayed in Figure 70 on page 4369. In this example, they are configured for RSTP and create a loop-free topology. Interface ge-0/0/7 on Switch 1 is a designated port on an administrative boundary. It connects to Switch 4. Switch 3 is the root bridge. Interface ge-0/0/6 on Switch 1 is the root port.

This example shows how to configure root protection on interface ge-0/0/7 to prevent it from transitioning to become the root port.
Figure 70: Network Topology for Root Protection

Table 543 on page 4369 shows the components that will be configured for root protection.

A spanning tree topology contains ports that have specific roles:

- The **root port** is responsible for forwarding data to the root bridge.
- The alternate port is a standby port for the root port. When a root port goes down, the alternate port becomes the active root port.
- The designated port forwards data to the downstream network segment or device.

This configuration example uses an RSTP topology. However, you also can configure root protection for STP or MSTP topologies at the `[edit protocols (mstp | stp)]` hierarchy level.

### Configuration

To configure root protection on an interface:

**CLI Quick Configuration**

To quickly configure root protection on interface `ge-0/0/7`, copy the following command and paste it into the switch terminal window:

```
[edit]
set protocols rstp interface ge-0/0/7 no-root-port
```

**Step-by-Step Procedure**

To configure root protection:

1. Configure interface `ge-0/0/7`:
   ```
   [edit protocols rstp]
   user@switch#
   set interface ge-0/0/7 no-root-port (Spanning Trees)
   ```

**Results**

Check the results of the configuration:

```
user@switch> show configuration protocols rstp
interface ge-0/0/7.0 {
    no-root-port;
}
```

**Verification**

To confirm that the configuration is working properly:

- **Displaying the Interface State Before Root Protection Is Triggered on page 4370**
- **Verifying That Root Protection Is Working on the Interface on page 4371**

### Displaying the Interface State Before Root Protection Is Triggered

**Purpose**

Before root protection is triggered on interface `ge-0/0/7`, confirm the interface state.
Action Use the operational mode command:

```
user@switch> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>128:513</td>
<td>128:513</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>128:514</td>
<td>128:514</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>128:515</td>
<td>128:515</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>128:516</td>
<td>128:516</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>128:517</td>
<td>128:517</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>128:518</td>
<td>128:2</td>
<td>16384.00aabbcc0348</td>
<td>20000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>128:519</td>
<td>128:1</td>
<td>16384.00aabbcc0348</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/7.0</td>
<td>128:520</td>
<td>128:520</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Meaning The output from the operational mode command `show spanning-tree interface` shows that `ge-0/0/7.0` is a designated port in a forwarding state.

Verifying That Root Protection Is Working on the Interface

Purpose A configuration change takes place on Switch 4. A smaller bridge priority on the Switch 4 causes it to send superior BPDUs to interface `ge-0/0/7`. Receipt of superior BPDUs on interface `ge-0/0/7` will trigger root protection. Verify that root protection is operating on interface `ge-0/0/7`.

Action Use the operational mode command:

```
user@switch> show spanning-tree interface
```

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated bridge ID</th>
<th>Designated Cost</th>
<th>Port</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>128:513</td>
<td>128:513</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/1.0</td>
<td>128:514</td>
<td>128:514</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>128:515</td>
<td>128:515</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/3.0</td>
<td>128:516</td>
<td>128:516</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>128:517</td>
<td>128:517</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/5.0</td>
<td>128:518</td>
<td>128:2</td>
<td>16384.00aabbcc0348</td>
<td>20000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-0/0/6.0</td>
<td>128:519</td>
<td>128:1</td>
<td>16384.00aabbcc0348</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>ge-0/0/7.0</td>
<td>128:520</td>
<td>128:520</td>
<td>32768.0019e2503f00</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Meaning The operational mode command `show spanning-tree interface` shows that interface `ge-0/0/7.0` has transitioned to a loop inconsistent state. The loop inconsistent state makes the interface block and prevents the interface from becoming a candidate for the root port. When the root bridge no longer receives superior STP BPDUs from the interface, the interface will recover and transition back to a forwarding state. Recovery is automatic.
**Related Documentation**

- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
- Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357
- Understanding Root Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 4311

**Configuration Tasks**

- Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure) on page 4372
- Configuring Spanning-Tree Protocols (J-Web Procedure) on page 4373
- Configuring VSTP (CLI Procedure) on page 4378
- Unblocking an Interface That Receives BPDUs in Error (CLI Procedure) on page 4380

**Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)**

NOTE: This procedure uses Junos OS for EX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. For ELS details, see “Getting Started with Enhanced Layer 2 Software” on page 3.

On EX Series switches running Rapid Spanning Tree Protocol (RSTP) (the default) or VLAN Spanning Tree Protocol (VSTP), you can force the original IEEE 802.1D Spanning Tree Protocol (STP) version to run in place of RSTP or VSTP. Configure the `force-version stp` statement for compatibility with older bridges that do not support RSTP or VSTP.

To force the spanning-tree protocol version to be the original IEEE 802.1D STP:

1. Enable IEEE 802.1D STP:

   ```
   [edit protocols]
   user@switch# set (rstp | vstp) force-version stp
   ```

   NOTE: After using the `force-version` statement to enable xSTP globally, apply the `force-version` statement for specific Layer 2 ports.

**Related Documentation**

- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 4306
- Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 4381
Configuring Spanning-Tree Protocols (J-Web Procedure)

For EX Series switches provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP). You can configure STP, RSTP, and MSTP by using the J-Web interface. You can configure bridge protocol data unit (BPDU) protection on interfaces to prevent them from receiving BPDUs that could result in STP misconfigurations, which could lead to network outages.

NOTE: In EX4300 switches, you can configure STP only by enabling RSTP and forcing it to act as STP. You need to select the Force STP check box from the RSTP configuration page.

To configure STP, MSTP, or RSTP for an EX Series switch by using the J-Web interface:

1. Select **Configure > Switching > Spanning Tree**.
   The Spanning Tree Configuration page displays the spanning-tree protocol configuration parameters and a list of interfaces configured for each spanning-tree protocol configuration.

   NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit. See Using the Commit Options to Commit Configuration Changes for details about all commit options.

2. Click one of the following options:
   - **Add**—Creates a spanning-tree protocol configuration.
     a. Select a protocol name.
     b. Enter information as described in Table 544 on page 4374.
     c. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.
   - **Edit**—Modifies a selected spanning-tree protocol configuration.
     a. Enter information as described in Table 544 on page 4374.
     b. Click **OK** to apply changes to the configuration or click **Cancel** to cancel without saving changes.
   - **Delete**—Deletes a selected spanning-tree protocol configuration.
### Table 544: Spanning-Tree Protocol Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol Name</td>
<td>Specifies the spanning-tree protocol type: STP, MSTP, or RSTP.</td>
<td>None.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables spanning-tree protocols on the interface.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>BPDU Protect</td>
<td>Specifies BPDU protection on all edge interfaces on the switch.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Specifies the number of seconds an interface waits before changing from spanning-tree learning and listening states to the forwarding state.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies the time interval in seconds at which the root bridge transmits configuration BPDUs.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Specifies the maximum-aging time in seconds for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Max Hops</td>
<td>(MSTP only) Specifies the number of hops in a region before the BPDU is discarded.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Configuration Name</td>
<td>(MSTP only) Specifies the MSTP region name carried in the MSTP BPDUs.</td>
<td>Type a name.</td>
</tr>
<tr>
<td>Revision Level</td>
<td>(MSTP only) Specifies the revision number of the MSTP configuration.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Force STP Version</td>
<td>Enables or disables STP.</td>
<td>To enable this option, select the check box.</td>
</tr>
</tbody>
</table>

**NOTE:** This option is supported only on EX4300 switches.
YourActionFunctionField

1. Click the **Ports** tab.
2. Choose one of the following options:
   - Click **Add** and select an interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.
   - Select an interface in the **Port/State** table and click **Edit**.
   - To delete an interface from the configuration, select it in the **Port/State** table and click **Remove**.

### Table 544: Spanning-Tree Protocol Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Specifies an interface for the spanning-tree protocol.</td>
<td>1. Click the <strong>Ports</strong> tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click <strong>Add</strong> and select an interface from the list. For an EX8200 Virtual Chassis configuration, select the member, FPC, and the interface from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select an interface in the <strong>Port/State</strong> table and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To delete an interface from the configuration, select it in the <strong>Port/State</strong> table and click <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Cost</td>
<td>Specifies the link cost to determine which bridge is the designated bridge and which interface is the designated interface.</td>
<td>Type a value.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the interface priority to determine which interface is elected as the root port.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>Disable Port</td>
<td>Disables the spanning-tree protocol on the interface.</td>
<td>To enable the option, select the check box.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is not supported on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Edge</td>
<td>Configures the interface as an edge interface. Edge interfaces immediately transition to a forwarding state.</td>
<td>To enable the option, select the check box.</td>
</tr>
<tr>
<td>No Root Port</td>
<td>Specifies an interface as a spanning-tree designated port. If the bridge receives superior STP BPDUs on a root-protected interface, that interface transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge that should not be the root bridge from being elected the root bridge. When the bridge stops receiving superior STP BPDUs on the root-protected interface, interface traffic is no longer blocked.</td>
<td>To enable the option, select the check box.</td>
</tr>
<tr>
<td>Interface Mode</td>
<td>Specifies the link mode.</td>
<td>1. To enable the option, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Point to Point</strong>—For a full-duplex link, the default link mode is point-to-point.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Shared</strong>—For a half-duplex link, the default link mode is shared.</td>
</tr>
</tbody>
</table>
### Table 544: Spanning-Tree Protocol Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPDU Timeout Action</td>
<td>Specifies the BPDU timeout action for the interface.</td>
<td>Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Block</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> For EX4300 switches, you can select one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Alarm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Block</td>
</tr>
<tr>
<td>MSTI (MSTP only)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSTI Name</td>
<td>Specifies a name (an MSTI ID) for the MST instance.</td>
<td>1. Click the MSTI tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Select an MSTI ID and click Edit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To delete an MSTI from the configuration, select the MSTI ID and click Remove.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> For EX4300 switches, the MSTI ID can be 1 through 64.</td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</td>
<td>Select a value from the list.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Specifies the VLAN for the MST instance.</td>
<td>In the VLAN box, choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Click Add, select a VLAN from the list, and click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To remove a VLAN association, select the VLAN ID, click Remove, and click OK.</td>
</tr>
</tbody>
</table>
### Table 544: Spanning-Tree Protocol Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>Specifies an interface for the MST instance.</td>
<td>1. In the Interfaces box, click <strong>Add</strong> and select an interface from the list, or select an interface from the list and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Specify the link cost to determine which bridge is the designated bridge and which interface is the designated interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Specify the interface priority to determine which interface is elected as the root port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. If you want to disable the interface, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete an interface configuration, select the interface, click <strong>Remove</strong>, and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

### Related Documentation

- **Configuring STP (CLI Procedure)**
  - Monitoring Spanning-Tree Protocols on page 4421
  - Unblocking an Interface That Receives BPDUs in Error (CLI Procedure) on page 4380
  - Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
  - Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  - Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
Configuring VSTP (CLI Procedure)

The default spanning-tree protocol for EX Series switches is Rapid Spanning Tree Protocol (RSTP). VLAN Spanning Tree Protocol (VSTP) is an alternate protocol that allows EX Series switches to run one or more Spanning Tree Protocol (STP) or RSTP instances for each VLAN on which VSTP is enabled. For networks with multiple VLANs, VSTP improves intelligent tree spanning by defining best paths within the VLANs instead of within the entire network.

NOTE: EX Series switches can have a maximum of 253 VLANs on VSTP. Therefore, to have as many spanning-tree protocol VLANs as possible, use both VSTP and RSTP. RSTP will then be applied to VLANs that exceed the limit for VSTP. Because RSTP is enabled by default, you just need to additionally enable VSTP.

You can configure VSTP for an interface at the global level (for all configured VLANs) or for a specific VLAN.

NOTE:

- If you configure VSTP on an interface at both the global and the specific VLAN level, the interface configuration that is defined at the specific VLAN level overrides the interface configuration that is defined at the global level.
- If you specify VSTP to be configured on an interface that is not configured to belong to the VLAN (or VLANs), an error message is displayed.
- Option `vlan all` is not supported in Junos OS Release 13.2X50.

To configure VSTP:

1. Configure VSTP on a group of VLANs, on all VLANs, or on a specific VLAN, or a specific interface within a VLAN, or on a specific interface that belongs to all VLANs:
   - To enable VSTP on multiple VLANs using a VLAN group:
     ```
     [edit protocols]
     user@switch# set vlan vlan-group group-name vlan vlan-id-range
     ```

     NOTE: EX Series switches can have a maximum of 253 VLANs on VSTP.

   - To enable VSTP on all VLANs:
NOTE: When you configure VSTP with the set protocol vstp vlan all command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration on your switch, you must set it separately with the set protocol vstp vlan 1 command.

[edit protocols]
user@switch# set vlan vlan all

NOTE: EX Series switches can have a maximum of 253 VLANs on VSTP. RSTP will then be applied to VLANs that exceed the limit for VSTP. Be sure that RSTP is also enabled (the default setting) when you use the command set vstp vlan all. In addition to this being a recommended practice, your configuration will not commit if VSTP is enabled on a switch with more than 253 VLANs.

• To enable VSTP on a VLAN using a single VLAN ID:
  [edit protocols]
  user@switch# set vlan vlan vlan-id

• To enable VSTP on a VLAN using a single VLAN name:
  [edit protocols]
  user@switch# set vlan vlan vlan-name

• To enable VSTP on an interface at the global level:
  [edit protocols]
  user@switch# set vlan vlan all interface interface-name

CAUTION: Ensure that the interface is a member of all VLANs before you add the interface to the VSTP configuration. If the interface is not a member of all VLANs, this VSTP configuration will fail when you try to commit it.

• To enable VSTP on an interface for a specific VLAN:
  [edit protocols]
  user@switch# set vlan vlan vlan-id-or-vlan-name interface interface-name

CAUTION: Ensure that the interface is a member of the specified VLAN before you add the interface to the VSTP configuration. If the interface is not a member of the specified VLAN, this VSTP configuration will fail when you try to commit it.

2. (Optional) Enable the Address Resolution Protocol (ARP) for faster MAC address recovery only if a routed VLAN interface (RVI) is configured:

• To enable ARP on VSTP for all VLANs:
To enable ARP on VSTP on a VLAN using a single VLAN ID:

```
[edit protocols]
user@switch# set vlan vlan all arp-on-stp
```

To enable ARP on VSTP on a VLAN using a single VLAN name:

```
[edit protocols]
user@switch# set vlan vlan-name arp-on-stp
```

**Unblocking an Interface That Receives BPDUs in Error (CLI Procedure)**

EX Series switches use bridge protocol data unit (BPDU) protection on interfaces to prevent them from receiving BPDUs that could trigger a spanning-tree misconfiguration. If BPDUs are received on a BPDU-protected interface, the interface either shuts down or transitions to a blocking state and stops forwarding frames. In the latter scenario, after the misconfiguration that triggered the BPDUs being sent to an interface is fixed in the topology, the interface can be unblocked and returned to service.

To unblock an interface and return it to service using the CLI:

- Automatically unblock an interface by configuring a timer that expires:

  ```
  [edit ethernet-switching-options]
  user@switch# set bpdu-block disable-timeout 30
  ```
  All interfaces on the switch will be re-enabled (unblocked) after the timer expires. However, once an interface on the switch receives a new spanning-tree protocol BPDU, the interface returns to the blocked state.

- Manually unblock an interface using the operational mode command:

  ```
  user@switch# clear ethernet-switching bpdu-error interface ge-0/0/6.0
  ```
  This command will only re-enable an interface but the BPDU configuration for the interface will continue to exist unless you remove the BPDU configuration explicitly.
Reverting to RSTP or VSTP from Forced IEEE 802.1D STP

On MX Series routers and EX Series switches on which Rapid Spanning Tree Protocol (RSTP) or VLAN Spanning Tree Protocol (VSTP) has been forced to run as the original IEEE 802.1D Spanning Tree Protocol (STP) version, you can revert back to RSTP or VSTP.

To revert from the forced instance of the original IEEE 802.1D STP version to the originally configured RSTP or VSTP version:

1. Remove the force-version statement from the following RSTP or VSTP configuration:

   ```
   user@host# delete protocols rstp force-version stp
   user@host# delete protocols vstp force-version stp
   ```

   Include this statement at the following hierarchy levels:

   - `[edit logical-systems routing-instance-name protocols rstp]`
   - `[edit protocols rstp]`
   - `[edit protocols vstp]`
   - `[edit routing-instances routing-instance-name protocols rstp]`
   - `[edit routing-instances routing-instance-name protocols vstp]`

2. Revert the forced IEEE 802.1D STP to run as the configured RSTP or VSTP:

   ```
   user@host# clear spanning-tree protocol-migration <interface interface-name> <routing-instance routing-instance-name>
   ```

   To revert the STP protocol globally, issue the statement without options (`clear spanning-tree protocol-migration`).

   To revert the STP protocol for the specified interface only, specify the `interface interface-name` option.

   To revert the STP protocol for a particular routing instance only, specify the `routing-instance routing-instance-name` option.

**Related Documentation**

- Spanning-Tree Protocols Supported
- RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 4306
- Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure) on page 4372
- Configuring Rapid Spanning-Tree Protocol
- Configuring VLAN Spanning-Tree Protocol

**Configuration Statements**

- `[edit protocols] Configuration Statement Hierarchy on EX Series Switches on page 4382`
[edit protocols] Configuration Statement Hierarchy on EX Series Switches

Each of the following topics lists the statements at a subhierarchy of the [edit protocols] hierarchy:

- [edit protocols bfd] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols bgp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols connections] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols dcbx] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols dot1x] Configuration Statement Hierarchy on EX Series Switches on page 1769
- [edit protocols igmp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols igmp-snooping] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols isis] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols lacp] Configuration Statement Hierarchy on EX Series Switches on page 2398
- [edit protocols link-management] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols lldp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols lldp-med] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols mld] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols mld-snooping] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols mpls] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols msdp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols mstp] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols mvpr] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols neighbor-discovery] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols oam] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols ospf] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols ospf3] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols pim] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols rip] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols ripng] Configuration Statement Hierarchy on EX Series Switches
- [edit protocols router-advertisement] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols router-discovery] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols rstp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols rsvp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols sflow] Configuration Statement Hierarchy on EX Series Switches on page 3708
• [edit protocols stp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols uplink-failure-detection] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols vrrp] Configuration Statement Hierarchy on EX Series Switches
• [edit protocols vstp] Configuration Statement Hierarchy on EX Series Switches

Related Documentation
• EX Series Switch Software Features Overview on page 27
• EX Series Virtual Chassis Software Features Overview on page 75
• Junos® OS for EX Series Switches, Release 13.2X50
**block (Spanning Trees)**

**Syntax**

```plaintext
block;
```

**Hierarchy Level**

- `edit protocols mstp interface (all | interface-name) bpdu-timeout-action`
- `edit protocols rstp interface (all | interface-name) bpdu-timeout-action`
- `edit protocols stp interface (all | interface-name) bpdu-timeout-action`
- `edit protocols vstp vlan vlan-id interface (all | interface-name) bpdu-timeout-action`

**Release Information**

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

**Description**

Configure loop protection on a specific interface.

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
- Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 4310
- Understanding VSTP for EX Series Switches on page 4306
bpdu-block

Syntax
bpdu-block {
  interface (all | [interface-name]);
  disable-timeout seconds;
}

Hierarchy Level
[edit ethernet-switching-options]

Release Information
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Configure BPDU protection on all interfaces or on a specified interface. If the interface receives incompatible BPDUs, it is disabled, or it is disabled for a specified timeout period (during which the BPDU packets are dropped).

The remaining statements are explained separately.

Required Privilege
Level
system—to view this statement in the configuration.
system-control—to add this statement to the configuration.

Related Documentation
• show spanning-tree bridge on page 4428
• show spanning-tree interface on page 4438
• clear ethernet-switching bpdu-error on page 4424
• Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357
• Unblocking an Interface That Receives BPDUs in Error (CLI Procedure) on page 4380
### bpdu-block-on-edge

**Syntax**
bpdu-block-on-edge;

**Hierarchy Level**
[edit protocols mstp],
[edit protocols rstp],
[edit protocols vstp]

**Release Information**
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.
Statement updated in Junos OS Release 11.1 for EX Series switches to change blocking behavior to port shutdown.

**Description**
Configure bridge protocol data unit (BPDU) protection on all edge ports of a switch.

**Required Privilege Level**
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

**Related Documentation**
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- clear ethernet-switching bpdushort error on page 4424
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
- Understanding VSTP for EX Series Switches on page 4306
bpdu-timeout-action (Spanning Trees)

**Syntax**

```
bpdu-timeout-action {
  block;
  log;
}
```

**Hierarchy Level**

- `edit protocols mstp interface (all | interface-name)`
- `edit protocols mstp interface (all | interface-name) arp-on-stp`
- `edit protocols rstp interface (all | interface-name)`
- `edit protocols rstp interface (all | interface-name) arp-on-stp`
- `edit protocols stp interface (all | interface-name)`
- `edit protocols stp interface (all | interface-name) arp-on-stp`
- `edit protocols vstp vlan vlan-id interface (all | interface-name)`
- `edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp`

**Release Information**

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

**Description**

Configure the BPDU timeout action on a specific interface. You must configure at least one action (`log`, `block`, or both).

The remaining statements are explained separately.

**Required Privilege**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- `show spanning-tree bridge` on page 4428
- `show spanning-tree interface` on page 4438
  - Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  - Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
  - Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
  - Understanding VSTP for EX Series Switches on page 4306
**bridge-priority (Spanning Trees)**

**Syntax**

`bridge-priority priority;`

**Hierarchy Level**

[edit protocols mstp],
[edit protocols mstp msti msti-id],
[edit protocols rstp],
[edit protocols stp],
[edit protocols vstp vlan vlan-id]

**Release Information**

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

**Description**

Configure the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.

**Default**

32,768

**Options**

`priority`—Bridge priority. It can be set only in increments of 4096.

- **Range:** 0 through 61,440
- **Default:** 32,768

**Required Privilege Level**

- `routing`—To view this statement in the configuration.
- `routing-control`—To add this statement to the configuration.

**Related Documentation**

- `show spanning-tree bridge` on page 4428
- `show spanning-tree interface` on page 4438
  - Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  - Understanding MSTP for EX Series Switches on page 4298
  - Understanding VSTP for EX Series Switches on page 4306
configuration-name (Spanning Trees)

Syntax  
configuration-name configuration-name;

Hierarchy Level  
[edit protocols mstp]

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  
Specify the configuration name. The configuration name is the MSTP region name carried in the MSTP BPDUs.

Required Privilege Level  
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding MSTP for EX Series Switches on page 4298
**cost (Spanning Trees)**

**Syntax**
```
cost cost;
```

**Hierarchy Level**
```
[edit protocols mstp interface (all | interface-name)],
[edit protocols mstp interface (all | interface-name) arp-on-stp],
[edit protocols mstp msti msti-id interface interface-name arp-on-stp],
[edit protocols mstp msti msti-id interface interface-name],
[edit protocols rstp interface (all | interface-name)],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp interface (all | interface-name)],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name)],
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
```

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

**Description**
For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure the link cost to control which bridge is the designated bridge and which interface is the designated interface.

**Default**
The link cost is determined by the link speed.

**Options**
- **cost**—Link cost associated with the port.

**Range**: 1 through 200,000,000

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
  - Understanding RSTP for EX Series Switches on page 4300
  - Understanding STP for EX Series Switches on page 4304
  - Understanding MSTP for EX Series Switches on page 4298
  - Understanding VSTP for EX Series Switches on page 4306

---

Copyright © 2013, Juniper Networks, Inc.
disable (Spanning Trees)

Syntax  
disable;

Hierarchy Level  
[edit protocols mpls],
[edit protocols mpls interface {all | interface-name}],
[edit protocols mstp],
[edit protocols mstp interface {all | interface-name}],
[edit protocols mstp interface {all | interface-name} arp-on-stp],
[edit protocols mstp msti msti-id vlan {vlan-id | vlan-name} interface {all | interface-name}],
[edit protocols mstp msti msti-id vlan {vlan-id | vlan-name} interface interface-name interface-name]
[edit protocols rstp],
[edit protocols rstp interface {all | interface-name}],
[edit protocols rstp interface {all | interface-name} arp-on-stp],
[edit protocols stp],
[edit protocols stp interface {all | interface-name}],
[edit protocols stp interface {all | interface-name} arp-on-stp],
[edit protocols vstp],
[edit protocols vstp vlan {vlan-id interface {all | interface-name}}]
[edit protocols vstp vlan {vlan-id interface {all | interface-name} interface-name interface-name} arp-on-stp]

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description  
Disable STP, MPLS, MSTP, RSTP, or VSTP on the switch or on a specific interface.

Required Privilege Level  
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation  
• show spanning-tree bridge on page 4428
• show spanning-tree interface on page 4438
  • Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  • Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
• Understanding STP for EX Series Switches on page 4304
• Understanding VSTP for EX Series Switches on page 4306
disable-timeout (Spanning Trees)

Syntax  disable-timeout timeout;

Hierarchy Level  [edit ethernet-switching-options bpdu-block]

Release Information  Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description  For interfaces configured for BPDU protection, specify the amount of time an interface receiving BPDUs is disabled.

Default  The disable timeout is not enabled.

Options  timeout —Amount of time, in seconds, the interface receiving BPDUs is disabled. Once the timeout expires, the interface is brought back into service.

Range: 10 through 3600 seconds

Required Privilege Level  system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation  • show spanning-tree bridge on page 4428

• show spanning-tree interface on page 4438

• Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330

• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313

• Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357

• Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 4308
edge (Spanning Trees)

Syntax

```plaintext
edge;
```

Hierarchy Level

```plaintext
[edit protocols mstp interface (all | interface-name)],
[edit protocols mstp interface (all | interface-name) arp-on-stp],
[edit protocols mstp msti msti-id interface interface-name],
[edit protocols mstp msti msti-id interface (all | interface-name) arp-on-stp],
[edit protocols rstp interface (all | interface-name)],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp interface (all | interface-name)],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name)],
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure interfaces as edge interfaces. Edge interfaces immediately transition to a forwarding state.

Default

Edge interfaces are not enabled.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding STP for EX Series Switches on page 4304
- Understanding VSTP for EX Series Switches on page 4306
## force-version (IEEE 802.1D STP)

**Syntax**

```plaintext
force-version stp;
```

**Hierarchy Level**

```plaintext
[edit logical-systems logical-system-name protocols (rstp | vstp)],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols (rstp | vstp)],
[edit protocols (rstp | vstp)],
[edit routing-instances routing-instance-name protocols (rstp | vstp)]
```

**Release Information**

Statement introduced in Junos OS Release 8.4.  
Support for logical systems added in Junos OS Release 9.6.

**Description**

Force the spanning-tree protocol version to be the original IEEE 802.1D STP.

**Required Privilege Level**

- routing—To view this statement in the configuration.  
- routing-control—To add this statement to the configuration.

**Related Documentation**

- [Spanning-Tree Protocols Supported](#)  
- [RSTP or VSTP Forced to Run as IEEE 802.1D STP on page 4306](#)  
- [Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure) on page 4372](#)  
- [Reverting to RSTP or VSTP from Forced IEEE 802.1D STP on page 4381](#)
### forward-delay (Spanning Trees)

**Syntax**
```
forward-delay seconds;
```

**Hierarchy Level**
```
[edit protocols mstp],
[edit protocols rstp],
[edit protocols stp],
[edit protocols vstp vlan vlan-id]
```

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

**Description**
For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specify how long a bridge interface remains in the listening and learning states before transitioning to the forwarding state.

**Default**
15 seconds

**Options**
- **seconds**—Number of seconds the bridge interface remains in the listening and learning states.
  - **Range:** 4 through 30 seconds
  - **Default:** 15 seconds

**Required Privilege Level**
- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

**Related Documentation**
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding MSTP for EX Series Switches on page 4298
- Understanding STP for EX Series Switches on page 4304
- Understanding VSTP for EX Series Switches on page 4306
hello-time (Spanning Trees)

Syntax hello-time seconds;

Hierarchy Level [edit protocols mstp], [edit protocols rstp], [edit protocols stp], [edit protocols vstp vlan vlan-id]


Description For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specify the time interval at which the root bridge transmits configuration BPDUs.

Default 2 seconds

Options seconds—Number of seconds between transmissions of configuration BPDUs.

Range: 1 through 10 seconds

Default: 2 seconds

Required Privilege Level routing—to view this statement in the configuration. routing-control—to add this statement to the configuration.

Related Documentation • show spanning-tree bridge on page 4428
• show spanning-tree interface on page 4438
  • Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  • Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
  • Understanding MSTP for EX Series Switches on page 4298
  • Understanding STP for EX Series Switches on page 4304
  • Understanding VSTP for EX Series Switches on page 4306
interface (BPDU Block)

Syntax

```
interface (all | [interface-name]) {
    (disable | drop | shutdown):
}
```

Hierarchy Level
[edit ethernet-switching-options bpdu-block]

Release Information
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description
Apply BPDU protection on all interfaces or on one or more specified interfaces.

Options
all—All interfaces.

[interface-name]—One or more Ethernet interface names.

The remaining statements are explained separately.

Required Privilege
system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation
• show spanning-tree bridge on page 4428
• show spanning-tree interface on page 4438
  • Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  • Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
  • Example: Configuring BPDU Protection on Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4357
interface (Spanning Trees)

Syntax  
interface interface-name  
                   { 
                     arp-on-stp;  
                     bpdu-timeout-action 
                        block;  
                        log;  
                     cost cost;  
                     disable;  
                     edge;  
                     mode mode;  
                     no-root-port;  
                     priority priority;  
                   }

Hierarchy Level  
[edit protocols mstp],  
[edit protocols mstp msti msti-id],  
[edit protocols rstp],  
[edit protocols stp],  
[edit protocols vstp vlan (all | vlan-id | vlan-name)]

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches.  
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.  
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description  
For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning 
Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure an interface.  
The edge, mode, and no-root-port options are not available at the [edit protocols mstp 
msti msti-id] hierarchy level.

Options  
interface-name—Name of an interface.  
The remaining statements are explained separately.

Required Privilege  
Level  
routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

Related Documentation  
- show spanning-tree bridge on page 4428  
- show spanning-tree interface on page 4438  
  - Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330  
  - Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313  
  - Example: Configuring Network Regions for VLANs with MSTP  
  - Example: Configuring Faster Convergence and Improving Network Stability with RSTP  
  - Configuring VSTP (CLI Procedure) on page 4378
log (Spanning Trees)

Syntax

```
log;
```

Hierarchy Level

```
[edit protocols mstp interface (all | interface-name) bpdu-timeout-action],
[edit protocols rstp interface (all | interface-name) bpdu-timeout-action],
[edit protocols stp interface (all | interface-name) bpdu-timeout-action],
[edit protocols vstp vlan_vlan-id interface (all | interface-name) bpdu-timeout-action]
```

Release Information

Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description

For interfaces configured for loop protection, configure the software to generate a message to be sent to the system log file `/var/log/messages` to record the loop-protection event.

Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- show spanning-tree bridge on page 4433
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Example: Configuring Loop Protection to Prevent Interfaces from Transitioning from Blocking to Forwarding in a Spanning Tree on EX Series Switches on page 4363
- Understanding Loop Protection for STP, RSTP, VSTP, and MSTP on EX Series Switches on page 4310
- Understanding VSTP for EX Series Switches on page 4306
max-age (Spanning Trees)

Syntax

```
max-age seconds;
```

Hierarchy Level

```
[edit protocols mstp],
[edit protocols rstp],
[edit protocols stp],
[edit protocols vstp vlan vlan-id]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specify the maximum age of received protocol BPDUs.

Default

20 seconds

Options

seconds—The maximum age of received protocol BPDUs.

Range: 6 through 40 seconds

Default: 20 seconds

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Related Documentation

- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
  - Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  - Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding MSTP for EX Series Switches on page 4298
- Understanding STP for EX Series Switches on page 4304
- Understanding VSTP for EX Series Switches on page 4306
max-hops (Spanning Trees)

Syntax
max-hops hops;

Hierarchy Level
[edit protocols mstp]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description
For Multiple Spanning Tree Protocol (MSTP), configure the maximum number of hops a BPDU can be forwarded in the MSTP region.

Default
20 hops

Options
hops — Number of hops the BPDU can be forwarded.

Range: 1 through 255 hops
Default: 20 hops

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• show spanning-tree bridge on page 4428
• show spanning-tree interface on page 4438
• Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
• Understanding MSTP for EX Series Switches on page 4298
## mode (Spanning Trees)

### Syntax

```
mode mode;
```

### Hierarchy Level

```
[edit protocols mstp interface (all | interface-name)],
[edit protocols mstp interface (all | interface-name) arp-on-stp],
[edit protocols mstp msti msti-id interface interface-name],
[edit protocols mstp msti msti-id interface interface-name) arp-on-stp],
[edit protocols rstp interface (all | interface-name)],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp interface (all | (all | interface-name)],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name)],
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
```

### Release Information

- Statement introduced in Junos OS Release 9.0 for EX Series switches.
- Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

### Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), configure the link mode to identify point-to-point links.

### Default

For a full-duplex link, the default link mode is **point-to-point**. For a half-duplex link, the default link mode is **shared**.

### Options

```
mode—Link mode:
  - point-to-point—Link is point to point.
  - shared—Link is shared media.
```

### Required Privilege Level

- **routing**—To view this statement in the configuration.
- **routing-control**—To add this statement to the configuration.

### Related Documentation

- [show spanning-tree bridge on page 4428](#)
- [show spanning-tree interface on page 4438](#)
  - Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  - Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding STP for EX Series Switches on page 4304
- Understanding VSTP for EX Series Switches on page 4306
**msti (Spanning Trees)**

**Syntax**
```
msti msti-id [vlan (vlan-id | vlan-name); interface interface-name {disable; cost cost; priority priority;};]
```

**Hierarchy Level**  
[edit protocols mstp]

**Release Information**  
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**  
Configure the Multiple Spanning Tree Instance (MSTI) identifier for Multiple Spanning Tree Protocol (MSTP). MSTI IDs are local to each region, so you can reuse the same MSTI ID in different regions.

**Default**  
MSTI is disabled.

**Options**
- `msti-id` — MSTI identifier.  
  - **Range:** 1 through 4094. The Common Instance Spanning Tree (CIST) is always MSTI 0.
  - The remaining statements are explained separately.

**Required Privilege Level**  
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Understanding MSTP for EX Series Switches on page 4298
**mstp (Spanning Trees)**

**Syntax**

```
mstp {
  bpdu-block-on-edge;
  bridge-priority priority;
  configuration-name name;
  disable;
  forward-delay seconds;
  hello-time seconds;
  interface ( all | interface-name ){
    arp-on-stp;
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  max-hops hops;
  msti msti-id {
    vlan (vlan-id | vlan-name);
    interface interface-name {
      disable;
      cost cost;
      priority priority;
    }
  }
  revision-level revision-level;
  traceoptions {
    file filename < files number > < size size > < no-stamp | world-readable | no-world-readable >;
    flag flag;
  }
}
```

**Hierarchy Level**
[edit protocols]

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure Multiple Spanning Tree Protocol (MSTP). MSTP is defined in the IEEE 802.1Q-2003 specification and is used to create a loop-free topology in networks with multiple spanning tree regions.

The statements are explained separately.

**Default**
MSTP is disabled.
Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• show spanning-tree bridge on page 4428
• show spanning-tree interface on page 4438
• Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
• Understanding MSTP for EX Series Switches on page 4298

no-root-port (Spanning Trees)

Syntax
no-root-port;

Hierarchy Level
[edit protocols mstp interface (all | interface-name)],
[edit protocols mstp interface (all | interface-name) arp-on-stp],
[edit protocols rstp interface (all | interface-name)],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp interface (all | interface-name)],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name)],
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]

Release Information
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description
Configure an interface to be a spanning-tree designated port. If the bridge receives superior STP bridge protocol data units (BPDUs) on a root-protected interface, that interface transitions to a root-prevented STP state (inconsistency state) and the interface is blocked. This blocking prevents a bridge from being elected the root bridge. When the bridge stops receiving superior STP BPDUs on the root-protected interface, interface traffic is no longer blocked.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
• show spanning-tree bridge on page 4428
• show spanning-tree interface on page 4438
• Example: Configuring Root Protection to Enforce Root Bridge Placement in Spanning Trees on EX Series Switches on page 4367
• Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
• Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
• Understanding VSTP for EX Series Switches on page 4306
priority (Spanning Trees)

Syntax

```
priority priority;
```

Hierarchy Level

```
[edit protocols mstp interface (all | interface-name)],
[edit protocols mstp;interface (all | interface-name) arp-on-stp],
[edit protocols mstp msti msti-id interface interface-name],
[edit protocols mstp msti msti-id interface interface-name arp-on-stp],
[edit protocols rstp interface (all | interface-name)],
[edit protocols rstp interface (all | interface-name) arp-on-stp],
[edit protocols stp interface (all | interface-name)],
[edit protocols stp interface (all | interface-name) arp-on-stp],
[edit protocols vstp vlan vlan-id interface (all | interface-name)],
[edit protocols vstp vlan vlan-id interface (all | interface-name) arp-on-stp]
```

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description

For Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), VLAN Spanning Tree Protocol (VSTP), or Multiple Spanning Tree Protocol (MSTP), specify the interface priority to control which interface is elected as the root port.

Default

The default value is 128.

Options

```
priority—Interface priority. The interface priority must be set in increments of 16.
```

Range: 0 through 240

Required Privilege Level

```
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.
```

Related Documentation

- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding STP for EX Series Switches on page 4304
- Understanding VSTP for EX Series Switches on page 4306
revision-level (Spanning Trees)

Syntax  revision-level revision-level;

Hierarchy Level  [edit protocols mstp]

Release Information  Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description  For Multiple Spanning Tree Protocol (MSTP), set the revision number of the MSTP configuration.

Default  The revision level is disabled.

Options  revision-level —Revision number of the MSTP region configuration.
         Range: 0 through 65535

Required Privilege  Level  routing—To view this statement in the configuration.
         routing-control—To add this statement to the configuration.

Related Documentation  • show spanning-tree bridge on page 4428
         • show spanning-tree interface on page 4438
         • Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
         • Understanding MSTP for EX Series Switches on page 4298
rstp (Spanning Trees)

Syntax
rstp {
  bpdu-block-on-edge;
  bridge-priority priority;
  disable;
  forward-delay seconds;
  hello-time seconds;
  interface (all | interface-name) {
    arp-on-stp;
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  traceoptions {
    file filename <files number > <size size> <no-stamp | no-world-readable | world-readable>;
    flag flag;
  }
}

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure Rapid Spanning Tree Protocol (RSTP). RSTP is defined in the IEEE 802.1D-2004 specification and is used to prevent loops in Layer 2 networks, which results in shorter convergence times than those provided by basic Spanning Tree Protocol (STP).

VSTP and RSTP can be configured concurrently. You can selectively configure up to 253 VLANs using VSTP; the remaining VLANs will be configured using RSTP. VSTP and RSTP are the only spanning-tree protocols that can be configured concurrently on the switch. See "Configuring VSTP (CLI Procedure)" on page 4378 for more information on configuring VSTP and RSTP concurrently.

BEST PRACTICE: Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that a spanning-tree protocol is running on all VLANs on your switch, even when your switch is supporting more than 253 VLANs.

The remaining statements are explained separately.
Default  RSTP is enabled on all Ethernet switching interfaces.

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding RSTP for EX Series Switches on page 4300
### stp (Spanning Trees)

**Syntax**
```
stp {
  bpdu-block-on-edge;
  bridge-priority priority;
  disable;
  forward-delay seconds;
  hello-time seconds;
  interface (all | interface-name) {
    arp-on-stp;
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  traceoptions {
    file filename <files number > <size size> <no-stamp | world-readable | no-world-readable>;
    flag flag;
  }
}
```

**Hierarchy Level**
[edit protocols]

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Configure Spanning Tree Protocol (STP). When you explicitly configure STP, the switches use the IEEE 802.1D 2004 specification, force version 0. This configuration runs a version of RSTP that is compatible with the classic, basic STP (defined in the IEEE 802.1D 1998 specification).

The remaining statements are explained separately.

**Default**
STP is disabled. By default, RSTP is enabled on all Ethernet switching ports.

**Required Privilege Level**
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring BPDU Protection on Edge Interfaces to Prevent STP Miscalculations on EX Series Switches on page 4352
- Configuring STP (CLI Procedure)
• Understanding STP for EX Series Switches on page 4304
traceoptions (Spanning Trees)

Syntax

traceoptions {
  file name <replace> <size size> <files number> <no-stamp>
  <(world-readable | no-world-readable)>
  flag flag <flag-modifier> <disable>;
}

Hierarchy Level

[edit protocols mpls],
[edit protocols mstp],
[edit protocols mvrp],
[edit protocols rstp],
[edit protocols stp],
[edit protocols vstp vlan vlan-id]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated in Junos OS Release 9.4 for EX Series switches to add VSTP support.

Description

Set protocol-level tracing options for MPLS, MVRP, STP, RSTP, MSTP, and VSTP.

Default

Traceoptions is disabled.

Options

disable—(Optional) Disable the tracing operation. One use of this option is to disable a
single operation when you have defined a broad group of tracing operations, such
as all.

file name—Name of the file to receive the output of the tracing operation. Enclose the
name in quotation marks. We recommend that you place STP tracing output in the
file /var/log/stp-log.

files number—(Optional) Maximum number of trace files. When a trace file named
trace-file reaches its maximum size, it is renamed trace-file .0, then trace-file .1, and
so on, until the maximum number of trace files is reached. Then, the oldest trace file
is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with
the size option.

Range: 2 through 1000 files

Default: 1 trace file

flag—Tracing operation to perform. To specify more than one tracing operation, include
multiple flag statements:

  • all—Trace all operations.
  • all-failures—Trace all failure conditions.
  • bpdu—Trace BPDU reception and transmission. Note that you must also use
    port-transmit-state-machine in order to log transmit operations.
  • bridge-detection-state-machine—Trace the bridge detection state machine.
• **error**—Trace all failure conditions.

• **events**—Trace events of the protocol state machine.

• **pdu**—Trace PDUs that were received and sent.

• **port-information-state-machine**—Trace the port information state machine.

• **port-migration-state-machine**—Trace the port migration state machine.

• **port-receive-state-machine**—Trace the port receive state machine.

• **port-role-select-state-machine**—Trace the port role selection state machine.

• **port-role-transit-state-machine**—Trace the port role transit state machine.

• **port-state-transit-state-machine**—Trace the port state transit state machine.

• **port-transmit-state-machine**—Trace the port transmit state machine.

• **ppmd**—Trace the state and events for the ppmd process.

• **socket**—Trace socket activity.

• **state-machine**—Trace state machine information.

• **state-machine-variables**—Trace when the state machine variables change.

• **timers**—Trace protocol timers.

• **topology-change-state-machine**—Trace the topology change state machine.

**no-stamp**—(Optional) Do not place timestamp information at the beginning of each line in the trace file.

**Default:** If you omit this option, timestamp information is placed at the beginning of each line of the tracing output.

**no-world-readable**—(Optional) Prevent any user from reading the log file.

**replace**—(Optional) Replace an existing trace file if there is one.

**Default:** If you do not include this option, tracing output is appended to an existing trace file.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named `trace-file` reaches this size, it is renamed `trace-file .0`. When the `trace-file` again reaches its maximum size, `trace-file .0` is renamed `trace-file .1` and `trace-file` is renamed `trace-file .0`. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
If you specify a maximum file size, you must also specify a maximum number of trace files with the files option.

**Syntax:** \( xk \) to specify KB, \( xm \) to specify MB, or \( xg \) to specify GB

**Range:** 10 KB through the maximum file size supported on your system

**Default:** 1 MB

**world-readable**—(Optional) Allow any user to read the log file.

**Required Privilege Level**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313
- Understanding MSTP for EX Series Switches on page 4298
- Understanding RSTP for EX Series Switches on page 4300
- Understanding STP for EX Series Switches on page 4304
- Understanding VSTP for EX Series Switches on page 4306
- Understanding Multiple VLAN Registration Protocol (MVRP) on EX Series Switches on page 2063
vlan (Spanning Trees)

Syntax
vlan (all | vlan-id | vlan-name) {
  bridge-priority priority;
  forward-delay seconds;
  hello-time seconds;
  interface interface-name {
    bpdu-timeout-action {
      block;
      log;
    }
    cost cost;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  traceoptions {
    file filename <files number > <size size> <no-stamp | world-readable |
      no-world-readable>;
    flag flag;
  }
}

Hierarchy Level
[edit protocols mstp msti msti-id]
[edit protocols vstp]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement updated with enhanced (? (CLI completion feature) functionality in Junos OS
Release 9.5 for EX Series switches.

Description
Configure the VLANs for a Multiple Spanning Tree Instance (MSTI) or VSTP instance.

NOTE: When you configure VSTP with the set protocol vstp vlan all
command, vlan-id 1 is excluded to be compatible with Cisco PVST+. If you
want vlan-id 1 to be included in VSTP, you must set it separately with the set
protocol vstp vlan1 command.

TIP: To display a list of all configured VLANs on the system, including VLANs
that are configured but not committed, type ? after vlan or vlans in your
configuration mode command line. Note that only one VLAN is displayed for
a VLAN range.

Default  Not enabled.
Options

- `vlan-id`—Numeric VLAN identifier.
- `vlan-name`—Name of the VLAN.

The remaining statements are explained separately.

**Required Privilege**

- **Level** routing—To view this statement in the configuration.
  - routing-control—To add this statement to the configuration.

**Related Documentation**

- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Understanding MSTP for EX Series Switches on page 4298
vlan (VSTP)

Syntax

```bash
vlan (all | vlan-id | vlan-name) {
  bridge-priority priority;
  forward-delay seconds;
  hello-time seconds;
  interface (all | interface-name) {
    bpdu-timeout-action {
      block;
      log;
    } cost cost;
    disable;
    edge;
    mode mode;
    no-root-port;
    priority priority;
  }
  max-age seconds;
  traceoptions {
    file filename <files number > <size size> <no-stamp | world-readable | no-world-readable>
    flag flag;
  }
}
```

Hierarchy Level

[edit protocols vstp]

Release Information

Statement introduced in Junos OS Release 9.4 for EX Series switches.
Statement updated with enhanced (CLI completion feature) functionality in Junos OS Release 9.5 for EX Series switches.
Option all introduced in Junos OS Release 10.0 for EX Series switches.

Description

Configure VSTP VLAN parameters.

NOTE: Option all is not supported in Junos OS Release 13.2X50.

TIP: To display a list of all configured VLANs on the system, including VLANs that are configured but not committed, type ? after vlan or vlans in your configuration mode command line. Note that only one VLAN is displayed for a VLAN range.

Options

- **all**—(Not supported on EX4300) All VLANs.
- **vlan-id**—Numeric VLAN identifier.
- **vlan-name**—Name of the VLAN.
The remaining statements are explained separately.

**Required Privilege**

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

**Related Documentation**

- [Understanding VSTP for EX Series Switches on page 4306](#)
vstp

Syntax
vstp {
  bpdu-block-on-edge;
  disable;
  force-version stp;
  vlan (all | vlan-id | vlan-name) {
    bridge-priority priority;
    forward-delay seconds;
    hello-time seconds;
    interface (all | interface-name) {
      arp-on-stp;
      bpdu-timeout-action {
        block;
        log;
      }
      cost cost;
      disable;
      edge;
      mode mode;
      no-root-port;
      priority priority;
    }
    max-age seconds;
    traceoptions {
      file filename <files number > <size > <no-stamp | no-world-readable >
      //world-readable>;
      flag flag;
    }
  }
}

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 9.4 for EX Series switches.

Description Configure VLAN Spanning Tree Protocol (VSTP). VSTP is used to prevent loops in Layer 2 networks on a per-VLAN basis.

You can have a maximum of 253 VSTP VLANs per switch.

If the number of VLANs on your switch exceeds the VSTP VLAN limit, you must use the vlan (Spanning Trees) statement to specify which VLANs or VLAN groups use VSTP. You also cannot use the vlan all option to configure VSTP when your switch has more than the maximum allowed VSTP VLANs. To ensure all VLANs are running a spanning-tree protocol, run RSTP for networks with large numbers of VLANs.

NOTE: When you configure VSTP with the set protocol vstp vlan all command, VLAN ID 1 is not set; it is excluded so that the configuration is compatible with Cisco PVST+. If you want VLAN ID 1 to be included in the VSTP configuration
on your switch, you must set it separately with the set protocol vstp vlan 1 command.

NOTE: Option vlan all is not supported in Junos OS Release 13.2X50.

BEST PRACTICE: Configure RSTP when you configure VSTP. RSTP overhead is minimal and this configuration ensures that some spanning tree protocol is running on all VLANs on your switch, even when your switch has more than the maximum number of allowed VSTP VLANs.

The remaining statements are explained separately.

Default VSTP is not enabled by default.

Required Privilege Level
- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Configuring VSTP (CLI Procedure) on page 4378
- Understanding VSTP for EX Series Switches on page 4306
CHAPTER 83

Administration

- Routine Monitoring on page 4421
- Operational Commands on page 4423

Routine Monitoring

Monitoring Spanning-Tree Protocols on page 4421

Purpose
Use the monitoring feature to view status and information about the spanning-tree protocol parameters on your EX Series switch.

Action
To display spanning-tree protocol parameter details in the J-Web interface, select Monitor > Switching > STP.

To display spanning-tree protocol parameter details in the CLI, enter the following commands:

- `show spanning-tree interface`
- `show spanning-tree bridge`

Meaning
Table 545 on page 4421 summarizes the spanning-tree protocol parameters.

Table 545: Summary of Spanning-Tree Protocols Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Parameters</td>
<td></td>
</tr>
<tr>
<td>Routing instance name</td>
<td>Displays bridge information for the specified routing instance.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The option is supported only on EX4300 switches.</td>
<td></td>
</tr>
<tr>
<td>Context ID</td>
<td>An internally generated identifier.</td>
</tr>
<tr>
<td>Enabled Protocol</td>
<td>Spanning-tree protocol type enabled.</td>
</tr>
</tbody>
</table>
### Table 545: Summary of Spanning-Tree Protocols Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root ID</td>
<td>Bridge ID of the elected spanning-tree root bridge.</td>
</tr>
<tr>
<td></td>
<td>The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.</td>
</tr>
<tr>
<td>Root cost</td>
<td>Calculated cost to reach the root bridge from the bridge where the command is entered.</td>
</tr>
<tr>
<td>Root port</td>
<td>Interface that is the current elected root port for this bridge.</td>
</tr>
<tr>
<td>Bridge ID</td>
<td>Locally configured bridge ID.</td>
</tr>
<tr>
<td>Hello time</td>
<td>The time for which the bridge interface remains in the listening or learning state.</td>
</tr>
<tr>
<td>Forward delay</td>
<td>The time for which the bridge interface remains in the listening or learning state before transitioning to the forwarding state.</td>
</tr>
<tr>
<td>Extended System ID</td>
<td>The system ID.</td>
</tr>
<tr>
<td>Inter Instance ID</td>
<td>An internally generated instance identifier.</td>
</tr>
<tr>
<td>Maximum age</td>
<td>Maximum age of received bridge protocol data units (BPDUs).</td>
</tr>
<tr>
<td>Number of topology changes</td>
<td>Total number of spanning-tree protocol topology changes detected since the switch last booted.</td>
</tr>
<tr>
<td>Time since last topology change</td>
<td>Number of seconds elapsed since the last topology change.</td>
</tr>
</tbody>
</table>

**NOTE:** This option is supported only on EX4300 switches.

### Spanning Tree Interface Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Interface configured to participate in the spanning-tree protocol instance.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Logical interface identifier configured to participate in the spanning-tree protocol instance.</td>
</tr>
<tr>
<td>Designated Port ID</td>
<td>Port ID of the designated port for the LAN segment to which the interface is attached.</td>
</tr>
<tr>
<td>Designated Bridge ID</td>
<td>ID of the designated bridge to which the interface is attached.</td>
</tr>
<tr>
<td>Port Cost</td>
<td>Configured cost for the interface.</td>
</tr>
</tbody>
</table>
### Table 545: Summary of Spanning-Tree Protocols Output Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port State</td>
<td>Spanning-tree protocol port state:</td>
</tr>
<tr>
<td></td>
<td>• Forwarding (FWD)</td>
</tr>
<tr>
<td></td>
<td>• Blocking (BLK)</td>
</tr>
<tr>
<td></td>
<td>• Listening</td>
</tr>
<tr>
<td></td>
<td>• Learning</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td>Role</td>
<td>MSTP or RSTP port role, Designated (DESG), backup (BKUP), alternate (ALT), or root.</td>
</tr>
</tbody>
</table>

#### Spanning Tree Statistics of Interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface for which statistics is being displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BPDUs Sent</th>
<th>Total number of BPDUs sent.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPDUs Received</td>
<td>Total number of BPDUs received.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Next BPDU Transmission</th>
<th>Number of seconds until the next BPDU is scheduled to be sent.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Related Documentation

- show spanning-tree interface on page 4438
- show spanning-tree bridge on page 4428
- Configuring Spanning-Tree Protocols (J-Web Procedure) on page 4373
- Configuring STP (CLI Procedure)
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Example: Faster Convergence and Improved Network Stability with RSTP on EX Series Switches on page 4313

#### Operational Commands
clear ethernet-switching bpdu-error

Syntax  
clear ethernet-switching bpdu-error interface interface-name

Release Information  
Command introduced in Junos OS Release 9.1 for EX Series switches. Command updated in Junos OS Release 11.1 for EX Series switches—a BPDU error shuts down the interface and this command brings the interface back up. Command introduced in Junos OS Release 11.1 for the QFX Series.

Description  
Clear bridge protocol data unit (BPDU) errors from an interface and bring up the interface.

Options  
interface-name—Clear BPDU errors on the specified interface.

Required Privilege Level  
clear

Related Documentation  
- show spanning-tree interface on page 4442
- Understanding BPDU Protection for STP, RSTP, and MSTP on EX Series Switches on page 4308
- Understanding BPDU Protection for STP, RSTP, and MSTP

List of Sample Output  
Clear ethernet-switching bpdu-error interface on page 4424

Sample Output  
clear ethernet-switching bpdu-error interface
user@switch> clear ethernet-switching bpdu-error interface xe-0/0/1.0
clear spanning-tree protocol-migration

**Syntax**

```
clear spanning-tree protocol-migration
<interface interface-name>
<routing-instance routing-instance-name>
```

**Release Information**

Command introduced in Junos OS Release 9.0.

**Description**

Revert from the original IEEE 802.1D Spanning Tree Protocol (STP) back to the Rapid Spanning Tree Protocol after the `force-version` statement has been removed from the configuration.

**Options**

- `none`—Reset the STP protocol for all interfaces and all routing instances.
- `interface interface-name`—(Optional) Reset the STP protocol for the specified interface only.
- `routing-instance routing-instance-name`—(Optional) Reset the STP protocol for a particular routing instance.

**Additional Information**

For information about the `force-version` statement, see the *Junos Routing Protocols Configuration Guide*, and “Forcing RSTP or VSTP to Run as IEEE 802.1D STP (CLI Procedure)” on page 4372.

**Required Privilege Level**

`clear`

**Sample Output**

```
clear spanning-tree protocol-migration

user@host> clear spanning-tree protocol-migration
```
clear spanning-tree statistics

Syntax

```
clear spanning-tree statistics
  <interface interface-name unit logical-unit-number>;
```

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Reset STP statistics for the all interfaces or a specified interface.

Options
- **none**—Reset STP counters for all interfaces.
- **interface-name**—(Optional) The name of the interface for which statistics should be reset.
- **logical-unit-number**—(Optional) The logical unit number of the interface.

Required Privilege
- **clear**

Related Documentation
- show spanning-tree bridge on page 4428
- show spanning-tree interface on page 4438
- Understanding STP for EX Series Switches on page 4304

List of Sample Output
- clear spanning-tree statistics on page 4426

Output Fields
This command produces no output.

Sample Output
```
clear spanning-tree statistics
```
```
user@switch> clear spanning-tree statistics
```
clear spanning-tree statistics

**Syntax**
```
clear spanning-tree statistics
  <interface interface-name>
  <logical-system logical-system-name>
```

**Syntax (EX Series Switches and the QFX Series)**
```
clear spanning-tree statistics
  <interface interface-name>
```

**Release Information**
Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**
Clear Spanning Tree Protocol statistics.

**Options**
- **none**—Reset STP counters for all interfaces for all routing instances.
- `interface interface-name`—(Optional) Clear STP statistics for the specified interface only.
- `logical-system logical-system-name`—(Optional) Clear STP statistics on a particular logical system.

**NOTE:** The logical-system option is not available on QFabric systems.

**Required Privilege Level**
clear

**Related Documentation**
- show spanning-tree statistics on page 4454

**List of Sample Output**
clear stp statistics on page 4427

**Sample Output**
clear stp statistics

```
user@host> clear stp statistics
```
**show spanning-tree bridge**

**Syntax**
```
show spanning-tree bridge
  <brief | detail>
  <msti msti-id>
  <vlan vlan-id>
```

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Display the configured or calculated spanning-tree protocol (can be either STP, RSTP, MSTP, or VSTP) parameters.

**Options**
- `none`—(Optional) Display brief spanning-tree protocol bridge information for all Multiple Spanning Tree Instances (MSTIs).
  
  - `brief | detail`—(Optional) Display the specified level of output.
  
  - `msti msti-id`—(Optional) Display spanning-tree protocol bridge information for the specified MSTI or Common and Internal Spanning Tree (CIST). Specify 0 for CIST. Specify a value from 1 through 4094 for an MSTI.
  
  - `vlan vlan-id`—(Optional) Display spanning-tree protocol bridge information for the specified VLAN. Specify a VLAN tag identifier from 1 through 4094.

**Required Privilege Level**
`view`

**Related Documentation**
- show spanning-tree interface on page 4438
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Understanding STP for EX Series Switches on page 4304
- Understanding RSTP for EX Series Switches on page 4300
- Understanding VSTP for EX Series Switches on page 4306

**List of Sample Output**
- show spanning-tree bridge on page 4431
- show spanning-tree bridge brief on page 4431
- show spanning-tree bridge detail on page 4432

**Output Fields**
Table 546 on page 4428 lists the output fields for the `show spanning-tree bridge` command. Output fields are listed in the approximate order in which they appear.

**Table 546: show spanning-tree bridge Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context ID</td>
<td>An internally generated identifier.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
</tbody>
</table>
Table 546: show spanning-tree bridge Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled protocol</td>
<td>Spanning-tree protocol type enabled.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Root ID</td>
<td>Bridge ID of the elected spanning tree root bridge. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Root cost</td>
<td>Calculated cost to reach the root bridge from the bridge where the command is entered.</td>
<td>VSTP all</td>
</tr>
<tr>
<td>Root port</td>
<td>Interface that is the current elected root port for this bridge.</td>
<td>VSTP all</td>
</tr>
<tr>
<td>CIST regional root</td>
<td>Bridge ID of the elected MSTP regional root bridge.</td>
<td>MSTP all</td>
</tr>
<tr>
<td>CIST internal root cost</td>
<td>Calculated cost to reach the regional root bridge from the bridge where the command is entered.</td>
<td>MSTP all</td>
</tr>
<tr>
<td>Hello time</td>
<td>Configured number of seconds between transmissions of configuration BPDUs.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Maximum age</td>
<td>Maximum age of received protocol BPDUs.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Forward delay</td>
<td>Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Message age</td>
<td>Number of seconds elapsed since the most recent BPDU was received.</td>
<td>VSTP all, RSTP all, STP all</td>
</tr>
<tr>
<td>Number of topology changes</td>
<td>Total number of STP topology changes detected since the switch last booted.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Time since last topology change</td>
<td>Number of seconds elapsed since the most recent topology change.</td>
<td>RSTP detail</td>
</tr>
<tr>
<td>Topology change initiator</td>
<td>Interface name of the interface that received the topology change request.</td>
<td>RSTP detail</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
<td>Level of Output</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>_topology change last recvd. from</td>
<td>Bridge ID of the bridge that requested the last topology change.</td>
<td>RSTP detail</td>
</tr>
<tr>
<td>Bridge ID (local)</td>
<td>Locally configured bridge ID. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Extended system ID (local)</td>
<td>Internally generated system identifier.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>MSTI regional root</td>
<td>Bridge ID of the elected MSTP regional root bridge.</td>
<td>MSTP detail</td>
</tr>
<tr>
<td>Internal instance ID (local)</td>
<td>An internally generated identifier.</td>
<td>VSTP all, RSTP all, MSTP all, STP all</td>
</tr>
<tr>
<td>Hello time (local)</td>
<td>Configured number of seconds between transmissions of configuration BPDUs.</td>
<td>RSTP detail, MSTP detail, STP detail</td>
</tr>
<tr>
<td>Maximum age (local)</td>
<td>Maximum age of received protocol BPDUs.</td>
<td>VSTP detail, RSTP detail, MSTP detail, STP detail</td>
</tr>
<tr>
<td>Forward delay (local)</td>
<td>Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.</td>
<td>RSTP detail, MSTP detail, STP detail</td>
</tr>
<tr>
<td>PathCost Method (local)</td>
<td>Bridges supporting 802.1D (legacy) implement only 16-bit values for path cost. Newer versions of this standard support 32-bit values.</td>
<td>VSTP detail, RSTP detail, MSTP detail, STP detail</td>
</tr>
<tr>
<td>Maximum Hop count (local)</td>
<td>Configured maximum number of hops a BPDU can be forwarded in the MSTP region.</td>
<td>MSTP detail</td>
</tr>
</tbody>
</table>
Sample Output

show spanning-tree bridge

```
user@switch> show spanning-tree bridge
STP bridge parameters
Context ID : 0
Enabled protocol : MSTP

STP bridge parameters for CIST
Root ID : 32768.00:11:f2:56:df:40
Root cost : 0
Root port : ge-0/0/1.0
CIST regional root : 32768.00:11:f2:56:df:40
CIST internal root cost : 20000
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 19
Message age : 0
Number of topology changes : 1
Time since last topology change : 108 seconds
Topology change initiator : ge-0/0/1.0
Topology change last recvd. from : 00:11:f2:56:df:4c

Local parameters
Bridge ID : 32768.00:11:f2:57:1c:00
Extended system ID : 0
Internal instance ID : 0

STP bridge parameters for MSTI 10
MSTI regional root : 32778.00:11:f2:56:df:40
Root cost : 20000
Root port : ge-0/0/1.0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 19
Number of topology changes : 1
Time since last topology change : 108 seconds
Topology change initiator : ge-0/0/1.0
Topology change last recvd. from : 00:11:f2:56:df:41

Local parameters
Bridge ID : 32778.00:11:f2:57:1c:00
Extended system ID : 0
Internal instance ID : 1
```

show spanning-tree bridge brief

```
user@switch> show spanning-tree bridge brief
STP bridge parameters
Context ID : 0
Enabled protocol : RSTP

Root ID : 32768.00:11:e2:50:95:a0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Message age : 0
Number of topology changes : 0

Local parameters
Bridge ID : 32768.00:11:e2:50:95:a0
```
Extended system ID      : 0
Internal instance ID    : 0

show spanning-tree bridge detail

user@switch> show spanning-tree bridge detail

STP bridge parameters
Context ID      : 0
Enabled protocol    : RSTP
Root ID       : 32768.00:19:e2:50:95:a0
Hello time        : 2 seconds
Maximum age       : 20 seconds
Forward delay     : 15 seconds
Message age       : 0
Number of topology changes : 0

Local parameters
Bridge ID       : 32768.00:19:e2:50:95:a0
Extended system ID      : 0
Internal instance ID    : 0
Hello time        : 2 seconds
Maximum age       : 20 seconds
Forward delay     : 15 seconds
Path cost method    : 32 bit
**show spanning-tree bridge**

**Syntax**
```
show spanning-tree bridge
  <brief | detail>
  <msti msti-id>
  <routing-instance routing-instance-name>
  <vlan-id vlan-id>
```

**Syntax (QFX Series)**
```
show spanning-tree bridge
  <brief | detail>
  <msti msti-id>
  <vlan-id vlan-id>
```

**Release Information**

**Description**
Display the configured or calculated Spanning Tree Protocol (STP) parameters.

**Options**
- `none`—(Optional) Display brief STP bridge information for all multiple spanning-tree instances (MSTIs).
- `brief | detail`—(Optional) Display the specified level of output.
- `msti msti-id`—(Optional) Display STP bridge information for the specified MSTI.
- `routing-instance routing-instance-name`—(Optional) Display STP bridge information for the specified routing instance.
- `vlan-id vlan-id`—(Optional) Display STP bridge information for the specified VLAN.

**Required Privilege**
view

**List of Sample Output**
- `show spanning-tree bridge routing-instance on page 4434`
- `show spanning-tree bridge msti on page 4435`
- `show spanning-tree bridge vlan-id (MSTP) on page 4436`
- `show spanning-tree bridge (RSTP) on page 4436`
- `show spanning-tree bridge vlan-id (RSTP) on page 4437`

**Output Fields**
Table 547 on page 4433 lists the output fields for the `show spanning-tree bridge` command. Output fields are listed in the approximate order in which they appear.

**Table 547: show spanning-tree bridge Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing instance name</td>
<td>Name of the routing instance under which the bridge is configured.</td>
</tr>
<tr>
<td>Enabled protocol</td>
<td>Spanning Tree Protocol type enabled.</td>
</tr>
<tr>
<td>Root ID</td>
<td>Bridge ID of the elected spanning-tree root bridge. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.</td>
</tr>
</tbody>
</table>
Table 547: show spanning-tree bridge Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root cost</td>
<td>Calculated cost to reach the root bridge from the bridge where the command is entered.</td>
</tr>
<tr>
<td>Root port</td>
<td>Interface that is the current elected root port for this bridge.</td>
</tr>
<tr>
<td>CIST regional root</td>
<td>Bridge ID of the elected MSTP regional root bridge.</td>
</tr>
<tr>
<td>CIST internal root cost</td>
<td>Calculated cost to reach the regional root bridge from the bridge where the command is entered.</td>
</tr>
<tr>
<td>Hello time</td>
<td>Configured number of seconds between transmissions of configuration bridge protocol data units (BPDUs).</td>
</tr>
<tr>
<td>Maximum age</td>
<td>Configured maximum expected arrival time of hello bridge protocol data units (BPDUs).</td>
</tr>
<tr>
<td>Forward delay</td>
<td>How long an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.</td>
</tr>
<tr>
<td>Hop count</td>
<td>Configured maximum number of hops a BPDU can be forwarded in the MSTP region.</td>
</tr>
<tr>
<td>Message age</td>
<td>Number of elapsed seconds since the most recent BPDU was received.</td>
</tr>
<tr>
<td>Number of topology changes</td>
<td>Total number of STP topology changes detected since the routing device last booted.</td>
</tr>
<tr>
<td>Time since last topology change</td>
<td>Number of elapsed seconds since the most recent topology change.</td>
</tr>
<tr>
<td>Bridge ID (Local)</td>
<td>Locally configured bridge ID. The bridge ID consists of a configurable bridge priority and the MAC address of the bridge.</td>
</tr>
<tr>
<td>Extended system ID</td>
<td>System identifier.</td>
</tr>
<tr>
<td>MSTI regional root</td>
<td>Bridge ID of the elected MSTP regional root bridge.</td>
</tr>
</tbody>
</table>

Sample Output

```
show spanning-tree bridge routing-instance
user@host> show spanning-tree bridge routing-instance vs1 detail
STP bridge parameters
Routing instance name : vs1
Enabled protocol : MSTP

STP bridge parameters for CIST
  Root ID : 32768.00:13:c3:9e:c8:80
  Root cost : 0
```
Root port : ge-10/2/0
CIST regional root : 32768.00:13:c3:9e:c8:80
CIST internal root cost : 22000
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Hop count : 18
Message age : 0
Number of topology changes : 1
Time since last topology change : 1191 seconds
Local parameters
  Bridge ID : 32768.00:90:69:0b:7f:d1
  Extended system ID : 1

STP bridge parameters for MSTI 1
  MSTI regional root : 32769.00:13:c3:9e:c8:80
  Root cost : 22000
  Root port : ge-10/2/0
  Hello time : 2 seconds
  Maximum age : 20 seconds
  Forward delay : 15 seconds
  Hop count : 18
  Number of topology changes : 1
  Time since last topology change : 1191 seconds
  Local parameters
    Bridge ID : 32769.00:90:69:0b:7f:d1
    Extended system ID : 1

STP bridge parameters for MSTI 2
  MSTI regional root : 32770.00:13:c3:9e:c8:80
  Root cost : 22000
  Root port : xe-10/2/0
  Hello time : 2 seconds
  Maximum age : 20 seconds
  Forward delay : 15 seconds
  Hop count : 18
  Number of topology changes : 1
  Time since last topology change : 1191 seconds
  Local parameters
    Bridge ID : 32770.00:90:69:0b:7f:d1
    Extended system ID : 1

show spanning-tree bridge msti

user@host> show spanning-tree bridge msti1 routing-instance vs1 detail
STP bridge parameters
Routing instance name : vs1
Enabled protocol : MSTP

STP bridge parameters for MSTI 1
  MSTI regional root : 32769.00:13:c3:9e:c8:80
  Root cost : 22000
  Root port : xe-10/2/0
  Hello time : 2 seconds
  Maximum age : 20 seconds
  Forward delay : 15 seconds
  Hop count : 18
  Number of topology changes : 1
  Time since last topology change : 1191 seconds
  Local parameters

Bridge ID                       : 32769.00:90:69:0b:7f:d1
Extended system ID              : 1

show spanning-tree bridge vlan-id (MSTP)

user@host> show spanning-tree bridge vlan-id 1101 routing-instance vs1 detail
STP bridge parameters
Routing instance name               : vs1
Enabled protocol                    : MSTP

STP bridge parameters for CIST
Root ID                           : 32768.00:13:c3:9e:c8:80
Root cost                         : 0
Root port                         : xe-10/2/0
CIST regional root                : 32768.00:13:c3:9e:c8:80
CIST internal root cost           : 22000
Hello time                        : 2 seconds
Maximum age                       : 20 seconds
Forward delay                     : 15 seconds
Hop count                         : 18
Message age                       : 0
Number of topology changes        : 0

Local parameters
Bridge ID                       : 32768.00:90:69:0b:7f:d1
Extended system ID              : 1
Hello time                      : 2 seconds
Maximum age                     : 20 seconds
Forward delay                   : 15 seconds
Path cost method                : 32 bit
Maximum hop count               : 20

show spanning-tree bridge (RSTP)

user@host> show spanning-tree bridge
STP bridge parameters
Routing instance name               : GLOBAL
Enabled protocol                    : RSTP

Root ID                           : 28672.00:90:69:0b:3f:d0
Hello time                        : 2 seconds
Maximum age                       : 20 seconds
Forward delay                     : 15 seconds
Message age                       : 0
Number of topology changes        : 58
Time since last topology change   : 14127 seconds

Local parameters
Bridge ID                       : 28672.00:90:69:0b:3f:d0
Extended system ID              : 0

STP bridge parameters for bridge VLAN 10
Root ID                           : 28672.00:90:69:0b:3f:d0
Hello time                        : 2 seconds
Maximum age                       : 20 seconds
Forward delay                     : 15 seconds
Message age                       : 0
Number of topology changes        : 58
Time since last topology change   : 14127 seconds

Local parameters
Bridge ID                       : 28672.00:90:69:0b:3f:d0
Extended system ID              : 0

STP bridge parameters for bridge VLAN 20
show spanning-tree bridge vlan-id (RSTP)

user@host> show spanning-tree bridge vlan-id 10
STP bridge parameters
Routing instance name : GLOBAL
Enabled protocol : RSTP

STP bridge parameters for VLAN 10
Root ID : 28672.00:90:69:0b:3f:d0
Hello time : 2 seconds
Maximum age : 20 seconds
Forward delay : 15 seconds
Message age : 0
Number of topology changes : 58
Time since last topology change : 14127 seconds
Local parameters
  Bridge ID : 28672.00:90:69:0b:3f:d0
  Extended system ID : 0
show spanning-tree interface

Syntax

show spanning-tree interface
  <brief | detail>
  <interface-name interface-name>
  <msti msti-id>
  <vlan-id vlan-id>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the configured or calculated interface-level spanning-tree protocol (can be either STP, RSTP, or MSTP) parameters. In brief mode, will not display interfaces that are administratively disabled or do not have a physical link.

Options

none—(Optional) Display brief STP interface information.

brief | detail—(Optional) Display the specified level of output.

interface-name interface-name—(Optional) Name of an interface.

msti msti-id—(Optional) Display STP bridge information for the specified MSTP instance ID or Common and Internal Spanning Tree (CIST). Specify 0 for CIST. Specify a value from 1 through 4094 for an MSTI.

vlan-id vlan-id—(Optional) For MSTP interfaces, display interface information for the specified VLAN. Specify a value from 0 through 4094.

Required Privilege Level

view

Related Documentation

• show spanning-tree bridge on page 4428
  • Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
  • Understanding STP for EX Series Switches on page 4304
  • Understanding RSTP for EX Series Switches on page 4300
  • Understanding MSTP for EX Series Switches on page 4298
  • Understanding VSTP for EX Series Switches on page 4306

List of Sample Output

show spanning-tree interface on page 4439
show spanning-tree interface brief on page 4440
show spanning-tree interface detail on page 4440
show spanning-tree interface ge-1/0/0 on page 4441

Output Fields

Table 548 on page 4439 lists the output fields for the show spanning-tree interface command. Output fields are listed in the approximate order in which they appear.
Table 548: show spanning-tree interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Interface configured to participate in the STP, RSTP, or MSTP instance.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Logical interface identifier configured to participate in the MSTP instance.</td>
</tr>
<tr>
<td>Designated port ID</td>
<td>Port ID of the designated port for the LAN segment this interface is attached to.</td>
</tr>
<tr>
<td>Designated bridge ID</td>
<td>Bridge ID of the designated bridge for the LAN segment this interface is attached to.</td>
</tr>
<tr>
<td>Port Cost</td>
<td>Configured cost for the interface.</td>
</tr>
<tr>
<td>Port State</td>
<td>STP port state. Forwarding (FWD), blocking (BLK), listening, learning, or disabled.</td>
</tr>
<tr>
<td>Port Role</td>
<td>MSTP or RSTP port role. Designated (DESG), backup (BKUP), alternate (ALT), (ROOT), or Root Prevented (Root-Prev).</td>
</tr>
<tr>
<td>Link type</td>
<td>MSTP or RSTP link type. Shared or point-to-point (pt-pt) and edge or non edge.</td>
</tr>
<tr>
<td>Alternate</td>
<td>Identifies the interface as an MSTP or RSTP alternate root port (yes) or non-alternate root port (no).</td>
</tr>
<tr>
<td>Boundary Port</td>
<td>Identifies the interface as an MSTP regional boundary port (yes) or non-boundary port (no).</td>
</tr>
<tr>
<td>Edge delay while expiry count</td>
<td>Number of times the edge delay timer expired on that interface.</td>
</tr>
<tr>
<td>Rcvd info while expiry count</td>
<td>Number of times the rcvd info timer expired on that interface.</td>
</tr>
</tbody>
</table>

Sample Output

```
show spanning-tree interface
```

```
user@switch> show spanning-tree interface

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>128:513</td>
<td>128:513</td>
<td>8192.0019e2500340</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>128:515</td>
<td>128:515</td>
<td>8192.0019e2500340</td>
<td>1000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>128:517</td>
<td>128:517</td>
<td>8192.0019e2500340</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/23.0</td>
<td>128:536</td>
<td>128:536</td>
<td>8192.0019e2500340</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0.0</td>
<td>128:513</td>
<td>128:513</td>
<td>8193.0019e2500340</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-0/0/2.0</td>
<td>128:515</td>
<td>128:515</td>
<td>8193.0019e2500340</td>
<td>1000</td>
<td>BLK</td>
<td>DIS</td>
</tr>
<tr>
<td>ge-0/0/4.0</td>
<td>128:517</td>
<td>128:517</td>
<td>8193.0019e2500340</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>
```
show spanning-tree interface brief

user@switch> show spanning-tree interface brief
Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Port identifier</th>
<th>Designated port ID</th>
<th>Port cost</th>
<th>Port state</th>
<th>Designated bridge ID</th>
<th>Port role</th>
<th>Link type</th>
<th>Boundary port</th>
<th>Edge delay while expiry count</th>
<th>Rcvd info while expiry count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/0.0</td>
<td>128.625</td>
<td>128.625</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/1.0</td>
<td>128.626</td>
<td>128.626</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/NONEDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/2.0</td>
<td>128.627</td>
<td>128.627</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/10.0</td>
<td>128.635</td>
<td>128.635</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/20.0</td>
<td>128.645</td>
<td>128.645</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/30.0</td>
<td>128.655</td>
<td>128.655</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

show spanning-tree interface detail

user@switch> show spanning-tree interface detail
Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Port identifier</th>
<th>Designated port ID</th>
<th>Port cost</th>
<th>Port state</th>
<th>Designated bridge ID</th>
<th>Port role</th>
<th>Link type</th>
<th>Boundary port</th>
<th>Edge delay while expiry count</th>
<th>Rcvd info while expiry count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/0.0</td>
<td>128.625</td>
<td>128.625</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/1.0</td>
<td>128.626</td>
<td>128.626</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/NONEDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/2.0</td>
<td>128.627</td>
<td>128.627</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/10.0</td>
<td>128.635</td>
<td>128.635</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/20.0</td>
<td>128.645</td>
<td>128.645</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ge-1/0/30.0</td>
<td>128.655</td>
<td>128.655</td>
<td>20000</td>
<td>Blocking</td>
<td>32768.00:19:e2:50:95:a0</td>
<td>Disabled</td>
<td>Pt-Pt/EDGE</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Port role : Disabled
Link type : Pt-Pt/NONEDGE
Boundary port : NA
Edge delay while expiry count : 0
Rvcd info while expiry count : 0

Interface name : ge-1/0/10.0
Port identifier : 128.635
Designated port ID : 128.635
Port cost : 20000
Port state : Blocking
Designated bridge ID : 32768.00:19:e2:50:95:a0
Port role : Disabled
Link type : Pt-Pt/NONEDGE
Boundary port : NA
Edge delay while expiry count : 0
Rvcd info while expiry count : 0

Interface name : ge-1/0/20.0
Port identifier : 128.645
Designated port ID : 128.645
Port cost : 20000
Port state : Blocking
Designated bridge ID : 32768.00:19:e2:50:95:a0
Port role : Disabled
Link type : Pt-Pt/NONEDGE
Boundary port : NA
Edge delay while expiry count : 0
Rvcd info while expiry count : 0
[output truncated]

show spanning-tree interface ge-1/0/0

user@switch> show spanning-tree interface ge-1/0/0

Interface    Port ID    Designated  Designated     Port    State  Role
port ID    bridge ID  Cost
ge-1/0/0.0 128:625  128:625  32768.0019e250:95a0 20000  BLK   DIS
show spanning-tree interface

Syntax

```
show spanning-tree interface
  <brief | detail>
  <msti msti-id>
  <routing-instance routing-instance-name>
  <vlan-id vlan-id>
```

Syntax (EX Series Switches and the QFX Series)

```
show spanning-tree interface
  <brief | detail>
  <msti msti-id>
  <vlan-id vlan-id>
```

Release Information

- Command introduced in Junos OS Release 8.4.
- Command introduced in Junos OS Release 9.0 for EX Series switches.
- Command introduced in Junos OS Release 11.1 for the QFX Series.

Description

Display the configured or calculated interface-level STP parameters.

Options

- none—Display brief STP interface information.
- brief | detail—(Optional) Display the specified level of output.
- msti msti-id—(Optional) Display STP interface information for the specified MST instance.
- routing-instance routing-instance-name—(Optional) Display STP interface information for the specified routing instance.
- vlan-id vlan-id—(Optional) Display STP interface information for the specified VLAN.

Required Privilege Level

view

List of Sample Output

- show spanning-tree interface on page 4443
- show spanning-tree interface (QFX Series) on page 4444
- show spanning-tree interface detail on page 4444
- show spanning-tree interface msti on page 4446
- show spanning-tree interface vlan-id on page 4446
- show spanning-tree interface (VSTP) on page 4447
- show spanning-tree interface vlan-id (VSTP) on page 4447

Output Fields

Table 549 on page 4442 lists the output fields for the `show spanning-tree interface` command. Output fields are listed in the approximate order in which they appear.

Table 549: show spanning-tree Interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name</td>
<td>Interface configured to participate in the STP, RSTP, VSTP, or MSTP instance.</td>
</tr>
</tbody>
</table>
Table 549: show spanning-tree Interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ID</td>
<td>Logical interface identifier configured to participate in the MSTP or VSTP instance.</td>
</tr>
<tr>
<td>Designated port ID</td>
<td>Port ID of the designated port for the LAN segment to which this interface is attached.</td>
</tr>
<tr>
<td>Designated bridge ID</td>
<td>Bridge ID of the designated bridge for the LAN segment to which this interface is attached.</td>
</tr>
<tr>
<td>Port Cost</td>
<td>Configured cost for the interface.</td>
</tr>
<tr>
<td>Port State</td>
<td>STP port state: forwarding (FWD), blocking (BLK), listening, learning, or disabled.</td>
</tr>
<tr>
<td>Port Role</td>
<td>MSTP, VSTP, or RSTP port role: designated (DESG), backup (BKUP), alternate (ALT), (ROOT), or Root Prevented (Root-Prev).</td>
</tr>
<tr>
<td>Link type</td>
<td>MSTP, VSTP, or RSTP link type. Shared or point-to-point (pt-pt) and edge or nonedge.</td>
</tr>
<tr>
<td>Alternate</td>
<td>Identifies the interface as an MSTP, VSTP, or RSTP alternate root port (Yes) or nonalternate root port (No).</td>
</tr>
<tr>
<td>Boundary Port</td>
<td>Identifies the interface as an MSTP regional boundary port (Yes) or nonboundary port (No).</td>
</tr>
</tbody>
</table>

Sample Output

show spanning-tree interface

```
show spanning-tree interface routing-instance vs1 detail

Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ael</td>
<td>128:1</td>
<td>128:1</td>
<td>32768.0090690b47d1</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/2</td>
<td>128:2</td>
<td>128:2</td>
<td>32768.0090690b47d1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/5</td>
<td>128:3</td>
<td>128:3</td>
<td>32768.0090690b47d1</td>
<td>29999</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/2/1</td>
<td>128:4</td>
<td>128:26</td>
<td>32768.0013c39ec880</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>xe-9/2/0</td>
<td>128:5</td>
<td>128:5</td>
<td>32768.0090690b47d1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for instance 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ael</td>
<td>128:1</td>
<td>128:1</td>
<td>32769.0090690b47d1</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/2</td>
<td>128:2</td>
<td>128:2</td>
<td>32769.0090690b47d1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/5</td>
<td>128:3</td>
<td>128:3</td>
<td>32769.0090690b47d1</td>
<td>29999</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/2/1</td>
<td>128:4</td>
<td>128:26</td>
<td>32769.0013c39ec880</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>xe-9/2/0</td>
<td>128:5</td>
<td>128:5</td>
<td>32769.0090690b47d1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>
```
### Spanning tree interface parameters for instance 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae1</td>
<td>128:1</td>
<td>128:1</td>
<td>32770.0090690b47d1</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/2</td>
<td>128:2</td>
<td>128:2</td>
<td>32770.0090690b47d1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/5</td>
<td>128:3</td>
<td>128:3</td>
<td>32770.0090690b47d1</td>
<td>29999</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/2/1</td>
<td>128:4</td>
<td>128:26</td>
<td>32770.0013c39ec880</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>xe-9/2/0</td>
<td>128:5</td>
<td>128:5</td>
<td>32770.0090690b47d1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

### show spanning-tree interface (QFX Series)

```
user@lf0> show spanning-tree interface routing-instance vs1 detail
```

### Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae1</td>
<td>128:1</td>
<td>128:1</td>
<td>32768.0090690b47d1</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/2</td>
<td>128:2</td>
<td>128:2</td>
<td>32768.0090690b47d1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/5</td>
<td>128:3</td>
<td>128:3</td>
<td>32768.0090690b47d1</td>
<td>29999</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/2/1</td>
<td>128:4</td>
<td>128:26</td>
<td>32768.0013c39ec880</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>xe-9/2/0</td>
<td>128:5</td>
<td>128:5</td>
<td>32768.0090690b47d1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

### Spanning tree interface parameters for instance 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae1</td>
<td>128:1</td>
<td>128:1</td>
<td>32769.0090690b47d1</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/2</td>
<td>128:2</td>
<td>128:2</td>
<td>32769.0090690b47d1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/5</td>
<td>128:3</td>
<td>128:3</td>
<td>32769.0090690b47d1</td>
<td>29999</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/2/1</td>
<td>128:4</td>
<td>128:26</td>
<td>32769.0013c39ec880</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>xe-9/2/0</td>
<td>128:5</td>
<td>128:5</td>
<td>32769.0090690b47d1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

### Spanning tree interface parameters for instance 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ae1</td>
<td>128:1</td>
<td>128:1</td>
<td>32770.0090690b47d1</td>
<td>1000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/2</td>
<td>128:2</td>
<td>128:2</td>
<td>32770.0090690b47d1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/1/5</td>
<td>128:3</td>
<td>128:3</td>
<td>32770.0090690b47d1</td>
<td>29999</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-2/2/1</td>
<td>128:4</td>
<td>128:26</td>
<td>32770.0013c39ec880</td>
<td>20000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
<tr>
<td>xe-9/2/0</td>
<td>128:5</td>
<td>128:5</td>
<td>32770.0090690b47d1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

### show spanning-tree interface detail

```
user@host> show spanning-tree interface routing-instance vs1 detail
```

### Spanning tree interface parameters for instance 0

```
Interface name : ae1
Port identifier : 128.1
Designated port ID : 128.1
Port cost : 1000
Port state : Forwarding
Designated bridge ID : 32768.00:90:69:0b:47:d1
Port role : Designated
Link type : Pt-Pt/NONEDGE
```
Boundary port : No

Interface name : ge-2/1/2
Port identifier : 128.2
Designated port ID : 128.2
Port cost : 20000
Port state : Forwarding
Designated bridge ID : 32768.00:90:69:0b:47:d1
Port role : Designated
Link type : Pt-Pt/NONEDGE
Boundary port : No

Interface name : ge-2/1/5
Port identifier : 128.3
Designated port ID : 128.3
Port cost : 29999
Port state : Forwarding
Designated bridge ID : 32768.00:90:69:0b:47:d1
Port role : Designated
Link type : Pt-Pt/NONEDGE
Boundary port : No

Interface name : ge-2/2/1
Port identifier : 128.4
Designated port ID : 128.26
Port cost : 20000
Port state : Forwarding
Designated bridge ID : 32768.00:13:c3:9e:c8:80
Port role : Root
Link type : Pt-Pt/NONEDGE
Boundary port : No

Interface name : xe-9/2/0
Port identifier : 128.5
Designated port ID : 128.5
Port cost : 2000
Port state : Forwarding
Designated bridge ID : 32768.00:90:69:0b:47:d1
Port role : Designated
Link type : Pt-Pt/NONEDGE
Boundary port : No

Interface name : xe-9/3/0
Port identifier : 128.6
Designated port ID : 128.6
Port cost : 2000
Port state : Forwarding
Designated bridge ID : 32768.00:90:69:0b:47:d1
Port role : Designated
Link type : Pt-Pt/NONEDGE
Boundary port : No

Spanning tree interface parameters for instance 1

Interface name : ael
Port identifier : 128.1
Designated port ID : 128.1
Port cost : 1000
Port state : Forwarding
Designated bridge ID : 32768.00:90:69:0b:47:d1
Port role                      : Designated
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

Interface name                 : ge-2/1/2
Port identifier                : 128.2
Designated port ID             : 128.2
Port cost                      : 20000
Port state                     : Forwarding
Designated bridge ID           : 32768.00:90:69:0b:47:d1
Port role                      : Designated
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

Interface name                 : ge-2/1/5
Port identifier                : 128.3
Designated port ID             : 128.3
Port cost                      : 29999
Port state                     : Forwarding
Designated bridge ID           : 32768.00:90:69:0b:47:d1
Port role                      : Designated
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

Interface name                 : ge-2/1/1
Port identifier                : 128.4
Designated port ID             : 128.4
Port cost                      : 20000
Port state                     : Forwarding
Designated bridge ID           : 32768.00:13:c3:9e:c8:80
Port role                      : Root
Link type                      : Pt-Pt/NONEDGE
Boundary port                   : No

show spanning-tree interface msti

```
user@host> show spanning-tree interface msti1 routing-instance vs1 detail
Spanning tree interface parameters for instance 1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>xe-7/0/0</td>
<td>128:1</td>
<td>128:1</td>
<td>32769.0090690b4fd1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-5/1/0</td>
<td>128:2</td>
<td>128:2</td>
<td>32769.0090690b4fd1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-5/1/1</td>
<td>128:3</td>
<td>128:3</td>
<td>32769.0090690b4fd1</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ae1</td>
<td>128:4</td>
<td>128:4</td>
<td>32769.0090690b47d1</td>
<td>10000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-5/1/4</td>
<td>128:5</td>
<td>128:3</td>
<td>32769.0090690b4d7d1</td>
<td>20000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>xe-7/2/0</td>
<td>128:6</td>
<td>128:6</td>
<td>32769.0090690b47d1</td>
<td>2000</td>
<td>FWD</td>
<td>ROOT</td>
</tr>
</tbody>
</table>
```

show spanning-tree interface vlan-id

```
user@host> show spanning-tree interface vlan-id101 routing-instance vs1 detail
Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Port Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-11/0/5</td>
<td>128:1</td>
<td>128:1</td>
<td>32768.0090690b7fd1</td>
<td>2000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-11/0/6</td>
<td>128:2</td>
<td>128:1</td>
<td>32768.0090690b7fd1</td>
<td>20000</td>
<td>BLK</td>
<td>BKUP</td>
</tr>
<tr>
<td>ge-11/1/0</td>
<td>128:3</td>
<td>128:2</td>
<td>32768.0090690b4fd1</td>
<td>20000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
<tr>
<td>ge-11/1/1</td>
<td>128:4</td>
<td>128:3</td>
<td>32768.0090690b4fd1</td>
<td>20000</td>
<td>BLK</td>
<td>ALT</td>
</tr>
</tbody>
</table>
```
show spanning-tree interface (VSTP)

```
user@host> show spanning-tree interface
Spanning tree interface parameters for instance 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/1</td>
<td>128:1</td>
<td>128:1</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-1/0/2</td>
<td>128:2</td>
<td>128:2</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for VLAN 10

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/1</td>
<td>128:1</td>
<td>128:1</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-1/0/2</td>
<td>128:2</td>
<td>128:2</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>

Spanning tree interface parameters for VLAN 20

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/1</td>
<td>128:1</td>
<td>128:1</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-1/0/2</td>
<td>128:2</td>
<td>128:2</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>
```

show spanning-tree interface vlan-id (VSTP)

```
user@host> show spanning-tree interface vlan-id 10
Spanning tree interface parameters for VLAN 10

<table>
<thead>
<tr>
<th>Interface</th>
<th>Port ID</th>
<th>Designated port ID</th>
<th>Designated bridge ID</th>
<th>Cost</th>
<th>State</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-1/0/1</td>
<td>128:1</td>
<td>128:1</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
<tr>
<td>ge-1/0/2</td>
<td>128:2</td>
<td>128:2</td>
<td>28672.0090690b3fe0</td>
<td>20000</td>
<td>FWD</td>
<td>DESG</td>
</tr>
</tbody>
</table>
```
show spanning-tree mstp configuration

Syntax

show spanning-tree mstp configuration
<brief | detail>

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display the MSTP configuration.

Options
none—Display MSTP configuration information.
brief | detail—(Optional) Display the specified level of output.

Required Privilege
view

Related Documentation
• show spanning-tree bridge on page 4428
• show spanning-tree statistics on page 4452
• mstp (Spanning Trees) on page 4404
• Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
• Understanding MSTP for EX Series Switches on page 4298

List of Sample Output
show spanning-tree mstp configuration on page 4449

Output Fields
Table 550 on page 4448 lists the output fields for the show spanning-tree mstp configuration command. Output fields are listed in the approximate order in which they appear.

Table 550: show spanning-tree mstp configuration Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context identifier</td>
<td>Internally generated identifier.</td>
</tr>
<tr>
<td>Region name</td>
<td>MSTP region name carried in the MSTP BPDUs.</td>
</tr>
<tr>
<td>Revision</td>
<td>Revision number of the MSTP configuration.</td>
</tr>
<tr>
<td>Configuration digest</td>
<td>Numerical value derived from the VLAN-to-instance mapping table.</td>
</tr>
<tr>
<td>MSTI</td>
<td>MSTI instance identifier.</td>
</tr>
<tr>
<td>Member VLANs</td>
<td>Identifiers for VLANs associated with the MSTI.</td>
</tr>
</tbody>
</table>
Sample Output

show spanning-tree mstp configuration

    user@host> show spanning-tree mstp configuration
    MSTP configuration information
    Context identifier : 0
    Region name        : region1
    Revision           : 0
    Configuration digest : 0xc92e7af9febb44d8df928b87f16b

  MSTI    Member VLANs
    0     0-100,105-4094
    1     101-102
    2     103-104
**show spanning-tree mstp configuration**

**Syntax**

```
show spanning-tree mstp configuration
<brief | detail>
<routing-instance routing-instance-name>
```

**Syntax (EX Series Switch and the QFX Series)**

```
show spanning-tree mstp configuration
<brief | detail>
```

**Release Information**

Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for the QFX Series.

**Description**

Display the MSTP configuration.

**Options**

- **none**—Display MSTP configuration information.
- **brief | detail**—(Optional) Display the specified level of output.
- **routing-instance routing-instance-name**—(Optional) Display MSTP configuration information for the specified routing instance.

**Required Privilege Level**

`view`

**List of Sample Output**

- `show spanning-tree mstp configuration detail on page 4451`
- `show spanning-tree mstp configuration detail (QFX Series) on page 4451`

**Output Fields**

Table 551 on page 4450 lists the output fields for the `show spanning-tree mstp configuration` command. Output fields are listed in the approximate order in which they appear.

**Table 551: show spanning-tree mstp configuration Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context id</td>
<td>Internally generated identifier.</td>
</tr>
<tr>
<td>Region name</td>
<td>MSTP region name carried in the MSTP BPDUs.</td>
</tr>
<tr>
<td>Revision</td>
<td>Revision number of the MSTP configuration.</td>
</tr>
<tr>
<td>Configuration digest</td>
<td>Numerical value derived from the VLAN-to-instance mapping table.</td>
</tr>
<tr>
<td>MSTI</td>
<td>MST instance identifier.</td>
</tr>
<tr>
<td>Member VLANs</td>
<td>VLAN identifiers associated with the MSTI.</td>
</tr>
</tbody>
</table>
Sample Output

show spanning-tree mstp configuration detail

user@host> show spanning-tree mstp configuration routing-instance vs1 detail
MSTP configuration information
Context identifier : 1
Region name : henry
Revision : 3
Configuration digest : 0x6da4b5c4fd587757eef35675365e1

MSTI Member VLANs
0 0-99,101-199,201-4094
1 100
2 200

show spanning-tree mstp configuration detail (QFX Series)

user@lf0> show spanning-tree mstp configuration routing-instance vs1 detail
MSTP configuration information
Context identifier : 1
Region name : henry
Revision : 3
Configuration digest : 0x6da4b5c4fd587757eef35675365e1

MSTI Member VLANs
0 0-99,101-199,201-4094
1 100
2 200
show spanning-tree statistics

Syntax

```
show spanning-tree statistics
  interface interface-name
  vlan vlan-id
  <brief | detail>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
Option `vlan vlan-id` introduced in Junos OS Release 10.1 for EX Series switches.

Description

Display STP statistics on an interface, or for a VLAN when VSTP is enabled.

Options

- `none`—Display brief STP statistics.
- `brief | detail`—(Optional) Display the specified level of output.
- `interface interface-name`—(Optional) The name of the interface.
- `vlan vlan-id`—(Optional) The name of a VLAN.

Required Privilege

view

Related Documentation

- show spanning-tree bridge on page 4428
- Example: Configuring Network Regions for VLANs with MSTP on EX Series Switches on page 4330
- Understanding STP for EX Series Switches on page 4304
- Understanding RSTP for EX Series Switches on page 4300
- Understanding MSTP for EX Series Switches on page 4298
- Understanding VSTP for EX Series Switches on page 4306

List of Sample Output

```
show spanning-tree statistics interface on page 4453
```

Output Fields

Table 552 on page 4452 lists the output fields for the `show spanning-tree statistics` command. Output fields are listed in the approximate order in which they appear.

Table 552: show spanning-tree statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPDUs sent</td>
<td>Total number of BPDUs sent.</td>
</tr>
<tr>
<td>BPDUs received</td>
<td>Total number of BPDUs received.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface for which the statistics are being displayed.</td>
</tr>
<tr>
<td>Next BPDU transmission</td>
<td>Number of seconds until the next BPDU is scheduled to be sent.</td>
</tr>
</tbody>
</table>
Sample Output

show spanning-tree statistics interface

```
user@switch> show spanning-tree statistics interface ge-0/0/4
Interface   BPDUs sent   BPDUs received  Next BPDU transmission
ge-0/0/4      7     190     0
```
show spanning-tree statistics

**Syntax**

```
show spanning-tree statistics
  <brief | detail>
  <interface interface-name>
  <routing-instance routing-instance-name>
```

**Syntax (EX Series Switch and the QFX Series)**

```
show spanning-tree statistics
  <brief | detail>
  <interface interface-name | vlan vlan-id>
```

**Release Information**

Command introduced in Junos OS Release 8.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Command introduced in Junos OS Release 11.1 for QFX Series switches.

**Description**

Display STP statistics.

**Options**

- `none`—Display brief STP statistics.
- `brief | detail`—(Optional) Display the specified level of output.
- `interface interface-name`—(Optional) Display STP statistics for the specified interface.

**Required Privilege**

`view`

**List of Sample Output**

- `show spanning-tree statistics routing-instance on page 4455`
- `show spanning-tree statistics interface routing-instance detail on page 4455`

**Output Fields**

Table 553 on page 4454 lists the output fields for the `show spanning-tree statistics` command. Output fields are listed in the approximate order in which they appear.

**Table 553: show spanning-tree statistics Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message type</td>
<td>Type of message being counted.</td>
</tr>
<tr>
<td>BPDUs sent</td>
<td>Total number of BPDU sent.</td>
</tr>
<tr>
<td>BPDUs received</td>
<td>Total number of BPDU received.</td>
</tr>
<tr>
<td>BPDUs sent in last interval</td>
<td>Number of BPDU sent within a specified interval.</td>
</tr>
<tr>
<td>BPDUs received in last interval</td>
<td>Number of BPDU received within a specified interval.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface for which the statistics are being displayed.</td>
</tr>
</tbody>
</table>
Table 553: show spanning-tree statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Next BPDU transmission</strong></td>
<td>Number of seconds until the next BPDU is scheduled to be sent.</td>
</tr>
</tbody>
</table>

Sample Output

*show spanning-tree statistics routing-instance*

```
user@host> show spanning-tree statistics routing-instance vs1 detail
Routing instance level STP statistics
Message type : bpdus
BPDUs sent    : 1396
BPDUs received: 1027
BPDUs sent in last interval : 5        (duration: 4 sec)
BPDUs received in last interval: 4        (duration: 4 sec)
```

*show spanning-tree statistics interface routing-instance detail*

```
user@host> show spanning-tree statistics interface ge-1/1/4 routing-instance vs1 detail
Interface   BPDUs sent   BPDUs received      Next BPDU transmission
ge-1/1/4    7           190                0
```
Virtual Chassis

- Overview on page 4459
- Configuration on page 4485
- Administration on page 4529
- Troubleshooting on page 4605
Overview

Virtual Chassis Overview on page 4459

Understanding EX4300 Virtual Chassis on page 4459
Understanding EX Series Virtual Chassis Components on page 4460
Understanding How the Master in an EX Series Virtual Chassis Is Elected on page 4467
Understanding Software Upgrade in an EX Series Virtual Chassis on page 4468
Understanding Global Management of an EX Series Virtual Chassis on page 4469
Understanding Nonvolatile Storage in an EX Series Virtual Chassis on page 4472
Understanding EX Series Virtual Chassis Port Link Aggregation on page 4472
Understanding EX Series Virtual Chassis Configuration on page 4475
Understanding Split and Merge in an EX Series Virtual Chassis on page 4476
Understanding Automatic Software Update on EX Series Virtual Chassis Member Switches on page 4479
Understanding MAC Address Assignment on a Virtual Chassis on page 4482
Understanding High Availability on an EX Series Virtual Chassis on page 4483

Understanding EX4300 Virtual Chassis

EX4300 Virtual Chassis brings the Virtual Chassis flexible, scaling switch solution to the Juniper Networks EX4300 Ethernet Switch. You can connect up to ten EX4300 switches together to form one EX4300 Virtual Chassis and manage the unit as a single chassis. The advantages of connecting multiple switches into a Virtual Chassis include better-managed bandwidth at a network layer, simplified configuration and maintenance because multiple switches can be managed as a single switch, increased fault tolerance and high availability (HA) because a Virtual Chassis can remain active and network traffic can be redirected to other member switches when a single member switch fails, and a simplified Layer 2 network topology that minimizes or eliminates the need for loop prevention protocols such as Spanning Tree Protocol (STP).

The Virtual Chassis also provides a flexible model for expanding your network. If you are using an EX4300 switch or EX4300 Virtual Chassis at the access layer, for instance, and need additional access ports to support more servers, computers, phones, or other
devices, you can add an EX4300 switch as a Virtual Chassis member to increase the number of access ports on your network with minimal complications to the existing network topology and switch configuration. You can add this new switch to a Virtual Chassis if the switch is installed in the same building or at a different site because the long-distance optical ports can be used to interconnect EX4300 switches into the a Virtual Chassis.

You configure an EX4300 Virtual Chassis by configuring optical interfaces connecting EX4300 switches into Virtual Chassis ports (VCPs). VCPs connect switches together to form a Virtual Chassis, and are responsible for passing all data and control traffic between member switches in the Virtual Chassis. All 40-Gigabit QSFP+ optical ports on an EX4300 switch are configured as VCPs by default. All 10-Gigabit optical ports on an EX4300 switch can be configured into VCPs. You can increase the VCP bandwidth between any two member switches by connecting multiple VCP links between the switches. When multiple VCP links are interconnecting the same two member switches, a Link Aggregation Group (LAG) bundle is formed when the links are identical speeds. For instance, if you have four 40-Gigabit links configured as VCPs between member switches, a LAG with four member links at 160Gbps of bandwidth is formed. 10-Gigabit and 40-Gigabit links configured as VCPs cannot be members of the same LAG, however.

All models of EX4300 switches can be interconnected into the same EX4300 Virtual Chassis. EX4300 switches cannot be interconnected into a Virtual Chassis with any other Juniper Networks product, including other EX Series Ethernet Switches.

An EX4300 Virtual Chassis is configured, monitored, and maintained like other EX Series Virtual Chassis. See “Understanding EX Series Virtual Chassis Components” on page 4460.

Related Documentation

- Configuring an EX4300 Virtual Chassis (CLI Procedure) on page 4485
- Understanding EX Series Virtual Chassis Components on page 4460
- Understanding How the Master in an EX Series Virtual Chassis Is Elected on page 4467
- Understanding EX Series Virtual Chassis Port Link Aggregation on page 4472
- Understanding EX Series Virtual Chassis Configuration on page 4475

Understanding EX Series Virtual Chassis Components

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Understanding EX8200 Virtual Chassis Components for information about EX8200 Virtual Chassis.

This topic describes the components of EX Series Virtual Chassis—including the components of any mixed Virtual Chassis that contains EX4200, EX4500, or EX4550 member switches—except EX8200 Virtual Chassis.
Maximum Number of Switches per Virtual Chassis

The maximum number of switches that a Virtual Chassis supports varies by Virtual Chassis and can depend on the Junos OS release running on the Virtual Chassis. Table 554 on page 4461 lists the maximum member switch support by Virtual Chassis and Junos OS release.

Table 554: Maximum Member Switch Support for Virtual Chassis by Junos OS Release

<table>
<thead>
<tr>
<th>Maximum Member Switch Support</th>
<th>Initial Junos OS Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200 Virtual Chassis</td>
<td>12.2R1—Initial release. Support for up to four EX2200 member switches.</td>
</tr>
<tr>
<td>EX3300 Virtual Chassis</td>
<td>11.3R1—Initial release. Support for up to six EX3300 member switches 12.2R1—Support for up to ten EX3300 member switches</td>
</tr>
<tr>
<td>EX4200 Virtual Chassis</td>
<td>9.0R1—Initial release. Support for up to ten EX4200 member switches</td>
</tr>
<tr>
<td>EX4300 Virtual Chassis</td>
<td>13.2X50-D10—Initial release. Support for up to ten EX4300 member switches</td>
</tr>
<tr>
<td>EX4500 Virtual Chassis</td>
<td>11.1R1—Initial release. Support for up to two EX4500 switches 11.4R1—Support for up to ten EX4500 member switches</td>
</tr>
<tr>
<td>EX4550 Virtual Chassis</td>
<td>12.2R1—Initial release. Support for up to ten EX4550 switches</td>
</tr>
</tbody>
</table>
### Table 554: Maximum Member Switch Support for Virtual Chassis by Junos OS Release (continued)

<table>
<thead>
<tr>
<th>Maximum Member Switch Support</th>
<th>Initial Junos OS Release</th>
</tr>
</thead>
</table>
| Mixed EX4200 and EX4500 Virtual Chassis | 11.1R1—Initial release. Support for up to two EX4500 switches and up to eight EX4200 switches  
11.2R1—Support for up to nine EX4200 switches  
11.4R1—Support for up to nine EX4500 switches |
| Mixed EX4200 and EX4550 Virtual Chassis | 12.2R1—Initial release. Support for up to ten total EX4200 and EX4550 switches |
| Mixed EX4200, EX4500, and EX4550 Virtual Chassis | 12.2R1—Initial release. Support for up to ten total EX4200, EX4500, and EX4550 switches |
| Mixed EX4500 and EX4550 Virtual Chassis | 12.2R1—Initial release. Support for up to ten total EX4500 and EX4550 switches |

### Virtual Chassis Ports (VCPs)

You use Virtual Chassis ports (VCPs) to interconnect the member switches in a Virtual Chassis.

Some switches have dedicated VCPs. Dedicated VCPs allow you to interconnect switches without requiring any additional interface configuration. These switches have dedicated VCPs:

- EX4200 switches, on the rear panel
- EX4500 switches, on the Virtual Chassis module
- EX4550 switches, on the Virtual Chassis module

To interconnect switches that do not have dedicated VCPs or to interconnect switches across greater distances than allowed by a dedicated-VCP connection, you configure an optical port as a VCP. You can configure those VCPs on these switches:

- EX2200 switches, through an uplink port
- EX3300 switches, through an uplink port

**NOTE:** Uplink ports 2 and 3 on EX3300 switches are configured as VCPs by default.

- EX4200 switches, through uplink module ports (SFP, SFP+, or XFP) or through an SFP+ port on the EX4200-24F switch
- EX4300 switches, through uplink ports
NOTE: All QSFP+ ports on an EX4300 switch are configured as VCPs by default.

- EX4500 switches, through any SFP+ port
- EX4550 switches, through any SFP+ port

All supported SFP, SFP+, and XFP uplink connections between EX4200, EX4500, and EX4550 switches can be configured as VCPs.

You can increase the Virtual Chassis bandwidth between member switches by configuring multiple optical ports connecting the switches as VCPs. The optical ports configured as VCPs automatically form a Link Aggregation Group (LAG) bundle. See “Understanding EX Series Virtual Chassis Port Link Aggregation” on page 4472.

Master Role

The member that functions in the master role in the Virtual Chassis:

- Manages the member switches.
- Runs Junos OS for EX Series switches in a master role.
- Runs the chassis management processes and control protocols.
- Represents all the member switches interconnected within the Virtual Chassis configuration. (The hostname and other properties that you assign to this switch during setup apply to all members of the Virtual Chassis configuration.)

When an EX Series switch that supports Virtual Chassis is powered on as a standalone switch, it is considered the master member. In a Virtual Chassis, one member functions as the master and a second member functions as the backup:

- In a preprovisioned configuration, one of the two members assigned as routing-engine functions as the master member. The selection of which member assigned as routing-engine functions as master and which as backup is determined by the software based on the master election algorithm. See “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467.
- In a configuration that is not preprovisioned, the selection of the master and backup is determined by the mastership priority value and secondary factors in the master election algorithm.

In any mixed Virtual Chassis configuration that includes EX4200 switches, EX4500 switches, or EX4550 switches, any switch can be configured in any role in any configuration.

Backup Role

The member that functions in the backup role in the Virtual Chassis:

- Maintains a state of readiness to take over the master role if the master fails.
- Runs Junos OS for EX Series switches in a backup role.
• Synchronizes with the master in terms of protocol states, forwarding tables, and so forth, so that it is prepared to preserve routing information and maintain network connectivity without disruption in case the master is unavailable.

You must have at least two member switches in the Virtual Chassis configuration in order to have a backup member.

• In a preprovisioned configuration, one of the two members assigned as routing-engine functions in the backup role. The selection of which member assigned as routing-engine functions as master and which as backup is determined by the software based on the master election algorithm. See “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467.

• In a configuration that is not preprovisioned, the selection of the master and backup is determined by the mastership priority value and secondary factors in the master election algorithm.

In any mixed Virtual Chassis configuration that includes EX4200 switches, EX4500 switches, or EX4550 switches, any switch can be configured in any role in any configuration.

Linecard Role

A member that functions in the linecard role in the Virtual Chassis:

• Runs only a subset of Junos OS for EX Series switches.

• Does not run the chassis control protocols.

• Can detect certain error conditions (such as an unplugged cable) on any interfaces that have been configured on it through the master.

The Virtual Chassis configuration must have at least three members in order to include a linecard member.

• In a preprovisioned configuration, you can explicitly configure a member with the linecard role, which makes it ineligible for functioning as a master or backup.

• In a configuration that is not preprovisioned, the members that are not selected as master or backup function as linecard members of the Virtual Chassis configuration. The selection of the master and backup is determined by the mastership priority value and secondary factors in the master election algorithm. A switch with a mastership priority of 0 is always in the linecard role.

Member Switch and Member ID

Each standalone EX Series switch that supports Virtual Chassis is a potential member of a Virtual Chassis configuration. When one of those switches is powered on, it receives a member ID that can be seen by viewing the front-panel LCD or by entering the show virtual-chassis command. If the switch is powered on as a standalone switch, that member’s member ID is always 0. When the switch is interconnected with other switches in a Virtual Chassis configuration, its member ID is assigned by the master based on various factors, such as the order in which the switch was added to the Virtual Chassis.
configuration or the member ID assigned by a preprovisioned configuration. See “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467.

If the Virtual Chassis configuration previously included a member switch and that member was physically disconnected or removed from the Virtual Chassis configuration, its member ID is not available for assignment as part of the standard sequential assignment by the master. For example, you might have a Virtual Chassis configuration composed of member 0, member 2, and member 3, because member 1 was removed. When you add another member switch and power it on, the master assigns it as member 4.

The member ID distinguishes the member switches from one another. You use the member ID:

- To assign a mastership priority value to a member switch
- To configure interfaces for a member switch (The function is similar to that of a slot number on Juniper Networks routers.)
- To apply some operational commands to a member switch
- To display status or characteristics of a member switch

Mastership Priority

In a configuration that is not preprovisioned, you can designate the role (master, backup, or linecard) that a member switch assumes by configuring its mastership priority (from 0 through 255). The mastership priority value is the factor in the master election algorithm with the highest precedence for selecting the master of the Virtual Chassis configuration. A switch with a mastership priority of 0 never assumes the backup or master role.

The default value for mastership priority is 128 for EX2200, EX3300, EX4200, EX4500, and EX4550 switches. When a standalone switch is powered on, it receives the default mastership priority value. Because it is the only member of the Virtual Chassis configuration, it is also the master. When you interconnect a standalone switch to an existing Virtual Chassis configuration (which implicitly includes its own master), we recommend that you explicitly configure the mastership priority of the members that you want to function as the master and backup.

NOTE: Configuring the same mastership priority value for both the master and backup helps to ensure a smooth transition from master to backup when the master becomes unavailable. It prevents the original master from preempting control from the backup when the backup has taken control of the Virtual Chassis configuration because the original master became unavailable.

In a preprovisioned configuration, you assign the role of each member switch.

Mixed Virtual Chassis

EX4200 switches, EX4500 switches, and EX4550 switches can be interconnected into the same Virtual Chassis to form a mixed EX4200 and EX4500 Virtual Chassis, mixed
EX4200 and EX4550 Virtual Chassis, mixed EX4500 and EX4550 Virtual Chassis, or mixed EX4200, EX4500, and EX4550 Virtual Chassis.

The other EX Series switches that support Virtual Chassis—EX2200, EX3300, and EX4300 switches—cannot be a part of any mixed Virtual Chassis.

A mixed Virtual Chassis supports up to 10 member switches regardless of whether the switches are EX4200 switches, EX4500 switches, or EX4550 switches. Any model of EX4200, EX4500, or EX4550 switch can be interconnected into the same mixed Virtual Chassis. The master election process that decides member switch roles in a mixed Virtual Chassis is identical to the master election process in a non-mixed Virtual Chassis, so any member switch in a mixed Virtual Chassis can assume the master, backup, or linecard role.

**Virtual Chassis Identifier (VCID)**

All members of a Virtual Chassis configuration share one Virtual Chassis identifier (VCID). This identifier is derived from internal parameters. When you are monitoring a Virtual Chassis configuration, the VCID is displayed in certain interface views and is also part of the `show virtual-chassis` output.

---

**Related Documentation**

- *Understanding EX8200 Virtual Chassis Components*
- *EX Series Virtual Chassis Overview*
  - Understanding EX4300 Virtual Chassis on page 4459
  - Example: Configuring an EX4200 Virtual Chassis with a Master and Backup in a Single Wiring Closet
  - Example: Configuring an EX4500 Virtual Chassis with a Master and Backup in a Single Wiring Closet
  - Example: Configuring an EX4200 Virtual Chassis Using a Preprovisioned Configuration File
  - Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure) on page 4497
  - Setting an Uplink Port as a Virtual Chassis Port on an EX4500 or EX4550 Switch (CLI Procedure)
Understanding How the Master in an EX Series Virtual Chassis Is Elected

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See EX8200 Virtual Chassis Overview for information about EX8200 Virtual Chassis.

All switches that are interconnected in a Virtual Chassis configuration are member switches of that Virtual Chassis. Each Virtual Chassis configuration has one member that functions as the master and controls the Virtual Chassis configuration.

When a Virtual Chassis configuration boots, the Juniper Networks Junos operating system (Junos OS) on the switches automatically runs a master election algorithm to determine which member switch assumes the role of master.

The algorithm proceeds from the top condition downward until the stated condition is satisfied:

1. Choose the member with the highest user-configured mastership priority (255 is the highest possible value). A switch with a mastership priority of 0 will always stay in the linecard role.
2. Choose the member that was master the last time the Virtual Chassis configuration booted.
3. Choose the member that has been included in the Virtual Chassis configuration for the longest period of time. (For this to be a deciding factor, there has to be a minimum time lapse of 1 minute between the power-ons of the individual interconnected member switches.)
4. Choose the member with the lowest MAC address.

The variations among switches and switch models do not impact the master election algorithm.

To ensure that a specific member is elected as the master:

1. Power on only the switch that you want to configure as master of the Virtual Chassis configuration.
2. Configure the mastership priority of that member to have the highest possible value (255).
3. Continue to configure other members through the master member.
4. Power on the other members.

You can also specify the switch roles by preprovisioning your Virtual Chassis. Preprovisioning a Virtual Chassis allows you to manually assign the member ID and role for each switch in the Virtual Chassis. See Configuring an EX3300 Virtual Chassis (CLI Procedure) and Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure).
Understanding Software Upgrade in an EX Series Virtual Chassis

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Understanding Software Upgrades in an EX8200 Virtual Chassis for information about EX8200 Virtual Chassis.

In a Virtual Chassis, each member switch must be running the same version of Juniper Networks Junos operating system (Junos OS).

You can install a new Junos OS release on the entire Virtual Chassis or on a particular member in the Virtual Chassis by using the same CLI command that you use to install Junos OS on standalone switches—the `request system software add` command.

You can use the automatic software update feature to automatically update the Junos OS version on member switches as you add them to a Virtual Chassis. See “Understanding Automatic Software Update on EX Series Virtual Chassis Member Switches” on page 4479. If you are not configuring the automatic software update feature, we recommend that you update the new member switch to the version of Junos OS running on the Virtual Chassis before adding the member switch to the Virtual Chassis.

In any mixed Virtual Chassis, the member switches must be running the same version of Junos OS. You can upgrade all member switches simultaneously by specifying a path to multiple Junos OS images in the same `request system software add` command. Multiple Junos OS images are needed to upgrade a mixed Virtual Chassis because an EX4200 switch runs a different version of Junos OS than an EX4500 or EX4550 switch. See Installing Software on a Mixed Virtual Chassis with EX4200, EX4500, and EX4550 Switches (CLI Procedure).

NOTE: EX4500 and EX4550 switches run the same Junos OS image. You do not need to use multiple Junos OS images when updating a mixed EX4500 and EX4550 Virtual Chassis.

You can also use nonstop software upgrade (NSSU) to upgrade Junos OS on all members. NSSU provides an orderly upgrade of each member of the Virtual Chassis and takes advantage of graceful Routing Engine switchover, nonstop active routing, and link aggregation to minimize traffic disruption during the upgrade. For more information about NSSU, see Understanding Nonstop Software Upgrade on EX Series Switches.
Understanding Global Management of an EX Series Virtual Chassis

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Understanding Global Management of an EX8200 Virtual Chassis for information about EX8200 Virtual Chassis.

A Virtual Chassis is composed of multiple switches, and it, therefore, has multiple console ports and multiple out-of-band management Ethernet ports located on the switches.

You can connect a PC or laptop directly to a console port of any member switch to set up and configure the Virtual Chassis. When you connect to the console port of any member switch, the console session is redirected to the master switch, as shown in Figure 71 on page 4470.
Figure 71: Console Session Redirection (EX4200 Virtual Chassis Pictured)

If the master becomes unavailable, the console session is disconnected from the old master and a new session is established with the newly elected master.

An out-of-band management Ethernet port is often referred to simply as a management Ethernet port. It uses a dedicated management channel for device maintenance and allows a system administrator to monitor and manage the switch by remote control.

The Virtual Chassis configuration can be managed remotely through SSH or Telnet using a global management interface called the virtual management Ethernet (VME) interface. The VME interface is a logical interface representing all of the out-of-band management ports on the member switches. When you connect to the Virtual Chassis configuration using the VME interface’s IP address, the connection is redirected to the master member as shown in Figure 72 on page 4471.
If the master management Ethernet link is unavailable, the session is redirected through the backup management Ethernet link. If there is no active management Ethernet link on the backup, the VME interface chooses a management Ethernet link on one of the linecard members, selecting the linecard member with the lowest member ID as its first choice.

You can configure an IP address for the VME global management interface at any time.

You can perform remote configuration and administration of all members of the Virtual Chassis configuration through the VME interface.

Related Documentation

- Understanding Global Management of an EX8200 Virtual Chassis
- Understanding EX Series Virtual Chassis Components on page 4460
- Example: Configuring an EX4200 Virtual Chassis with a Master and Backup in a Single Wiring Closet
Configuring the Virtual Management Ethernet Interface for Global Management of an EX Series Virtual Chassis (CLI Procedure)

Understanding Nonvolatile Storage in an EX Series Virtual Chassis

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Understanding File Storage in an EX8200 Virtual Chassis for information about EX8200 Virtual Chassis.

The EX2200, EX3300, EX4200, EX4300, EX4500, and EX4550 switches store the Juniper Networks Junos operating system (Junos OS) system files in internal flash memory. In the Virtual Chassis configurations, both the master and the backup switch store the configuration information for all the member switches.

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Understanding Virtual Chassis Port Link Aggregation in an EX8200 Virtual Chassis for information about EX8200 Virtual Chassis.

You can combine physical Ethernet ports belonging to different member switches of a Virtual Chassis configuration to form a logical point-to-point link, known as a link aggregation group (LAG) or bundle. A LAG provides more bandwidth than a single Ethernet link can provide. Additionally, link aggregation provides network redundancy by load-balancing traffic across all available links. If one of the links fails, the system automatically load-balances traffic across all remaining links.

Nonvolatile Memory Features

Junos OS optimizes the way the Virtual Chassis stores its configuration if a member switch or the Virtual Chassis configuration is shut down improperly:

- If the master is not available, the backup switch takes on the role of the master and its internal flash memory takes over as the alternate location for maintaining nonvolatile configuration memory.
- If a member switch is taken offline for repair, the master stores the configuration of the member switch.

Related Documentation

- Understanding File Storage in an EX8200 Virtual Chassis
- Command Forwarding Usage with an EX Series Virtual Chassis on page 4529
- Monitoring System Properties on page 714

Understanding EX Series Virtual Chassis Port Link Aggregation
Similarly, if a Virtual Chassis member switch that has LAG member interfaces on multiple member switches fails for any reason, the traffic traversing the LAG can be redirected through the active member switch. This setup has benefits for failover purposes and can be especially beneficial in cases when a member switch needs to be inactive for some time, such as during a software upgrade using NSSU.

You can configure any optical uplink port that can be used to connect EX2200, EX3300, EX4200, EX4300, EX4500, or EX4550 switches together into a Virtual Chassis port (VCP). You can configure multiple optical uplink interfaces between two member switches in the same Virtual Chassis as VCPs. If you have configured two or more optical ports as VCPs connecting the same member switches, the optical uplink ports configured as VCPs automatically form a LAG provided the optical uplink ports are configured to operate at the same link speeds. Each LAG is assigned a positive-integer identifier called a trunk ID.

On EX2200 and EX2200-C switches only, you can also configure the RJ-45 interfaces, including built-in network ports with 10/100/1000BASE-T Gigabit Ethernet connectors and 1000BASE-T RJ-45 transceivers, into VCPs. On EX2200 and EX2200-C switches, a LAG that includes up to 8 interfaces configured as VCPs automatically forms. The LAG bundles includes all interfaces configured as VCPs, regardless of whether the interfaces are optical transceiver interfaces, RJ-45 transceiver interfaces, or built-in network ports with 10/100/1000BASE-T Gigabit Ethernet connectors.

You can create an optical VCP LAG connecting any two member switches in any Virtual Chassis, including VCP LAG connections interconnecting different switch models in a mixed Virtual Chassis.

On an EX2200 switch only, you can also configure all RJ-45 interfaces, including built-in network ports with 10/100/1000BASE-T Gigabit Ethernet connectors and 1000BASE-T RJ-45 transceivers, on EX2200 and EX2200-C switches, into VCPs. The RJ-45 interfaces also automatically form a LAG when configured into VCPs.

Table 555 on page 4473 provides the maximum member link limit for each optical VCP LAG.

### Table 555: Maximum Member Links in LAGs Over Optical Interface VCPs

<table>
<thead>
<tr>
<th>Member Switch 1</th>
<th>Member Switch 2</th>
<th>Maximum Member Links in VCP LAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2200 Switch</td>
<td>EX2200 Switch</td>
<td>8</td>
</tr>
<tr>
<td>EX3300 Switch</td>
<td>EX3300 Switch</td>
<td>8</td>
</tr>
<tr>
<td>EX4200 Switch</td>
<td>EX4200 Switch</td>
<td>8</td>
</tr>
<tr>
<td>EX4200 Switch</td>
<td>EX4500 Switch</td>
<td>8</td>
</tr>
<tr>
<td>EX4200 Switch</td>
<td>EX4550 Switch</td>
<td>8</td>
</tr>
<tr>
<td>EX4500 Switch</td>
<td>EX4500 Switch</td>
<td>8</td>
</tr>
<tr>
<td>EX4500 Switch</td>
<td>EX4550 Switch</td>
<td>8</td>
</tr>
</tbody>
</table>
Table 555: Maximum Member Links in LAGs Over Optical Interface VCPs (continued)

<table>
<thead>
<tr>
<th>Member Switch 1</th>
<th>Member Switch 2</th>
<th>Maximum Member Links in VCP LAG</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX4550 Switch</td>
<td>EX4550 Switch</td>
<td>8</td>
</tr>
</tbody>
</table>

A LAG over uplink VCPs provides higher overall bandwidth for forwarding traffic between the member switches connected by the optical VCPs, faster management communications, and greater redundancy of operations among the members than would be available without the LAG. A LAG over uplink VCPs provides an additional Virtual Chassis link throughput for the switches.

See “Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure)” on page 4497 for information about configuring uplink ports as VCPs.

NOTE: The interfaces that are included within a bundle or LAG are sometimes referred to as member interfaces. Do not confuse this term with member switches, which refers to switches that are interconnected as a Virtual Chassis. It is possible to create a LAG that is composed of member interfaces that are located in different member switches of a Virtual Chassis.

Related Documentation

- Understanding Virtual Chassis Port Link Aggregation in an EX8200 Virtual Chassis
- EX Series Virtual Chassis Overview
- Understanding Aggregated Ethernet Interfaces and LACP on page 2272
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring Aggregated Ethernet High-Speed Uplinks with LACP Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- Example: Configuring an EX4200 Virtual Chassis Interconnected Across Multiple Wiring Closets
- Example: Connecting EX4500 Member Switches in a Virtual Chassis Across Wiring Closets
- Example: Configuring Link Aggregation Groups Using EX4200 Uplink Virtual Chassis Ports
Understanding EX Series Virtual Chassis Configuration

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Understanding EX8200 Virtual Chassis Components for information about EX8200 Virtual Chassis.

You configure and manage almost all aspects of an EX Series Virtual Chassis configuration through the master switch of the Virtual Chassis. However, you can also configure Virtual Chassis parameters when a switch is a standalone switch not interconnected with other members.

EX Series switches that support Virtual Chassis have some innate characteristics of a Virtual Chassis by default. A standalone switch is assigned member ID 0 and is the master of itself. Therefore, you can edit its Virtual Chassis configuration. When the standalone switch is interconnected with an existing Virtual Chassis configuration, the Virtual Chassis configuration statements and any uplink Virtual Chassis port (VCP) settings that you previously specified on the standalone switch remain part of its configuration.

A switch is not recognized by the Virtual Chassis as a member switch until it is interconnected with the master or interconnected with an existing member of the Virtual Chassis.

EX2200, EX3300, and EX4300 switches do not have dedicated VCPs. These switches form a Virtual Chassis by configuring optical ports connecting the member switches into VCPs. You can expand the uplink connections on these switches over long distances to connect switches at different locations into the same Virtual Chassis.

NOTE: Uplink ports 2 and 3 on any EX3300 switch are configured, by default, as VCPs. You can change this default configuration or configure another uplink port as a VCP on an EX3300 switch.

QSFP+ ports on an EX4300 switch are also configured, by default, as VCPs.

On all other EX Series switches, the optical ports are not configured as VCPs by default.

When an EX4200, EX4500, or EX4550 switch is located too far away to be interconnected through dedicated VCPs, you can configure an optical port as a VCP.

A link aggregation group (LAG) will be formed automatically when the new switch is added to the configuration if more than one such link with the same speed is detected between optical VCPs on the new member and an existing member. See “Understanding EX Series Virtual Chassis Port Link Aggregation” on page 4472.

When an optical port is set as a VCP, it cannot be used for any other purpose. If you want to use the optical port for another purpose, you must delete the VCP setting. You can
execute this command directly on the member whose uplink VCP setting you want to delete or through the master of the Virtual Chassis configuration.

**CAUTION:** Deleting a VCP in a Virtual Chassis configuration can cause the Virtual Chassis configuration to split. For more information, see “Understanding Split and Merge in an EX Series Virtual Chassis” on page 4476.

You can create a preprovisioned configuration. This type of configuration allows you to deterministically control the member ID and role assigned to a member switch by associating the switch with its serial number. For an example of a preprovisioned configuration, see *Example: Configuring an EX4200 Virtual Chassis Using a Preprovisioned Configuration File*.

**NOTE:** If a switch is interconnected with other switches in a Virtual Chassis configuration, each individual switch that is included as a member of the configuration is identified with a member ID. The member ID functions as an FPC slot number. When you are configuring interfaces for a Virtual Chassis configuration, you specify the appropriate member ID as the slot element of the interface name.

The default factory settings for a Virtual Chassis configuration include FPC 0 as a member of the default VLAN because FPC 0 is configured as part of the ethernet-switching family. To include the FPC in the default VLAN, add the ethernet-switching family to the configurations for those interfaces.

---

**Related Documentation**

- *Understanding EX8200 Virtual Chassis Components*
- *Understanding EX Series Virtual Chassis Components on page 4460*
- *Understanding How the Master in an EX Series Virtual Chassis Is Elected on page 4467*
- *Configuring an EX3300 Virtual Chassis (CLI Procedure)*
- *Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)*

---

**Understanding Split and Merge in an EX Series Virtual Chassis**

**NOTE:** This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis.

In a Virtual Chassis, two or more switches are connected together to form a unit that is managed as a single chassis. If there is a disruption to the Virtual Chassis configuration due to member switches failing or being removed from the configuration, the Virtual Chassis configuration splits into two separate Virtual Chassis. This situation could cause disruptions in the network if the two separate configurations share common resources, such as global IP addresses. The split and merge feature provides a method to prevent
the separate Virtual Chassis configurations from adversely affecting the network and also allows the two parts to merge back into a single Virtual Chassis configuration.

**NOTE:** If a Virtual Chassis configuration splits into separate parts, we recommend that you resolve the problem that caused the Virtual Chassis configuration to split as soon as possible.

You can also use this feature to merge two active but separate Virtual Chassis that have not previously been part of the same configuration into one Virtual Chassis configuration.

**NOTE:** The split and merge feature is enabled by default on EX Series switches. You can disable the split and merge feature by using the `set virtual-chassis no-split-detection` command.

This topic describes:

- **What Happens When a Virtual Chassis Configuration Splits** on page 4477
- **Merging Virtual Chassis Configurations** on page 4478

**What Happens When a Virtual Chassis Configuration Splits**

When a Virtual Chassis configuration splits into two separate Virtual Chassis configurations, the individual member switches detect this topology change and run the master election algorithm to select a new master for each of the two Virtual Chassis configurations. The new masters then determine whether their Virtual Chassis configuration remains active. One of the configurations remains active based on the following:

- It contains both the stable master and the stable backup (that is, the master and backup from the original Virtual Chassis configuration before the split).
- It contains the stable master and the configuration is greater than half the Virtual Chassis size.
- It contains the stable backup and is at least half the Virtual Chassis size.

In accordance with the rules given in the second and third list items, if the Virtual Chassis configuration splits into two equal parts and the stable master and stable backup are in different parts, then the part that contains the stable backup becomes active.

**NOTE:** The number of members in the Virtual Chassis configuration includes all member switches connected to date minus the number whose Virtual Chassis member IDs have been recycled (that is, made available for reassignment). Therefore, the size of the Virtual Chassis configuration increases when a new member switch is detected and decreases when a member switch’s ID is recycled.
These rules ensure that only one of the two separate Virtual Chassis configurations created by the split remains active. The member switches in the inactive Virtual Chassis configuration remain in a linecard role. For the inactive members to become active again, one of the following things must happen:

- The problem that caused the original Virtual Chassis configuration to split is resolved, allowing the two Virtual Chassis configurations to merge.
- You load the factory default configuration on the inactive members, which causes the inactive members to function as standalone switches or become part of a different Virtual Chassis configuration.

**NOTE:** When you remove a member switch from a Virtual Chassis configuration, we recommend that you recycle the member ID using the request virtual-chassis recycle command.

### Merging Virtual Chassis Configurations

There are two scenarios in which separate Virtual Chassis merge:

- A Virtual Chassis configuration that had split into two is now merging back into a single configuration because the problem that had caused it to split has been resolved.
- You want to merge two Virtual Chassis that had not previously been configured together.

Every Virtual Chassis configuration has a unique ID (VCID) that is automatically assigned when the Virtual Chassis configuration is formed. You can also explicitly assign a VCID using the set virtual-chassis id command. A VCID that you assign takes precedence over automatically assigned VCIDs.

When you reconnect the separate Virtual Chassis configurations or connect them for the first time, the members determine whether or not the separate Virtual Chassis configurations can merge. The members use the following rules to determine whether a merge is possible:

- If the Virtual Chassis configurations have the same VCID, then the configurations can merge. If the two Virtual Chassis were formed as the result of a split, they have the same VCID.
- If the VCIDs are different, then the two configurations can merge only if both are active (inactive configurations cannot merge, ensuring that members removed from one Virtual Chassis configuration do not become members of another Virtual Chassis configuration). If the configurations to merge are both active and one of them has a user-configured VCID, this ID becomes the ID of the merged Virtual Chassis. If neither Virtual Chassis has a user-configured VCID, then the VCID of the configuration with the highest mastership priority becomes the ID of the merged Virtual Chassis. The resulting merged Virtual Chassis configuration is active.

When you connect two Virtual Chassis configurations, the following events occur:
1. Connecting the two split Virtual Chassis configurations triggers the shortest-path-first (SPF) algorithm. The SPF algorithm computes the network topology and then triggers the master election algorithm. The master election algorithm waits for the members to synchronize the topology information before running.

2. The master election algorithm merges the VCIDs of all the members.

3. Each member runs the master election algorithm to select a master and a backup from among all members with the same VCIDs. For more information, see “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467.

4. The master determines whether the Virtual Chassis configuration is active or inactive. (See “What Happens When a Virtual Chassis Configuration Splits” on page 4477.)

5. If the Virtual Chassis configuration is active, the master assigns roles to all members. If the Virtual Chassis configuration is inactive, the master assigns all members the role of linecard.

6. When the other members receive their role from the master, they change their role to backup or linecard. They also use the active or inactive state information sent by the master to set their own state to active or inactive and to construct the Virtual Chassis member list from the information sent by the master.

7. If the Virtual Chassis state is active, the master waits for messages from the members indicating that they have changed their roles to the assigned roles, and then the master changes its own role to master.

**NOTE:** When you merge two Virtual Chassis that had not previously been part of the same Virtual Chassis configuration, any configuration settings (such as the settings for Telnet and FTP services, graceful Routing Engine switchover (GRES), fast failover, VLANs, and so on) that exist on the new master become the configuration settings for all members of the new Virtual Chassis, overwriting any other configuration settings.

### Related Documentation
- Understanding EX Series Virtual Chassis Configuration on page 4475
- Example: Assigning the Virtual Chassis ID to Determine Precedence During an EX4200 Virtual Chassis Merge
- Assigning the Virtual Chassis ID to Determine Precedence During an EX Series Virtual Chassis Merge (CLI Procedure) on page 4503
- Disabling Split and Merge in an EX Series Virtual Chassis (CLI Procedure) on page 4502

**Understanding Automatic Software Update on EX Series Virtual Chassis Member Switches**

You can use the automatic software update feature to automatically update the Juniper Networks Junos operating system (Junos OS) version on prospective member switches as you add them to an EX Series Virtual Chassis.
This topic includes:

- Automatic Software Update Basics on page 4480
- Automatic Software Update Restrictions on page 4480

**Automatic Software Update Basics**

When you have configured automatic software update on a Virtual Chassis, the Junos OS version is updated on the new member switch when you add it to the Virtual Chassis. The new member switch immediately joins the Virtual Chassis configuration and is put in the active state.

For a standalone switch to join an existing Virtual Chassis, it must be running the same version of Junos OS that is running on the Virtual Chassis master. When the master in a Virtual Chassis detects that a new switch has been added to the configuration, it checks the software version on the new switch. If the software version on the new switch is not the same as the version running on the master, the master keeps the new switch in the inactive state. If you have not enabled the automatic software update feature, you have to manually install the correct software version on each prospective member switch as it is added to the Virtual Chassis.

**Automatic Software Update Restrictions**

You cannot use automatic software update in certain scenarios, and you must ensure that the software release version on the Virtual Chassis is supported by the release on the prospective member switch.

You cannot use the automatic software update feature to update software for a prospective member switch in the following scenarios:

- The Virtual Chassis was preprovisioned and is running Junos OS Release 10.4R2 or earlier.
- You configured the `mastership-priority` command to manually configure the mastership priority of at least one Virtual Chassis member switch and the Virtual Chassis was running Junos OS Release 10.4R2 or earlier when you committed this configuration.
- The Junos OS versions on the Virtual Chassis and the prospective member switch are different versions of the same major Junos OS release. For instance, if a Virtual Chassis is running Junos OS Release 10.4R1, the prospective member switch cannot be updated using automatic software update if it is running Junos OS Release 10.4R2, 10.4R3, or any other Junos OS Release 10.4 release version.

The automatic software update feature also has a Junos OS release dependency between the release that is already running on the Virtual Chassis and the release that is running on the prospective member switch.

Table 556 on page 4481 summarizes automatic software update support for each Junos OS release combination.
## Table 556: Automatic Software Update Support

<table>
<thead>
<tr>
<th>Virtual Chassis Junos OS Release</th>
<th>Supported Junos OS Releases for Prospective Member Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>All versions of Junos OS 9.0 through 9.6</td>
<td>All versions of Junos OS 9.0 through 9.6, Junos OS Releases 10.0R1 through 10.0R4, All versions of Junos OS Release 10.1, Junos OS Releases 10.2R1 through 10.2R3, Junos OS Releases 10.3R1 through 10.3R3</td>
</tr>
<tr>
<td>Junos OS Releases 10.0R1 through 10.0R4</td>
<td>All versions of Junos OS 9.0 through 9.6, Junos OS Releases 10.0R1 through 10.0R4, All versions of Junos OS Release 10.1, Junos OS Releases 10.2R1 through 10.2R3, Junos OS Releases 10.3R1 through 10.3R3</td>
</tr>
<tr>
<td>Junos OS Release 10.0R5 and later 10.0 releases</td>
<td>Junos OS Release 10.2R4 and later 10.2 releases, Junos OS Release 10.3R4 and later 10.3 releases, All versions of Junos OS Release 10.4, All versions of Junos OS Release 11.1</td>
</tr>
<tr>
<td>All versions of Junos OS Release 10.1</td>
<td>All versions of Junos OS 9.0 through 9.6, Junos OS Releases 10.0R1 through 10.0R4, Junos OS Releases 10.2R1 through 10.2R3, Junos OS Releases 10.3R1 through 10.3R3</td>
</tr>
<tr>
<td>Junos OS Releases 10.2R1 through 10.2R3</td>
<td>All versions of Junos OS 9.0 through 9.6, Junos OS Releases 10.0R1 through 10.0R4, All versions of Junos OS Release 10.1, Junos OS Releases 10.3R1 through 10.3R3</td>
</tr>
<tr>
<td>Junos OS Release 10.2R4 and later 10.2 releases</td>
<td>Junos OS Release 10.0R5, Junos OS Release 10.3R4 and later 10.3 releases, All versions of Junos OS Release 10.4, All versions of Junos OS Release 11.1</td>
</tr>
<tr>
<td>Junos OS Releases 10.3R1 through 10.3R3</td>
<td>All versions of Junos OS 9.0 through 9.6, Junos OS Releases 10.0R1 through 10.0R4, All versions of Junos OS Release 10.1, Junos OS Releases 10.2R1 through 10.2R3</td>
</tr>
<tr>
<td>Junos OS Release 10.3R4 and later 10.3 releases</td>
<td>Junos OS Release 10.0R5, All versions of Junos OS Release 10.4, All versions of Junos OS Release 11.1</td>
</tr>
<tr>
<td>Junos OS Releases 10.4R1 through 10.4R3</td>
<td>All versions of Junos OS 9.0 through 9.6, Junos OS Releases 10.0R1 through 10.0R4, All versions of Junos OS Release 10.1, Junos OS Releases 10.2R1 through 10.2R3, Junos OS Releases 10.3R1 through 10.3R3</td>
</tr>
<tr>
<td>Junos OS Release 10.4R4 and later 10.4 releases</td>
<td>Junos OS Release 10.0R5, Junos OS Release 10.2R4 and later 10.2 releases, Junos OS Release 10.3R4 and later 10.3 releases, All versions of Junos OS Release 11.1</td>
</tr>
</tbody>
</table>
Table 556: Automatic Software Update Support (continued)

<table>
<thead>
<tr>
<th>Virtual Chassis Junos OS Release</th>
<th>Supported Junos OS Releases for Prospective Member Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junos OS Release 11.1R1</td>
<td>All versions of Junos OS Release 10.4</td>
</tr>
<tr>
<td></td>
<td>Junos OS Release 11.2 and later Junos OS releases</td>
</tr>
<tr>
<td>Junos OS Release 11.1R2 and</td>
<td>Junos OS Release 10.0R5</td>
</tr>
<tr>
<td>later Junos OS releases</td>
<td>Junos OS Release 10.2R4 and later 10.2 releases</td>
</tr>
<tr>
<td></td>
<td>Junos OS Release 10.3R4 and later 10.3 releases</td>
</tr>
<tr>
<td></td>
<td>Junos OS Release 11.2 and later Junos OS releases</td>
</tr>
</tbody>
</table>

Related Documentation

- Understanding Software Upgrade in an EX Series Virtual Chassis on page 4468
- Example: Configuring Automatic Software Update on EX4200 Virtual Chassis Member Switches
- Configuring Automatic Software Update on EX Series Virtual Chassis Member Switches (CLI Procedure) on page 4502

Understanding MAC Address Assignment on a Virtual Chassis

In a Virtual Chassis, multiple Juniper Networks EX Series Ethernet Switches—each with its own set of interfaces with unique MAC addresses—are connected together to form one chassis that can be managed as a single switch. The MAC address assigned to each network-facing interface on the switch changes when the switch joins a Virtual Chassis. Because all Layer 2 traffic decisions are based on an interface's MAC address, understanding MAC address assignment is important to understanding how network traffic is forwarded and received by the Virtual Chassis. For additional information about how a network uses MAC addresses to forward and receive traffic, see “Understanding Bridging and VLANs on EX Series Switches” on page 2049.

When a Virtual Chassis is formed, the MAC address of the switch in the master role becomes the system MAC base address. The Virtual Chassis assigns the system MAC base address as the MAC address for all Layer 3 interfaces within the Virtual Chassis. The Virtual Chassis also assigns the system MAC base address to the virtual management Ethernet (VME) interface and to all of the virtual LANs (VLANs) in the Virtual Chassis.

The system MAC base address does not change in the event of a switchover if the switch that was originally configured in the master role remains a member of the Virtual Chassis. If the switch that was originally configured in the master role is removed from the Virtual Chassis, the MAC address of the current member switch in the master role is assigned as the system MAC base address after the MAC persistence timer interval has expired. You can configure the MAC persistence timer interval.

For Layer 2 and aggregated Ethernet interfaces, the Virtual Chassis assigns a unique MAC address that is derived from the member switch MAC address to each interface. The assignment of a unique MAC address to each network interface helps ensure that functions that require MAC address differentiation—such as redundant trunk groups (RTGs), Link Aggregation Control Protocol (LACP), and general monitoring functions—can function properly.
NOTE: Unique MAC address assignment for Layer 2 and aggregated Ethernet interfaces in a Virtual Chassis was introduced in Junos OS Release 11.3. The same MAC address could be assigned to interfaces on different member switches in the same Virtual Chassis prior to this release.

If you reconfigure a Layer 2 interface into a Layer 3 interface, or the reverse, within a Virtual Chassis, the MAC address of that interface changes accordingly.

MAC addresses are assigned to interfaces in a Virtual Chassis automatically—no user configuration is possible or required. You can view the MAC addresses that are assigned to the interfaces by using the `show interfaces` command.

**Related Documentation**
- Understanding MAC Address Assignment in an EX Series Switch
- Configuring the Timer for the Backup Member to Start Using Its Own MAC Address, as Master of an EX Series Virtual Chassis (CLI Procedure) on page 4501
- EX Series Virtual Chassis Overview
- EX8200 Virtual Chassis Overview

### Understanding High Availability on an EX Series Virtual Chassis

You increase your network's high availability (HA) when you interconnect a Juniper Networks EX Series Ethernet switch into a Virtual Chassis. A Virtual Chassis is more fault tolerant than a standalone EX series switch because it remains up when a single member switch fails.

You can further improve HA by configuring the HA features available for your EX Series Virtual Chassis. You can, for instance, configure Link Aggregation Groups (LAG) bundles to include member links on multiple member switches in the same Virtual Chassis. This configuration increases fault tolerance because traffic traversing the LAG can be redirected to an active member switch when a single member switch fails.

A Virtual Chassis has dual Routing Engines—the switch in the master role and the switch in the backup role—and therefore supports many HA features not supported on standalone EX Series switches. For a complete list of High Availability features available for your EX Series Virtual Chassis, see “EX Series Virtual Chassis Software Features Overview” on page 75.

Many HA features for the EX Series Virtual Chassis are designed to improve network resiliency after a Routing Engine switchover. Table 557 on page 4484 describes the effects of a Routing Engine switchover when no high availability features are enabled and when some High Availability features are enabled.
Table 557: Effects of a Routing Engine Switchover

<table>
<thead>
<tr>
<th>High Availability Feature</th>
<th>Effect of Routing Engine Switchover</th>
</tr>
</thead>
<tbody>
<tr>
<td>No HA features enabled</td>
<td>Kernel and forwarding state information is not preserved to the backup Routing Engine. A convergence process that requires all interfaces on the Virtual Chassis to be taken offline has to be performed before the Virtual Chassis returns online. The switchover can take several minutes and the Virtual Chassis does not send or receive traffic until the switchover is complete.</td>
</tr>
<tr>
<td>Graceful Routing Engine switchover (GRES) enabled</td>
<td>Kernel and forwarding state information is preserved on both Routing Engines, so the convergence process does not occur and the switchover happens quickly with minimal traffic loss.</td>
</tr>
<tr>
<td>Nonstop active routing (NSR), Nonstop bridging (NSB), or both enabled</td>
<td>Layer 2 protocols that are supported by NSB are not disrupted by a Routing Engine switchover when NSB is enabled. Layer 2 protocol information for all active Layer 2 protocols is stored on both Routing Engines when NSB is enabled. Layer 3 protocols that are supported by NSR are not disrupted by a Routing Engine switchover when NSR is enabled. Layer 3 protocol information for all active Layer protocols is stored on both Routing Engines when NSR is enabled.</td>
</tr>
<tr>
<td>Graceful Protocol Restart enabled</td>
<td>Traffic is not interrupted during the switchover. Interface and kernel information is preserved. Graceful restart protocol extensions quickly collect and restore routing information for supported protocols from the neighboring devices.</td>
</tr>
</tbody>
</table>

Related Documentation
- [EX Series Virtual Chassis Overview](#)
- [High Availability Features for EX Series Switches Overview](#)
CHAPTER 85

Configuration

- Configuration Tasks on page 4485
- Configuration Statements on page 4504

Configuration Tasks

- Configuring an EX4300 Virtual Chassis (CLI Procedure) on page 4485
- Adding a New Switch to an Existing EX4300 Virtual Chassis (CLI Procedure) on page 4490
- Replacing a Member Switch of an EX Series Virtual Chassis Configuration (CLI Procedure) on page 4492
- Configuring Mastership of an EX Series Virtual Chassis (CLI Procedure) on page 4495
- Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure) on page 4497
- Configuring the Timer for the Backup Member to Start Using Its Own MAC Address, as Master of an EX Series Virtual Chassis (CLI Procedure) on page 4501
- Disabling Split and Merge in an EX Series Virtual Chassis (CLI Procedure) on page 4502
- Configuring Automatic Software Update on EX Series Virtual Chassis Member Switches (CLI Procedure) on page 4502
- Assigning the Virtual Chassis ID to Determine Precedence During an EX Series Virtual Chassis Merge (CLI Procedure) on page 4503
- Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504

Configuring an EX4300 Virtual Chassis (CLI Procedure)

In an EX4300 Virtual Chassis, you interconnect the EX4300 switches by using uplink ports configured as Virtual Chassis ports (VCPs). The QSFP+ uplink ports, which support 40Gbps speeds and can connect switches that are up to 492 feet (150 m) apart, are configured as VCPs by default. The SFP+ uplink ports, which support 10Gbps speeds and can connect switches that are up to 6.2 miles (10 km) apart, can be configured into VCPs.

The simplest way to interconnect EX4300 switches into a Virtual Chassis is to install the switches within 492 feet of one another and interconnect them into a Virtual Chassis by using the QSFP+ ports.
If the member switches must be installed in locations that are more than 492 feet apart—such as at a different site or at a distant location within the same site—or if you are using the QSFP+ ports for another purpose, you must configure the SFP+ uplink module ports into VCPs. If you need additional VCP bandwidth between two member switches, you can configure additional ports as VCPs between the member switches. The ports that have identical speeds become links in a link aggregation group (LAG) to provide resiliency to the Virtual Chassis; for instance, if you had two QSFP+ ports and two SFP+ ports configured as VCPs connecting to the same switch, you would have two LAGs—one LAG with two 40Gbps QSFP+ port member links and another with two 10Gbps SFP+ port member links—between the member switches.

NOTE: A Virtual Chassis configuration has two Routing Engines—the master switch and the backup switch. Therefore, we recommend that you always use commit synchronize rather than simply commit to save configuration changes made for a Virtual Chassis. This ensures that the configuration changes are saved on both Routing Engines.

An EX4300 Virtual Chassis can be configured with either:

- A nonprovisioned configuration—The master sequentially assigns a member ID to other member switches. The role is determined by the mastership priority value and other factors in the master election algorithm.
- A preprovisioned configuration—You can deterministically control the member ID and role assigned to a member switch by tying the member switch to its serial number.

NOTE: You must configure a VLAN on all interfaces in an EX4300 Virtual Chassis, with the exception of the interfaces on member switch 0, before the interfaces can send or receive traffic. The interfaces on member switch 0 are initially placed into the default VLAN; the interfaces on all other member switches are not placed into any VLAN. See “Configuring VLANs for EX Series Switches (CLI Procedure)” on page 2119.

NOTE: On an EX4300 Virtual Chassis, STP is disabled on all interfaces except the interfaces on member switch 0 until a type of STP is enabled. See Configuring STP (CLI Procedure) to enable STP on the interfaces in your EX4300 Virtual Chassis.

This topic includes:

- Configuring an EX4300 Virtual Chassis with a Nonprovisioned Configuration File on page 4487
- Configuring an EX4300 Virtual Chassis with a Preprovisioned Configuration File on page 4488
Configuring an EX4300 Virtual Chassis with a Nonprovisioned Configuration File

You can use a nonprovisioned configuration to configure an EX4300 Virtual Chassis.

To configure the Virtual Chassis using a nonprovisioned configuration:

NOTE: We recommend that you physically cable the optical ports as the final step of this procedure.

You can, however, configure an EX4300 Virtual Chassis while the cables are physically connected.

1. Power on only the switch that you will use as the master switch.

2. Run the EZSetup program on the master switch, specifying the identification parameters. See Connecting and Configuring an EX Series Switch (CLI Procedure) for details.

NOTE: The properties that you specify for the master switch apply to the entire Virtual Chassis configuration.

3. (Optional) Configure the master switch with the virtual management Ethernet (VME) interface for out-of-band management of the Virtual Chassis:

   [edit]
   user@switch# set interfaces vme unit 0 family inet address /ip-address/mask/

4. (Optional) Configure mastership priority for the other member switches.

   [edit virtual-chassis]
   user@switch# set member 0 mastership-priority 255
   user@switch# set member 1 mastership-priority 255
   user@switch# set member 2 mastership-priority 10
   user@switch# set member 3 mastership-priority 9
   user@switch# set member 4 mastership-priority 8
   user@switch# set member 5 mastership-priority 7
   user@switch# set member 6 mastership-priority 6
   user@switch# set member 7 mastership-priority 5
   user@switch# set member 8 mastership-priority 4
   user@switch# set member 9 mastership-priority 3

The mastership priority value determines the roles in a non-provisioned Virtual Chassis configuration. The switches with the highest mastership priority values assume the master and backup roles. All other switches assume the linecard role.

If you do not configure the mastership priority for any switch in your Virtual Chassis, including when you do not configure the Virtual Chassis, all switches assume the default mastership priority of 128. The master election algorithm selects the roles for the member switches. In most cases, the switches that have been powered on the longest assume the master and backup roles when all Virtual Chassis member switches are configured with the same mastership priority. See "Understanding How the Master in an EX Series Virtual Chassis Is Elected" on page 4467 for additional information on the master election algorithm.
A switch with a mastership priority of 0 never assumes the master or backup role.

**NOTE:** We recommend that you specify the same mastership priority value for the intended master and backup members.

5. (Optional. Recommended for a two-member Virtual Chassis) On the master switch, disable the split and merge feature:

```
[edit virtual-chassis]
user@switch# set no-split-detection
```

6. Power on the other member switches.

7. On each individual member switch, configure the SFP+ optical ports that will be used to interconnect the EX4300 member switches into VCPs.

**NOTE:** Because QSFP+ ports are configured into VCPs by default, you do not usually have to perform this step when you are using a QSFP+ port as a VCP.

You only need to configure a QSFP+ port as a VCP if you previously configured the QSFP+ port into a network port. If you previously configured the QSFP+ port into a network port, perform this step to configure the QSFP+ port into a VCP.

```
user@switch-0> request virtual-chassis vc-port set pic-slot 1 port 0
user@switch-0> request virtual-chassis vc-port set pic-slot 1 port 1
user@switch-1> request virtual-chassis vc-port set pic-slot 1 port 0
user@switch-1> request virtual-chassis vc-port set pic-slot 1 port 1
user@switch-2> request virtual-chassis vc-port set pic-slot 1 port 0
user@switch-2> request virtual-chassis vc-port set pic-slot 1 port 1
user@switch-3> request virtual-chassis vc-port set pic-slot 1 port 0
user@switch-3> request virtual-chassis vc-port set pic-slot 1 port 1
```

**NOTE:** If you want to change the member ID that the master has assigned to a member switch, use the `request virtual-chassis renumber` command.

### Configuring an EX4300 Virtual Chassis with a Preprovisioned Configuration File

Preprovisioning a Virtual Chassis configuration allows you to assign the member ID and role for each switch in the Virtual Chassis.

To configure a Virtual Chassis using a preprovisioned configuration:

**NOTE:** We recommend that you physically cable the optical ports as the final step of this procedure.

You can, however, configure an EX4300 Virtual Chassis while the cables are physically connected.
1. Make a list of the serial numbers of all the switches to be connected in a Virtual Chassis configuration.

2. Note the intended role (routing-engine or line-card) of each switch. If you configure the member with a routing-engine role, it is eligible to function in the master or backup role. If you configure the member with a line-card role, it is not eligible to function in the master or backup role.

3. Power on only the switch that you plan to use as the master switch.

4. Run the EZSetup program on the master switch, specifying the identification parameters. See Connecting and Configuring an EX Series Switch (CLI Procedure) for details.

   **NOTE:** The properties that you specify for the master switch apply to the entire Virtual Chassis configuration.

5. (Optional) Configure the master switch with the virtual management Ethernet (VME) interface for out-of-band management of the Virtual Chassis:

   ```
   [edit]
   user@switch# set interfaces vme unit 0 family inet address /ip-address/mask/
   ```

6. Specify the preprovisioned configuration mode:

   ```
   [edit virtual-chassis]
   user@switch# set preprovisioned
   ```

7. Specify all the members that you want included in the Virtual Chassis, listing each switch’s serial number with the desired member ID and role.

   **NOTE:** You can retrieve the switch’s serial number using the show chassis hardware command output or by viewing the serial number ID label on the switch. See Locating the Serial Number on an EX4300 Switch or Component.

   ```
   [edit virtual-chassis]
   user@switch# set member 0 serial-number abc123 role routing-engine
   user@switch# set member 1 serial-number def456 role routing-engine
   user@switch# set member 2 serial-number ghi789 role line-card
   user@switch# set member 3 serial-number jkl012 role line-card
   user@switch# set member 4 serial-number mn013 role line-card
   user@switch# set member 5 serial-number pqr014 role line-card
   user@switch# set member 6 serial-number stu015 role line-card
   user@switch# set member 7 serial-number vwx016 role line-card
   user@switch# set member 8 serial-number yzz017 role line-card
   user@switch# set member 9 serial-number aaa018 role line-card
   ```

8. (Optional. Recommended for a two-member Virtual Chassis) Disable the split and merge feature:

   ```
   [edit virtual-chassis]
   user@switch# set no-split-detection
   ```
9. Power on the other member switches. The member IDs and roles have been determined by the configuration, so you can power on the member switches in any order.

10. On each individual member switch, configure the SFP+ optical ports that will be used to interconnect the EX4300 member switches into VCPs.

   **NOTE:** You can also use the `request virtual-chassis vc-port` command to configure a QSFP+ port into a VCP.

   Because QSFP+ ports are configured into VCPs by default, you do not usually have to perform this step when you are using a QSFP+ port as a VCP.

   You only need to configure a QSFP+ port as a VCP if you previously configured the QSFP+ port into a network port. If you previously configured the QSFP+ port into a network port, perform this step to configure the QSFP+ port into a VCP.

   ```
   user@switch-0> request virtual-chassis vc-port set pic-slot1port0
   user@switch-0> request virtual-chassis vc-port set pic-slot1port1
   user@switch-1> request virtual-chassis vc-port set pic-slot1port0
   user@switch-1> request virtual-chassis vc-port set pic-slot1port1
   user@switch-2> request virtual-chassis vc-port set pic-slot1port0
   user@switch-2> request virtual-chassis vc-port set pic-slot1port1
   user@switch-3> request virtual-chassis vc-port set pic-slot1port0
   user@switch-3> request virtual-chassis vc-port set pic-slot1port1
   ```

   **NOTE:** You cannot modify the mastership priority when you are using a pre provisioned configuration. The mastership priority values are generated automatically and controlled by the role that is assigned to the member switch in the configuration file. The two Routing Engines are assigned the same mastership priority value. However, the member that was powered on first has higher prioritization according to the master election algorithm. See “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467.

   Related Documentation

   - Configuring Mastership of an EX Series Virtual Chassis (CLI Procedure) on page 4495
   - Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537

Adding a New Switch to an Existing EX4300 Virtual Chassis (CLI Procedure)

You can use this procedure to add an EX4300 switch to an EX4300 Virtual Chassis.

Before you begin, be sure you have:

- Mounted the new switch in a rack.
- Confirmed that the new switch is powered off.
• If you are expanding a preprovisioned configuration, made a note of the serial number (the number is on the back of the switch). You will need to edit the Virtual Chassis configuration to include the serial number of the new member switch.

• If you are expanding a preprovisioned configuration, edit the existing Virtual Chassis configuration to include the serial number of the new member switch. The parameters specified in the master Virtual Chassis configuration file are applied to the new switch after it has been interconnected to an existing member switch.

NOTE: If you are expanding a preprovisioned Virtual Chassis configuration, you can use the autoprovisioning feature to add member switches to that configuration.

• (Optional) Configured Ethernet interfaces on different member switches into the same LAG. See Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch.

An active member switch might temporarily go down before coming back up as part of this procedure. Having traffic load-balanced across member switches using a LAG helps alleviate traffic loss during this procedure.

To add a new member switch to an existing Virtual Chassis configuration:

1. If the new member switch has been previously configured, revert that switch's configuration to the factory defaults before interconnecting it into the Virtual Chassis. See “Reverting to the Default Factory Configuration for the EX Series Switch” on page 504.

2. Interconnect the unpowered new switch to one member of the existing Virtual Chassis configuration using a QSFP+ or SFP+ port.

   Connect only one VCP on the unpowered new switch to a VCP on a member switch in the existing Virtual Chassis at this point of the procedure.

3. Power on the new switch.

4. (SFP+ interface only) Set the SFP+ interface as a Virtual Chassis Port (VCP):

   ```
   user@switch> request virtual-chassis vc-port set pic-slot1 port port-number
   ```

   NOTE: QSFP+ ports are configured as VCPs, by default. You do not, therefore, typically need to perform this step on QSFP+ ports.

   You can use the `request virtual-chassis vc-port` to set a QSFP+ port as a VCP if the QSFP+ port had previously been configured as a network port.

5. Confirm that the new member switch is now included within the Virtual Chassis configuration by entering the `show virtual-chassis` command. The new member switch should be listed in the output and the Status is Prsnt.

6. Cable the next port into the Virtual Chassis, using Steps 2 through 5.
CAUTION: If you immediately cable both VCPs on the new switch into the existing Virtual Chassis at the same time, a member switch that was already part of the Virtual Chassis might become nonoperational for several seconds. Network traffic to this switch is dropped during the downtime.

The member switch will return to the normal operational state with no user intervention, and normal operation of the Virtual Chassis will resume after this downtime.

Related Documentation
- Configuring an EX4300 Virtual Chassis (CLI Procedure) on page 4485

Replacing a Member Switch of an EX Series Virtual Chassis Configuration (CLI Procedure)

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Adding or Replacing a Member Switch or an External Routing Engine in an EX8200 Virtual Chassis (CLI Procedure) for information about EX8200 Virtual Chassis.

You can replace a member EX2200, EX3300, EX4200, EX4300, EX4500, or EX4550 switch in a Virtual Chassis without disrupting network service on the other members. You can retain the existing configuration of the member switch and apply it to a new member switch, or you can free up the member ID and make it available for assignment to a new member switch.

If you want to replace a member switch of a mixed Virtual Chassis that contains EX4200, EX4500, or EX4550 switches, see Removing an EX4200, EX4500, or EX4550 Switch From a Mixed Virtual Chassis (CLI Procedure).

To replace a member switch, use the procedure that matches what you need to accomplish:

- Remove, Repair, and Reinstall the Same Switch on page 4493
- Remove a Member Switch, Replace It with a Different Switch, and Reapply the Old Configuration on page 4493
- Remove a Member Switch and Make Its Member ID Available for Reassignment to a Different Switch on page 4494
Remove, Repair, and Reinstall the Same Switch

If you need to repair a member switch, you can remove it from the Virtual Chassis configuration without disrupting network service for the other members. The master stores the configuration for the member ID so that it can be reapplied when the member switch (with the same base MAC address) is reconnected.

To remove, repair, and reinstall the member switch:

1. Power off and disconnect the member switch to be repaired.
2. Repair, as necessary.
3. Reconnect the switch and power it on.

Remove a Member Switch, Replace It with a Different Switch, and Reapply the Old Configuration

If you are unable to repair a member switch, you can replace it with a different member switch while retaining the previous configuration. The master stores the configuration of the member that was removed. When you connect a different member switch, the master assigns a new member ID. But the old configuration is still stored under the previous member ID of the previous member switch.

NOTE: If you have used a preprovisioned configuration, you can use the replace command to change the serial number in the Virtual Chassis configuration file. Substitute the serial number of the replacement member switch (on the back of the switch) for the serial number of the member switch that was removed.

To remove and replace a switch and reapply the old configuration:

1. Power off and disconnect the member switch to be replaced.
2. If the replacement member switch has been previously configured, revert that switch’s configuration to the factory defaults. See “Reverting to the Default Factory Configuration for the EX Series Switch” on page 504.
3. If you are interconnecting a switch using a dedicated VCP, connect one VCP on the replacement member switch to a VCP of another Virtual Chassis member switch.

   If you are interconnecting a switch using an optical port configured as a VCP, cable the optical ports together then configure the port on the Virtual Chassis as a VCP:

   ```
   user@switch> request virtual-chassis vc-port set pic-slot1 port port-number
   ```

4. Power on the new member switch.
5. Confirm that the new member switch is now included in the Virtual Chassis configuration by checking the front-panel LCD or the for the member ID. It should display a member ID in the range from 0 through 9.
If you are using a switch that does not have an LCD interface, confirm the switch is part of the Virtual Chassis configuration by entering the `show virtual-chassis` and reviewing the output.

6. Cable the other VCP on the new member switch into the Virtual Chassis. Use the instruction in step 3 to complete this step.

   CAUTION: If you immediately cable both VCPs on the new switch into the existing Virtual Chassis at the same time, a member switch that was already part of the Virtual Chassis might become nonoperational for several seconds. Network traffic to this switch is dropped during the downtime.

   The member switch will return to the normal operational state with no user intervention, and normal operation of the Virtual Chassis will resume after this downtime.

7. On the master switch, issue the `request virtual-chassis renumber` command from the Virtual Chassis master to change the member switch’s current member ID to the member ID of the member switch that was removed from the Virtual Chassis configuration.

Remove a Member Switch and Make Its Member ID Available for Reassignment to a Different Switch

When you remove a member switch from the Virtual Chassis configuration, the master keeps that member switch’s member ID in reserve. To make that member switch’s member ID available for reassignment, issue the `request virtual-chassis recycle` command from the Virtual Chassis master.

   NOTE: When you add or delete members in a Virtual Chassis configuration, internal routing changes might cause temporary traffic loss for a few seconds.

Related Documentation

- Adding or Replacing a Member Switch or an External Routing Engine in an EX8200 Virtual Chassis (CLI Procedure)
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
- Adding a New EX4200 Switch to an Existing EX4200 Virtual Chassis (CLI Procedure)
- Adding an EX4200 Switch to a Preprovisioned EX4500 Virtual Chassis or a Preprovisioned Mixed EX4200 and EX4500 Virtual Chassis (CLI Procedure)
- Adding an EX4500 Switch to a Preprovisioned EX4200 Virtual Chassis (CLI Procedure)
- Adding an EX4500 Switch to a Nonprovisioned EX4200 Virtual Chassis (CLI Procedure)
Configuring Mastership of an EX Series Virtual Chassis (CLI Procedure)

NOTE: This topic applies to all EX Series Virtual Chassis except EX8200 Virtual Chassis. See Configuring an EX8200 Virtual Chassis (CLI Procedure) for information about EX8200 Virtual Chassis.

You can designate the role (master, backup, or linecard) that a member switch performs within any Virtual Chassis, whether or not you are using a preprovisioned configuration.

NOTE: A Virtual Chassis configuration has two Routing Engines—one is the switch in the master role and the other is the switch in the backup role. Therefore, we recommend that you always use commit synchronize rather than commit to save configuration changes made for a Virtual Chassis. This ensures that the configuration changes are saved in both Routing Engines.

This topic describes:

- Configuring Mastership Using a Preprovisioned Configuration File on page 4495
- Configuring Mastership Using a Configuration File That Is Not Preprovisioned on page 4496

Configuring Mastership Using a Preprovisioned Configuration File

To configure mastership using a preprovisioned configuration:

1. Note the serial numbers of the switches that you want to function in the master role and backup role.

2. Power on only the switch that you want to function in the master role.

3. Edit the configuration to specify the preprovisioned configuration mode:

   ```
   [edit virtual-chassis]
   user@switch# set preprovisioned
   ```

4. Specify the serial numbers of the member switches that you want to function as master and backup, specifying their role as routing-engine:

   ```
   [edit]
   user@switch# set virtual-chassis member 0 serial-number abc123 role routing-engine
   user@switch# set virtual-chassis member 1 serial-number def456 role routing-engine
   ```
You cannot directly modify the mastership priority value when you are using a preprovisioned configuration. The mastership priority values are generated automatically and controlled by the role that is assigned to the member switch in the configuration file. The two members assigned the routing-engine role are assigned the same mastership priority value (128). However, the member that was powered on first has higher priority for the master role election according to the master election algorithm. See “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467. Only two members can be configured with the routing-engine role.

5. Specify the serial numbers of any other member switches that you are including in the Virtual Chassis configuration. You can also explicitly configure their role as line-card.

Configuring Mastership Using a Configuration File That Is Not Preprovisioned

To configure mastership of the Virtual Chassis through a configuration that is not preprovisioned:

1. Power on only the switch that you want to function in the master role.

2. Configure the highest possible mastership priority value (255) for the member that you want to function in the master role:

   [edit virtual-chassis]
   user@switch# set member 0 mastership-priority 255

3. Configure the same mastership priority value (continue to edit the Virtual Chassis configuration on the master) for the member that you want to be in the backup role:

   [edit virtual-chassis]
   user@switch# set member 1 mastership-priority 255

   NOTE: We recommend that the master and backup have the same mastership priority value to prevent the master and backup status from switching back and forth between master and backup members in failover conditions.

4. Use the default mastership priority value (128) for the remaining member switches or configure the mastership priority to a value that is lower than the value specified for members functioning in the master and backup roles.

Related Documentation

- Configuring an EX8200 Virtual Chassis (CLI Procedure)
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
- Adding a New EX4200 Switch to an Existing EX4200 Virtual Chassis (CLI Procedure)
- Adding an EX4200 Switch to a Preprovisioned EX4500 Virtual Chassis or a Preprovisioned Mixed EX4200 and EX4500 Virtual Chassis (CLI Procedure)
• Adding an EX4500 Switch to a Preprovisioned EX4200 Virtual Chassis (CLI Procedure)
• Adding an EX4500 Switch to a Nonprovisioned EX4200 Virtual Chassis (CLI Procedure)

Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure)

The procedure described in this topic can be used to connect two EX series switches together within the same Virtual Chassis.

You typically configure an uplink port as a Virtual Chassis Port (VCP) for one of the following reasons:

• You want to interconnect two EX series switches into a Virtual Chassis that are located in different wiring closets or sites, and the switches are farther apart then the maximum length of the dedicated VCP cable.
• You are configuring an EX Series Virtual Chassis composed of switches that support Virtual Chassis but do not have dedicated VCPs. EX2200, EX3300, and EX4300 switches support Virtual Chassis but do not have dedicated VCPs.

You must manually configure VCPs to connect EX2200 switches together to form an EX2200 Virtual Chassis. See Setting a Port on an EX2200 Switch as a Virtual Chassis Port (CLI Procedure).

This procedure is usually not needed to configure an EX3300 Virtual Chassis. Uplink ports 2 and 3 on an EX3300 switch are configured as VCPs by default and, therefore, do not require user configuration to be set as VCPs. We recommend that you use this procedure to configure an uplink port on an EX3300 switch as a VCP only if you configured ports 2 and 3 as network uplink ports and the ports need to be reconfigured as VCPs, or when ports 2 and 3 cannot be used as VCPs for an unexpected reason. You can use this procedure to configure any uplink port on an EX3300 switch as a VCP.

QSFP+ ports on EX4300 switches are configured as VCPs, by default. You must use this procedure if you want to configure an SFP+ port on an EX4300 switch as a VCP, or if you want to configure a QSFP+ port that had been configured into a network port back into a VCP.

You can interconnect EX4200, EX4500, and EX4550 switches that are beyond the reach of the dedicated Virtual Chassis cables as members of a Virtual Chassis by using the uplink ports—including the ports on the SFP uplink module, SFP+ uplink module, or XFP uplink module—and connecting the uplink ports. To use the uplink ports or SFP network ports for interconnecting member switches, you must explicitly set the uplink ports as VCPs.

NOTE: You cannot set a 1000BASE-T copper SFP transceiver (EX-SFP-1GE-T) connection as a VCP on EX4200, EX4500, and EX4550 switches.
NOTE: When an uplink port is set as a VCP, it cannot be used for any other purpose. You can set one port as a VCP and configure the other port in trunk mode as an uplink to another switch.

Before you set an uplink port as a VCP:

1. Install the uplink module in the member switches that you want to interconnect, if you are configuring an uplink module port as a VCP.

2. Power on and connect to the switch that you plan to designate as the master of the Virtual Chassis.

NOTE: Do not power on the other switches at this point.

3. Run EZSetup on the switch that you are configuring to be the master. Follow the prompts to specify the hostname and other identification, time zone, and network properties. See Connecting and Configuring an EX Series Switch (CLI Procedure) for details. The properties that you specify for the master apply to the entire Virtual Chassis, including all the member switches that you later interconnect with the master.

4. If you want to configure and manage the Virtual Chassis remotely, specify the VME global management interface. You can configure the VME global management interface when you are setting up the master or you can do it after completing the other configuration steps for the Virtual Chassis. See Configuring the Virtual Management Ethernet Interface for Global Management of an EX Series Virtual Chassis (CLI Procedure).

5. Configure mastership of the Virtual Chassis by using either the nonprovisioned or preprovisioned configuration. See "Configuring Mastership of an EX Series Virtual Chassis (CLI Procedure)" on page 4495 for details.

NOTE: A Virtual Chassis has two Routing Engines, one in the master and the other in the backup. Therefore, we recommend that you always use commit synchronize rather than simply commit to save configuration changes made for a Virtual Chassis. This ensures that the configuration changes are saved in both Routing Engines.

Before you begin to interconnect a Virtual Chassis across long distances, such as between wiring closets:

- Prepare the existing Virtual Chassis for interconnecting with a potential member switch that is beyond the reach of a dedicated Virtual Chassis cable by setting at least one uplink VCP on an existing member of the Virtual Chassis.

- Prepare the potential member switch for interconnecting with the existing Virtual Chassis by setting at least one uplink VCP on the standalone switch.
NOTE: We recommend that you set two uplink VCPs within each wiring closet for redundancy.

This topic describes:
1. Setting an Uplink VCP Between the Member Switches on page 4499
2. Setting an Uplink VCP on a Standalone Switch on page 4499

Setting an Uplink VCP Between the Member Switches

You can set an uplink port as a VCP.

NOTE: If you use the SFP+ uplink module, you must configure all member switches to support either 1-gigabit SFP transceivers or 10-gigabit SFP+ transceivers on EX4200 switches. See Setting the Mode on an SFP+ or SFP+ MACsec Uplink Module (CLI Procedure).

To set the uplink ports for the local member switch (for example, member 0) and for a different member switch (for example, member 1) to function as VCPs:

1. Set one uplink port of member 0 as a VCP. You do not need to specify the member-member-id option, because the command applies by default on the member where it is executed.
   
   ```
   user@switch> request virtual-chassis vc-port set pic-slot 1 port 0
   ```

2. Set one uplink port of member 1 as a VCP.
   
   ```
   user@switch> request virtual-chassis vc-port set pic-slot 1 port 0 member 1
   ```
   
   This step includes the member-member-id option, because it is executed on a different member switch than the local member switch.

Setting an Uplink VCP on a Standalone Switch

You can set an uplink VCP on a standalone switch. You must set an uplink port on the standalone switch as a VCP prior to physically interconnecting the switch with the existing Virtual Chassis. Otherwise, the master cannot detect that the switch is a member of the Virtual Chassis.

To set one uplink VCP on the potential member, which is currently operating as a standalone switch:

1. Power on the standalone switch.

2. Set one uplink port as a VCP. You do not need to specify the member-member-id option, because the command applies by default on the member where it is executed.
   
   ```
   user@switch> request virtual-chassis vc-port set pic-slot 1 port 0
   ```
NOTE: If you do specify the member member-id option, use member ID 0. Because the switch is not yet interconnected with the other members of the Virtual Chassis, its current member ID is 0. Its member ID will change when it is interconnected with the Virtual Chassis. It does not impact the functioning of the uplink VCP that its VCP is set with 0 as the member ID. The VCP has significance only on the local switch.

3. After you have set the uplink VCP on the standalone switch, physically interconnect its uplink port with the VCP uplink ports of the members in the existing Virtual Chassis. The new member switch reboots and joins the now expanded Virtual Chassis with a different member ID.

NOTE: The setting for the new member switch's uplink VCP remains intact and is not affected by the change of member ID.

4. If you have additional members in the second wiring closet, set a redundant VCP uplink on another member switch by issuing the request virtual-chassis vc-port command.

Related Documentation

- Configuring an EX3300 Virtual Chassis (CLI Procedure)
- Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
- Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)
- Example: Configuring an EX4200 Virtual Chassis Interconnected Across Multiple Wiring Closets
- Example: Configuring an EX4200 Virtual Chassis Using a Preprovisioned Configuration File
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
Configuring the Timer for the Backup Member to Start Using Its Own MAC Address, as Master of an EX Series Virtual Chassis (CLI Procedure)

When a backup member takes control of a Virtual Chassis because of a reset or other temporary failure, the backup member uses the MAC address of the old master switch as the system MAC base address. This process helps ensure a smooth transition of mastership with no disruption to network connectivity.

The MAC persistence timer is used in situations in which the master switch is no longer a member of the Virtual Chassis because it has been physically disconnected or removed. If the old master switch does not rejoin the Virtual Chassis before the timer elapses, the new master switch starts using its own MAC address as the system’s MAC base address. For information regarding how the system MAC base address is used to assign MAC addresses to ports in a Virtual Chassis, see “Understanding MAC Address Assignment on a Virtual Chassis” on page 4482.

The default timer value is 10 minutes. The maximum timer value is 60 minutes.

You can disable the MAC persistence timer starting in Junos OS Release 12.2. When the MAC persistence timer is disabled, the MAC address of the old master switch is used as the system MAC base address; no MAC address changes occur within the Virtual Chassis even when the old master switch is no longer a member of the Virtual Chassis because it has been physically disconnected or removed.

To configure or modify the MAC persistence timer:

```
[edit virtual-chassis]
user@switch# set mac-persistence-timer minutes
```

To disable the MAC persistence timer:

```
[edit virtual-chassis]
user@switch# set mac-persistence-timer disable
```

Related Documentation

- Configuring an EX3300 Virtual Chassis (CLI Procedure)
- Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
- Understanding EX Series Virtual Chassis Components on page 4460
Disabling Split and Merge in an EX Series Virtual Chassis (CLI Procedure)

The split and merge feature is enabled by default on all EX Series switches in a Virtual Chassis. You can disable the split and merge feature. If you disable the split and merge feature and the Virtual Chassis splits, both parts of the split Virtual Chassis configuration remain active.

In a preprovisioned Virtual Chassis, if both of the Routing Engines end up in the same Virtual Chassis configuration after a split, the other part of the split Virtual Chassis configuration remains inactive. If the Routing Engines end up in different parts of the split Virtual Chassis configuration and the rest of the member switches are configured as having linecard roles, then a backup Routing Engine might not be selected for either part.

We recommend disabling split and merge on an EX Series Virtual Chassis with two member switches. A two-member switch Virtual Chassis that has disabled split and merge can reform more quickly and with less complications as a result of the feature being disabled.

To disable the split and merge feature in a Virtual Chassis:

```
[edit]
user@switch# set virtual-chassis no-split-detection
```

Related Documentation

- Example: Assigning the Virtual Chassis ID to Determine Precedence During an EX4200 Virtual Chassis Merge
- Understanding Split and Merge in an EX Series Virtual Chassis on page 4476

Configuring Automatic Software Update on EX Series Virtual Chassis Member Switches (CLI Procedure)

**NOTE:** Automatic software update is not supported on an EX8200 Virtual Chassis.

The automatic software update feature allows you to automatically update the software version on prospective member switches as they are added so that they can join the Virtual Chassis.

**NOTE:** The version of Junos OS running on the Virtual Chassis must be compatible with the software running on the prospective member switch for an automatic software update to occur. For information on Junos OS compatibility and other automatic software update restrictions, see “Understanding Automatic Software Update on EX Series Virtual Chassis Member Switches” on page 4479.

Before you begin, ensure that you know the name or the URL of the software package to be used by the automatic software update feature.
To configure the automatic software update feature:

```
[edit]
user@switch# set virtual-chassis auto-sw-update package-name package-name
```

If the software package is located on a local directory on the switch, use the following format for `package-name`:

```
/pathname/package-name
```

If the software package is to be downloaded and installed from a remote location, use one of the following formats:

```
ftp://hostname/pathname/package-name
ftp://username:prompt@ftp.hostname.net/pathname/package-name
http://hostname/pathname/package-name
```

### Related Documentation
- Example: Configuring Automatic Software Update on EX4200 Virtual Chassis Member Switches
- Understanding Automatic Software Update on EX Series Virtual Chassis Member Switches on page 4479

---

**Assigning the Virtual Chassis ID to Determine Precedence During an EX Series Virtual Chassis Merge (CLI Procedure)**

Every Virtual Chassis has a unique ID that is automatically assigned when the Virtual Chassis configuration is formed. You can also explicitly assign a Virtual Chassis ID using the `set virtual-chassis id` command. When two Virtual Chassis configurations attempt to merge, the Virtual Chassis ID that you assigned takes precedence over the automatically assigned Virtual Chassis IDs and becomes the ID for the newly merged Virtual Chassis configuration.

To configure the Virtual Chassis ID:

```
[edit]
user@switch# set virtual-chassis id id
```

### Related Documentation
- Example: Assigning the Virtual Chassis ID to Determine Precedence During an EX4200 Virtual Chassis Merge
- Understanding Split and Merge in an EX Series Virtual Chassis on page 4476
Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure)

In a Virtual Chassis, one member switch is assigned the master role and has the master Routing Engine. Another member switch is assigned the backup role and has the backup Routing Engine. Graceful Routing Engine switchover (GRES) enables the master and backup Routing Engines in a Virtual Chassis configuration to switch from the master to backup without interruption to packet forwarding. When you configure graceful Routing Engine switchover, the backup Routing Engine automatically synchronizes with the master Routing Engine to preserve kernel state information and the forwarding state.

To set up the Virtual Chassis configuration to use graceful Routing Engine switchover (GRES):

1. Set up a minimum of two switches in a Virtual Chassis configuration with mastership priority of 255:

   ```
   [edit]
   user@switch# set virtual-chassis member 0 mastership-priority 255
   [edit]
   user@switch# set virtual-chassis member 1 mastership-priority 255
   ```

2. Set up graceful Routing Engine switchover:

   ```
   [edit]
   user@switch# set chassis redundancy graceful-switchover
   ```

Commit the configuration.

**NOTE:** We recommend that you use the `commit synchronize` command to save any configuration changes that you make to a multimember Virtual Chassis.

### Related Documentation

- Example: Configuring an EX4200 Virtual Chassis with a Master and Backup in a Single Wiring Closet
- High Availability Features for EX Series Switches Overview
- Understanding EX Series Virtual Chassis Configuration on page 4475

### Configuration Statements

- [edit virtual-chassis] Configuration Statement Hierarchy on EX Series Switches on page 4504

[edit virtual-chassis] Configuration Statement Hierarchy on EX Series Switches

This topic lists supported and unsupported configuration statements in the [edit virtual-chassis] hierarchy level on EX Series switches.

- Supported statements are those that you can use to configure some aspect of a software feature on the switch.
• **Unsupported** statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.

• Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see “EX Series Switch Software Features Overview” on page 27.

This topic lists:

• Supported Statements in the [edit virtual-chassis] Hierarchy Level on page 4505
• Unsupported Statements in the [edit virtual-chassis] Hierarchy Level on page 4505

**Supported Statements in the [edit virtual-chassis] Hierarchy Level**

The following hierarchy shows the *[edit virtual-chassis]* configuration statements supported on EX Series switches:

```plaintext
virtual-chassis {
   auto-sw-update {
      (ex4200 | ex4500)
      package-name package-name;
   }
   fast-failover (ge | vcp disable | xe);
   graceful-restart {
      disable;
   }
   id id;
   mac-persistence-timer [minutes | disable];
   member member-id {
      location location;
      mastership-priority number;
      no-management-vlan;
      role (line-card | routing-engine);
      serial-number;
   }
   no-split-detection;
   preprovisioned;
   traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable> <match regex>;
      flag flag;
   }
   vc-port {
      lag-hash (packet-based | source-port-based);
   }
   vcp-no-hold-time;
}
```

**Unsupported Statements in the [edit virtual-chassis] Hierarchy Level**

All statements in the *[edit virtual-chassis]* hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented.
Related Documentation

- Configuring an EX2200 Virtual Chassis (CLI Procedure)
- Configuring an EX3300 Virtual Chassis (CLI Procedure)
- Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
- Configuring an EX4300 Virtual Chassis (CLI Procedure) on page 4485
- Configuring a Mixed Virtual Chassis with EX4200, EX4500, and EX4550 Member Switches (CLI Procedure)
- Configuring an EX8200 Virtual Chassis (CLI Procedure)
auto-sw-update

Syntax

auto-sw-update {
    (ex4200 | ex4500)
    package-name package-name;
}

Hierarchy Level
[edit virtual-chassis]

Release Information
Statement introduced in Junos OS Release 10.0 for EX Series switches. The ex4200 and ex4500 options introduced in Junos OS Release 12.2 for EX Series switches.

Description
Enable the automatic software update feature for Virtual Chassis configurations.

You should only use the ex4200 and ex4500 keywords when configuring a mixed Virtual Chassis.

You must enter the auto-sw-update statement twice—once to specify the path to a Junos OS package for an EX4200 switch and again to specify the path to Junos OS package for an EX4500 or EX4550 switch—when enabling the automatic software update for a mixed EX4200 and EX4500 Virtual Chassis, mixed EX4200 and EX4550 Virtual Chassis, or mixed EX4200, EX4500, or EX4550 Virtual Chassis.

The Junos OS package for an EX4500 switch updates the software for EX4500 and EX4550 switches. You do not, therefore, need to specify the ex4500 keyword when configuring automatic software update for a mixed EX4500 and EX4550 Virtual Chassis. You also only have to enter the ex4500 keyword once to configure automatic software update for all EX4500 and EX4550 member switches in the same mixed Virtual Chassis.

The remaining statement is explained separately.

Default
The automatic software update feature is disabled.

Options

package-name package-name—Specify a path to a Junos OS software image.

ex4200—Specify a path to a Junos OS image for an EX4200 switch when enabling automatic software update for a mixed EX4200 and EX4500 Virtual Chassis, mixed EX4200 and EX4550 Virtual Chassis, or mixed EX4200, EX4500, or EX4550 Virtual Chassis.

ex4500—Specify a path to a Junos OS image for an EX4500 switch, an EX4550 switch, or both types of switches when enabling automatic software update for a mixed EX4200 and EX4500 Virtual Chassis, mixed EX4200 and EX4550 Virtual Chassis, or mixed EX4200, EX4500, or EX4550 Virtual Chassis.

The Junos OS package for an EX4500 switch updates the software for EX4500 and EX4550 switches. Therefore, you only have to enter this command once to upgrade the EX4500 and EX4550 member switches in the same mixed Virtual Chassis.
The `ex-4500` keyword also does not need to be specified when configuring automatic software update for a mixed EX4500 and EX4550 Virtual Chassis.

**Required Privilege Level**
- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

**Related Documentation**
- *Example: Configuring Automatic Software Update on EX4200 Virtual Chassis Member Switches*
- *Configuring Automatic Software Update on EX Series Virtual Chassis Member Switches (CLI Procedure) on page 4502*
graceful-restart (Enabling Globally)

Syntax

graceful-restart {
  disable;
  helper-disable;
  maximum-helper-recovery-time seconds;
  maximum-helper-restart-time seconds;
  notify-duration seconds;
  recovery-time seconds;
  restart-duration seconds;
  stale-routes-time seconds;
}

Hierarchy Level
[edit logical-systems logical-system-name routing-options],
[edit logical-systems logical-system-name routing-instances routing-instance-name routing-options],
[edit routing-options],
[edit routing-instances routing-instance-name routing-options]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 12.1 for the QFX Series.

Description
Configure graceful restart globally to enable the feature. You cannot enable graceful
restart for specific protocols unless graceful restart is also enabled globally.

For VPNs, the graceful-restart statement allows a router whose VPN control plane is
undergoing a restart to continue to forward traffic while recovering its state from
neighboring routers.

For BGP, if you configure graceful restart after a BGP session has been established, the
BGP session restarts and the peers negotiate graceful restart capabilities.

Default
Graceful restart is disabled by default.

Options
The remaining statements are explained separately.

Required Privilege
Level
routing—to view this statement in the configuration.
routing-control—to add this statement to the configuration.

Related Documentation
- Enabling Graceful Restart
- Configuring Routing Protocols Graceful Restart
- Configuring Graceful Restart for MPLS-Related Protocols
- Configuring VPN Graceful Restart
- Configuring Logical System Graceful Restart
- Graceful Restart Configuration Statements
- Configuring Graceful Restart for QFabric Systems
### graceful-switchover

<table>
<thead>
<tr>
<th>Syntax</th>
<th>graceful-switchover;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hierarchy Level</strong></td>
<td>[edit chassis redundancy]</td>
</tr>
<tr>
<td><strong>Release Information</strong></td>
<td>Statement introduced in Junos OS Release 9.2 for EX Series switches.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>For switches with more than one Routing Engine, including those in a Virtual Chassis, configure the master Routing Engine to switch over gracefully to a backup Routing Engine without interruption to packet forwarding.</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Graceful Routing Engine switchover (GRES) is disabled.</td>
</tr>
<tr>
<td><strong>Required Privilege Level</strong></td>
<td>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</td>
</tr>
</tbody>
</table>
| **Related Documentation** | • Example: Configuring Nonstop Active Routing on EX Series Switches  
• Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504  
• Configuring Nonstop Active Routing on EX Series Switches (CLI Procedure)  
• Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure) |
id

Syntax  

id id;

Hierarchy Level  

[edit virtual-chassis]

Release Information  

Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description  

Configure the alphanumeric string that identifies a Virtual Chassis configuration.

Options  

id—Virtual Chassis ID (VCID), which uses the ISO family address format—for example, 9622.6ac8.5345.

Required Privilege

Level  

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

• Example: Assigning the Virtual Chassis ID to Determine Precedence During an EX4200 Virtual Chassis Merge

• Assigning the Virtual Chassis ID to Determine Precedence During an EX Series Virtual Chassis Merge (CLI Procedure) on page 4503

• Configuring an EX8200 Virtual Chassis (CLI Procedure)

• Understanding Virtual Chassis Member ID Numbering in an EX8200 Virtual Chassis
### location (Virtual Chassis)

<table>
<thead>
<tr>
<th>Syntax</th>
<th>location location;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy Level</td>
<td>[edit virtual-chassis member member-id]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 11.1 for EX Series switches.</td>
</tr>
<tr>
<td>Description</td>
<td>Set a description of the location of the Virtual Chassis member switch or external Routing Engine.</td>
</tr>
</tbody>
</table>

The Location field is visible to users who enter the `show virtual-chassis status detail` command.

Setting this description has no effect on the operation of the Virtual Chassis member.

<table>
<thead>
<tr>
<th>Options</th>
<th>location—Location of the current member switch or external Routing Engine. The location can be any single word.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required Privilege Level</td>
<td>system—To view this statement in the configuration.</td>
</tr>
<tr>
<td></td>
<td>system-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• Example: Configuring an EX4200 Virtual Chassis Using a Preprovisioned Configuration File</td>
</tr>
<tr>
<td></td>
<td>• Example: Configuring a Preprovisioned Mixed EX4200 and EX4500 Virtual Chassis</td>
</tr>
<tr>
<td></td>
<td>• Example: Setting Up a Full Mesh EX8200 Virtual Chassis with Two EX8200 Switches and Redundant XRE200 External Routing Engines</td>
</tr>
<tr>
<td></td>
<td>• Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)</td>
</tr>
<tr>
<td></td>
<td>• Configuring a Mixed Virtual Chassis with EX4200, EX4500, and EX4550 Member Switches (CLI Procedure)</td>
</tr>
<tr>
<td></td>
<td>• Configuring an EX8200 Virtual Chassis (CLI Procedure)</td>
</tr>
</tbody>
</table>
mac-persistence-timer

Syntax  
mac-persistence-timer [minutes | disable];

Hierarchy Level  
[edit virtual-chassis]

Release Information  
Statement introduced in Junos OS Release 9.0 for EX Series switches. 
Option disable introduced in Junos OS Release 12.2 for EX Series switches. 
The maximum timer limit changed from no maximum timer limit to 60 minutes in Junos 
OS Release 12.2 for EX Series switches.

Description  
Specify how long the Virtual Chassis continues to use the MAC address of the switch 
that was originally configured in the master role as the system MAC base address after 
the original master switch is removed from the Virtual Chassis. The system MAC base 
address does not change in the event of a switchover provided the switch originally 
configured in the master role remains a member of the Virtual Chassis.

The maximum timer limit is 60 minutes starting in Junos OS Release 12.2. There are no 
minimum or maximum timer limits in prior Junos OS releases.

Default  
The MAC persistence timer is set to 10 minutes by default.

Options  
minutes—Time in minutes that the member switch in the backup role continues to use 
the system MAC base address of the old master before using its own system MAC 
base address after the switch in the master role is physically disconnected or removed 
from the Virtual Chassis.

disable—Disable the MAC persistence timer. The system MAC base address never changes 
when the MAC persistence timer is disabled, even when the switch in the master 
role is physically disconnected or removed from the Virtual Chassis.

Required Privilege  
Level  
system—to view this statement in the configuration. 
system-control—to add this statement to the configuration.

Related Documentation  
• Configuring the Timer for the Backup Member to Start Using Its Own MAC Address, as 
  Master of an EX Series Virtual Chassis (CLI Procedure) on page 4501
mastership-priority

Syntax
mastership-priority number;

Hierarchy Level
[edit virtual-chassis member member-id]

Release Information
Statement introduced in Junos OS Release 9.0 for EX Series switches. Mastership priority option 0 introduced in Junos OS Release 11.1 for EX Series switches.

Description
The mastership priority value is the most important factor in determining the role of the member switch within the Virtual Chassis configuration. Other factors (see “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467) also affect the election of the master.

The mastership priority value takes the highest precedence in the master election algorithm. The member switch with highest mastership priority becomes the master of the Virtual Chassis configuration. Toggling back and forth between master and backup status in failover conditions is undesirable, so we recommend that you assign the same mastership priority value to both the master and the backup. Secondary factors in the master election algorithm determine which of these two members (that is, the two members that are assigned the highest mastership priority value) functions as the master of the Virtual Chassis configuration.

This statement is not used for the EX8200 Virtual Chassis, which determines mastership by external Routing Engine uptime. See Understanding Virtual Chassis Roles in an EX8200 Virtual Chassis.

A switch with a mastership priority of 0 never takes the master or backup role.

Default
128

Options
number—Mastership priority value.
Range: 0 through 255

Required Privilege Level
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation
• Example: Configuring an EX3300 Virtual Chassis with a Master and Backup
• Example: Configuring an EX4200 Virtual Chassis with a Master and Backup in a Single Wiring Closet
• Example: Configuring an EX4200 Virtual Chassis Interconnected Across Multiple Wiring Closets
• Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
member

Syntax

```plaintext
member member-id {
  location location
  mastership-priority number;
  no-management-vlan;
  serial-number;
  role;
}
```

Hierarchy Level

[edit virtual-chassis]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure a switch or an XRE200 External Routing Engine as a member of a Virtual Chassis.

NOTE: The mastership-priority and no-management-vlan statements are not used in an EX8200 Virtual Chassis.

Default

When an EX3300, EX4200, EX4500, or EX4550 switch is powered on as a standalone switch (not interconnected through its Virtual Chassis ports (VCPs) with other switches), its default member ID is 0.

There is no default member ID in an EX8200 Virtual Chassis. An EX8200 Virtual Chassis must be preprovisioned, and that process configures the member IDs.

Options

- `member-id`—Identifies a specific member switch of a Virtual Chassis configuration.
  
  **Range:** 0 through 9

  The exact range for a specific Virtual Chassis depends on the number of switches allowed in the Virtual Chassis.

  In an EX8200 Virtual Chassis, member IDs 0 through 7 are reserved for EX8200 member switches and member IDs 8 and 9 are reserved for the master and backup external Routing Engines.

  The remaining statements are explained separately.

Required Privilege Level

- `system`—To view this statement in the configuration.
- `system-control`—To add this statement to the configuration.

Related Documentation

- [Example: Configuring an EX4200 Virtual Chassis Using a Preprovisioned Configuration File](#)
- [Example: Setting Up a Full Mesh EX8200 Virtual Chassis with Two EX8200 Switches and Redundant XRE200 External Routing Engines](#)
- [Configuring an EX3300 Virtual Chassis (CLI Procedure)](#)
### no-management-vlan

**Syntax**
no-management-vlan;

**Hierarchy Level**
[edit virtual-chassis member member-id]

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Remove the specified member's out-of-band management port from the virtual management Ethernet (VME) global management VLAN of the Virtual Chassis configuration.

For a member that is functioning in a linecard role, you can use this configuration to reserve the member's management Ethernet port for local troubleshooting:

```config
virtual-chassis {
    member 2 {
        no-management-vlan;
    }
}
```

You cannot configure the IP address for a local management Ethernet port using the CLI or the J-Web interface. To do this, you need to use the shell `ifconfig` command.

**Required Privilege Level**
system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

**Related Documentation**
- Example: Setting Up a Multimember EX4200 Virtual Chassis Access Switch with a Default Configuration
- Configuring the Virtual Management Ethernet Interface for Global Management of an EX Series Virtual Chassis (CLI Procedure)
- Understanding Global Management of an EX Series Virtual Chassis on page 4469
**no-split-detection**

**Syntax**  
no-split-detection;

**Hierarchy Level**  
[edit virtual-chassis]

**Release Information**  
Statement introduced in Junos OS Release 9.3 for EX Series switches.

**Description**  
Disable the split and merge feature in a Virtual Chassis configuration.

We recommend using this statement to disable the split and merge feature when configuring a two-member EX Series Virtual Chassis. Enabling this statement on a two-member Virtual Chassis ensures that both switches remain in the correct Virtual Chassis roles in the event of a Virtual Chassis split.

**Default**  
The split and merge feature is enabled.

**Required Privilege Level**  
system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**
- Example: Assigning the Virtual Chassis ID to Determine Precedence During an EX4200 Virtual Chassis Merge
- Disabling Split and Merge in an EX Series Virtual Chassis (CLI Procedure) on page 4502
- Assigning the Virtual Chassis ID to Determine Precedence During an EX Series Virtual Chassis Merge (CLI Procedure) on page 4503
- Understanding Split and Merge in an EX Series Virtual Chassis on page 4476
package-name

Syntax  package-name package-name;

Hierarchy Level  [edit virtual-chassis auto-sw-update]

Release Information  Statement introduced in Junos OS Release 10.0 for EX Series switches.

Description  Specify the software package name or location of the software package to be used by the automatic software update feature for Virtual Chassis configurations.

Default  No package name is specified.

Options  package-name—Name of the software package or the URL to the software package to be used.

• If the software package is located on a local directory on the switch, use the following format for package-name:
  /pathname/package-name

• If the software package is to be downloaded and installed from a remote location, use one of the following formats:
  ftp://hostname/pathname/package-name
  ftp://username:prompt@ftp.hostname.net/pathname/package-name
  http://hostname/pathname/package-name

Required Privilege  Level  system—To view this statement in the configuration.
  system-control—To add this statement to the configuration.

Related Documentation  • Example: Configuring Automatic Software Update on EX4200 Virtual Chassis Member Switches
  • Configuring Automatic Software Update on EX Series Virtual Chassis Member Switches (CLI Procedure) on page 4502
## preprovisioned

<table>
<thead>
<tr>
<th>Syntax</th>
<th>preprovisioned:</th>
</tr>
</thead>
</table>

### Hierarchy Level

```
[edit virtual-chassis]
```

### Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

### Description

Enable the preprovisioned configuration mode for a Virtual Chassis configuration.

When the preprovisioned configuration mode is enabled, you cannot use the CLI or the J-Web interface to change the mastership priority or member ID of member switches.

You must use this statement to configure an EX8200 Virtual Chassis. Nonprovisioned configuration of an EX8200 Virtual Chassis is not supported.

### Required Privilege

- **Level**
  - system—To view this statement in the configuration.
  - system-control—To add this statement to the configuration.

### Related Documentation

- **Example: Configuring an EX4200 Virtual Chassis Using a Preprovisioned Configuration File**
- **Example: Setting Up a Full Mesh EX8200 Virtual Chassis with Two EX8200 Switches and Redundant XRE200 External Routing Engines**
- **Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)**
- **Configuring an EX8200 Virtual Chassis (CLI Procedure)**
- **Adding a New EX4200 Switch to an Existing EX4200 Virtual Chassis (CLI Procedure)**
- **Replacing a Member Switch of an EX Series Virtual Chassis Configuration (CLI Procedure) on page 4492**
**redundancy (Graceful Switchover)**

**Syntax**

```
redundancy {
  failover {
    on-disk-failure;
    on-loss-of-keepalives;
  }
  graceful-switchover;
}
```

**Hierarchy Level**

[edit chassis]

**Release Information**

Statement introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Enable redundant Routing Engines on a Virtual Chassis with two or more member switches or on a standalone EX6200 or EX8200 switch with more than one Routing Engine.

The remaining statements are explained separately.

**Default**

Redundancy is enabled for the Routing Engines.

**Required Privilege Level**

- interface—To view this statement in the configuration.
- interface-control—To add this statement to the configuration.

**Related Documentation**

- [graceful-switchover on page 2234](#)
- [Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504](#)
- [Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure)](#)
- [High Availability Features for EX Series Switches Overview](#)
## role

| Syntax                  | role (line-card | routing-engine); |
|-------------------------|-----------------|
| Hierarchy Level         | [edit virtual-chassis preprovisioned member member-id] |

**Release Information**
Statement introduced in Junos OS Release 9.0 for EX Series switches.

**Description**
Specify the roles of the members of the Virtual Chassis in a preprovisioned Virtual Chassis.

### EX Series Virtual Chassis (except EX8200 Virtual Chassis)

Specify the role to be performed by each member switch. Associate the role with the member’s serial number.

When you use a preprovisioned configuration, you cannot modify the mastership priority or member ID of member switches through the user interfaces. The mastership priority value is generated by the software, based on the assigned role:

- A member configured as `routing-engine` is assigned the mastership priority 129.
- A member configured as `line-card` is assigned the mastership priority 0.
- A member listed in the preprovisioned configuration without an explicitly specified role is assigned the mastership priority 128.

The configured role specifications are permanent. If both `routing-engine` members fail, a `line-card` member cannot take over as master of the Virtual Chassis configuration. You must delete the preprovisioned configuration to change the specified roles in a Virtual Chassis.

Explicitly configure two members as `routing-engine` and configure additional switches as members of the preprovisioned Virtual Chassis by specifying only their serial numbers. If you do not explicitly configure the role of the additional members, they function in a linecard role by default. In that case, a member that is functioning in a linecard role can take over mastership if the members functioning as master and backup (`routing-engine` role) both fail.

### EX8200 Virtual Chassis

Specify the role to be performed by each XRE200 External Routing Engine and each EX8200 member switch. Associate the role with the member’s serial number. An EX8200 Virtual Chassis cannot function when both external Routing Engines, which must be configured in the `routing-engine` role, have failed.

**Options**
- `line-card`—Enables the member to be eligible to function only in the linecard role. Any member of the Virtual Chassis configuration other than the master or backup functions in the linecard role and runs only a subset of Junos OS for EX Series switches. A member functioning in the linecard role does not run the control protocols or the chassis management processes.
A Virtual Chassis must have at least three members for one member to function in the linecard role.

In an EX8200 Virtual Chassis configuration, all member switches must be in the linecard role.

- **routing-engine**—Enables the member to function as a master or backup of the Virtual Chassis configuration. The master manages all members of the Virtual Chassis configuration and runs the chassis management processes and control protocols. The backup synchronizes with the master in terms of protocol states, forwarding tables, and so forth, so that it is prepared to preserve routing information and maintain network connectivity without disruption in case the master is unavailable.

(All Virtual Chassis composed of EX2200, EX3300, EX4200, EX4500, or EX4550 switches) Specify two and only two members as **routing-engine**. The software determines which of the two members assigned the **routing-engine** role functions as master, based on the master election algorithm. See “Understanding How the Master in an EX Series Virtual Chassis Is Elected” on page 4467. In these Virtual Chassis, the **routing-engine** role is associated with a switch.

(Ex8200 Virtual Chassis) All XRE200 External Routing Engines must be in the **routing-engine** role.

### Required Privilege

- **system**—To view this statement in the configuration.
- **system-control**—To add this statement to the configuration.

### Related Documentation

- **Example: Configuring an EX4200 Virtual Chassis Using a Preprovisioned Configuration File**
- **Example: Setting Up a Full Mesh EX8200 Virtual Chassis with Two EX8200 Switches and Redundant XRE200 External Routing Engines**
- **Configuring an EX3300 Virtual Chassis (CLI Procedure)**
- **Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)**
- **Configuring an EX8200 Virtual Chassis (CLI Procedure)**
- **Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)**
- **Adding a New EX4200 Switch to an Existing EX4200 Virtual Chassis (CLI Procedure)**
- **Replacing a Member Switch of an EX Series Virtual Chassis Configuration (CLI Procedure) on page 4492**
serial-number

Syntax

serial-number serial-number;

Hierarchy Level

[edit virtual-chassis preprovisioned member member-id]

Release Information

Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

In a preprovisioned Virtual Chassis composed of EX2200, EX3300, EX4200, EX4300, EX4500, or EX4550 switches, specify the serial number of each member switch to be included in the Virtual Chassis configuration. If you do not include the serial number within the Virtual Chassis configuration, the switch cannot be recognized as a member of a preprovisioned configuration.

In an EX8200 Virtual Chassis configuration, specify the serial number of each XRE200 External Routing Engine and each EX8200 member switch to be included in the Virtual Chassis configuration. If you do not include the serial number within the Virtual Chassis configuration, the external Routing Engine or switch cannot be recognized as a member of the configuration.

Options

serial-number—Permanent serial number for the external Routing Engine or for the member switch.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation

• Configuring an EX2200 Virtual Chassis (CLI Procedure)
• Configuring an EX3300 Virtual Chassis (CLI Procedure)
• Configuring an EX4300 Virtual Chassis (CLI Procedure) on page 4485
• Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
• Configuring an EX8200 Virtual Chassis (CLI Procedure)
• Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)
traceoptions (Virtual Chassis)

Syntax

```
traceoptions {
  file filename <files number> <no-stamp> <replace> <size size> <world-readable | no-world-readable>;
  flag flag <detail> <disable> <receive> <send>;
}
```

Hierarchy Level
[edit virtual-chassis]

Release Information

Description
Define tracing operations for the Virtual Chassis configuration.

Default
Tracing operations are disabled.

Options
detail—(Optional) Generate detailed trace information for a flag.
disable—(Optional) Disable a flag.

file filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.

files number—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the size option.

Range: 2 through 1000
Default: 3 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:

- all—All tracing operations.
- auto-configuration—Trace Virtual Chassis ports (VCPs) that have been automatically configured.
- csn—Trace Virtual Chassis complete sequence number (CSN) packets.
- error—Trace Virtual Chassis errored packets.
- hello—Trace Virtual Chassis hello packets.
- krt—Trace Virtual Chassis KRT events.

TIP: The all flag displays a subset of logs that are useful in debugging most issues. For more detailed information, use all detail.
- **lsp**—Trace Virtual Chassis link-state packets.
- **lsp-generation**—Trace Virtual Chassis link-state packet generation.
- **me**—Trace Virtual Chassis ME events.
- **normal**—Trace normal events.
- **packets**—Trace Virtual Chassis packets.
- **parse**—Trace reading of the configuration.
- **psn**—Trace partial sequence number (PSN) packets.
- **route**—Trace Virtual Chassis routing information.
- **spf**—Trace Virtual Chassis SPF events.
- **state**—Trace Virtual Chassis state transitions.
- **task**—Trace Virtual Chassis task operations.

**no-stamp**—(Optional) Do not place a timestamp on any trace file.

**no-world-readable**—(Optional) Restrict file access to the user who created the file.

**receive**—(Optional) Trace received packets.

**replace**—(Optional) Replace a trace file rather than appending information to it.

**send**—(Optional) Trace transmitted packets.

**size size**—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named `trace-file` reaches its maximum size, it is renamed `trace-file.0`, then `trace-file.1`, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum number of files, you also must specify a maximum file size with the `files` option.

**Syntax:** `xk` to specify KB, `xm` to specify MB, or `xg` to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege Level**
- system—To view this statement in the configuration.
- system-control—To add this statement to the configuration.

**Related Documentation**
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
- Verifying the Member ID, Role, and Neighbor Member Connections of an EX Series Virtual Chassis Member on page 4534
- Verifying That Virtual Chassis Ports on an EX Series Switch Are Operational on page 4535
- Verifying Virtual Chassis Ports in an EX8200 Virtual Chassis
- Troubleshooting an EX Series Virtual Chassis on page 4605
### vcp-no-hold-time

**Syntax**  
`vcp-no-hold-time;`

**Hierarchy Level**  
`[edit virtual-chassis]`

**Release Information**  
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**  
Disable the Virtual Chassis port (VCP) holddown timer for all VCPs in the Virtual Chassis.

The VCP holddown timer is an internal mechanism that delays a Virtual Chassis reconvergence for several seconds when a VCP becomes inactive. The purpose of this delay is to provide the VCP time to return online without having to reconverge the Virtual Chassis to adjust to the inactive VCP. All traffic to the VCP is dropped while the VCP is inactive. If the VCP remains down for a time that exceeds the VCP holddown timer, a Virtual Chassis reconvergence occurs.

When this statement is enabled, the VCP holddown timer is disabled and the Virtual Chassis reconvergence occurs when a VCP becomes inactive. The period of time where traffic is dropped waiting for the VCP to return online is avoided.

We recommend enabling this statement after a Virtual Chassis is operational. We recommend disabling this statement when you are adding or removing member switches from your Virtual Chassis.

The VCP holddown timer cannot be viewed and is not user-configurable. You can only control whether the VCP holddown timer is enabled or disabled by configuring this statement.

**Default**  
The VCP holddown timer is enabled by default on all EX series switches that support this statement. The VCP holddown timer is not configurable on all EX series switches that do not support this statement.

**Required Privilege Level**  
- system—to view this statement in the configuration.
- system-control—to add this statement to the configuration.

**Related Documentation**  
- Understanding EX4300 Virtual Chassis on page 4459
- Understanding EX Series Virtual Chassis Components on page 4460
virtual-chassis

Syntax

virtual-chassis {
  auto-sw-update {
    (ex4200 | ex4500)
    package-name package-name;
  }
  fast-failover (ge | vcp disable | xe);
  graceful-restart {
    disable;
  }
  id id;
  mac-persistence-timer [minutes | disable];
  member member-id {
    location location;
    mastership-priority number;
    no-management-vlan;
    serial-number;
    role;
  }
  no-split-detection;
  preprovisioned;
  traceoptions (Virtual Chassis) {
    file filename <files number> <size size> <world-readable | no-world-readable> <match regex>;
    flag flag ;
  }
  vc-port {
    lag-hash (packet-based | source-port-based);
  }
  vcp-no-hold-time;
}

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure Virtual Chassis information.

The remaining statements are explained separately.

Default A standalone EX2200, EX3300, EX4200, EX4500, or EX4550 switch is a Virtual Chassis by default. It has a default member ID of 0, a default mastership priority of 128, and a default role as master.

A standalone XRE200 External Routing Engine or EX8200 switch is not part of an EX8200 Virtual Chassis until a Virtual Chassis configuration is set up.

Required Privilege Level system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Documentation • Example: Configuring an EX3300 Virtual Chassis with a Master and Backup
• Example: Configuring an EX4200 Virtual Chassis with a Master and Backup in a Single Wiring Closet
• Example: Setting Up a Full Mesh EX8200 Virtual Chassis with Two EX8200 Switches and Redundant XRE200 External Routing Engines
• Configuring an EX3300 Virtual Chassis (CLI Procedure)
• Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
• Configuring an EX8200 Virtual Chassis (CLI Procedure)
CHAPTER 86

Administration

• Routine Monitoring on page 4529
• Operational Commands on page 4540

Routine Monitoring

• Command Forwarding Usage with an EX Series Virtual Chassis on page 4529
• Verifying the Member ID, Role, and Neighbor Member Connections of an EX Series Virtual Chassis Member on page 4534
• Verifying That Virtual Chassis Ports on an EX Series Switch Are Operational on page 4535
• Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
• Verifying That Graceful Routing Engine Switchover Is Working in the Virtual Chassis on page 4538

Command Forwarding Usage with an EX Series Virtual Chassis

Some CLI commands can be run either on all members or on a specific member of a Virtual Chassis configuration. This functionality is referred to as command forwarding.

You can always specify that these commands be applied to all member switches in the Virtual Chassis by using the all-members option, or to a specific member switch by using the member-member-id option. If neither option is specified, the default command forwarding behavior, which varies by command, is used. See the Default row in Table 558 on page 4530 to learn the command forwarding behavior for a specific command.

For example, to collect information about a particular member switch prior to contacting Juniper Networks Technical Assistance Center (JTAC), use the request support information member member-id command to gather data for the specified member switch. If you want to gather this data for all member switches in the Virtual Chassis, you can enter the request support information command, which by default uses the all-members option, or the request support information all-members command.

Table 558 on page 4530 provides a list of commands that can be run either on all members of the Virtual Chassis configuration or on a specific member switch.
### Table 558: Commands That Can be Run on All or Specific Members of the Virtual Chassis Configuration

<table>
<thead>
<tr>
<th>Commands Available for Command Forwarding</th>
<th>Purpose</th>
<th>all-members</th>
<th>member-member-id</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>request support information</td>
<td>Displays information for the specified member switch.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td></td>
<td>all-members</td>
</tr>
</tbody>
</table>

- **forwarding-available** commands:
  - **request support information**:
    - **Purpose**: Use this command when you contact JTAC about your component problem. This command is the equivalent of using the following CLI commands:
      - `show version`
      - `show chassis firmware`
      - `show chassis hardware`
      - `show chassis environment`
      - `show interfaces extensive` (for each configured interface)
      - `show configuration` (excluding any SECRET-DATA)
      - `show system virtual-memory`
  - **request system partition hard-disk**:
    - **Purpose**: Set up the hard disk for partitioning. After this command is issued, the hard disk is partitioned the next time the system is rebooted. When the hard disk is partitioned, the contents of /altroot and /altconfig are saved and restored. All other data on the hard disk is at risk of being lost.
  - **request system reboot**:
    - **Purpose**: Reboots Junos OS for EX Series switches after a software upgrade and occasionally to recover from an error condition.
      - Reboots all members of the Virtual Chassis configuration.
      - Reboots the specified member switch.
      - all-members
Table 558: Commands That Can be Run on All or Specific Members of the Virtual Chassis Configuration (continued)

<table>
<thead>
<tr>
<th>Commands Available for Command Forwarding</th>
<th>Purpose</th>
<th>all-members</th>
<th>member-member-id</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>request system snapshot</td>
<td>Back up the currently running and active file system.</td>
<td>Backs up the file systems on all members of the Virtual Chassis configuration.</td>
<td>Backs up the file system on the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>request system storage cleanup</td>
<td>Free storage space on the switch by rotating log files and proposing a list of files for deletion. User input is required for file deletion.</td>
<td>Runs cleanup on all members of the Virtual Chassis configuration.</td>
<td>Runs cleanup on the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show log user</td>
<td>Display users who are viewing the system log.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>master switch only</td>
</tr>
<tr>
<td>show system alarms</td>
<td>Display active system alarms.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system audit</td>
<td>Display the state and checksum values for file systems.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system boot-messages</td>
<td>Display initial messages generated by the system kernel upon startup. These messages are the contents of /var/run/dmesg.boot.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
</tbody>
</table>
### Table 558: Commands That Can be Run on All or Specific Members of the Virtual Chassis Configuration (continued)

<table>
<thead>
<tr>
<th>Commands Available for Command Forwarding</th>
<th>Purpose</th>
<th>all-members</th>
<th>member-member-id</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show system buffers</strong></td>
<td>Display information about the buffer pool that the Routing Engine uses for local traffic. Local traffic is the routing and management traffic that is exchanged between the Routing Engine and the Packet Forwarding Engine within the switch, as well as the routing and management traffic from IP (that is, from OSPF, BGP, SNMP, ping operations, and so on).</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td><strong>show system connections</strong></td>
<td>Display information about the active IP sockets on the Routing Engine. Use this command to verify which servers are active on a system and which connections are currently in progress.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td><strong>show system core-dumps</strong></td>
<td>Display a core file generated by an internal Junos OS process.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td><strong>show system directory-usage</strong></td>
<td>Display directory usage information.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>master switch only</td>
</tr>
<tr>
<td><strong>show system processes</strong></td>
<td>Display information about software processes that are running on the switch and that have controlling terminals.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td></td>
<td>all-members</td>
</tr>
</tbody>
</table>
### Table 558: Commands That Can be Run on All or Specific Members of the Virtual Chassis Configuration (continued)

<table>
<thead>
<tr>
<th>Commands Available for Command Forwarding</th>
<th>Purpose</th>
<th>all-members</th>
<th>member-member-id</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>show system reboot all-members</td>
<td>Display pending system reboots or halts.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system snapshot all-members</td>
<td>Display information about the backup software that is located in the /altroot and /altconfig file systems. To back up software, use the request system snapshot command.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system software all-members</td>
<td>Display the Junos OS extensions loaded on your switch.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system statistics all-members</td>
<td>Display systemwide protocol-related statistics.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system storage all-members</td>
<td>Display statistics about the amount of free disk space in the switch’s file systems.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system uptime all-members</td>
<td>Display the current time and information about how long the switch, the switch software, and any existing protocols have been running</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
<tr>
<td>show system users all-members</td>
<td>Show all users who are currently logged in.</td>
<td>Shows all users who are currently logged in to any members of the Virtual Chassis configuration.</td>
<td>Shows all users who are currently logged in to the specified member switch.</td>
<td>all-members</td>
</tr>
</tbody>
</table>
Table 558: Commands That Can be Run on All or Specific Members of the Virtual Chassis Configuration (continued)

<table>
<thead>
<tr>
<th>Commands Available for Command Forwarding</th>
<th>Purpose</th>
<th>all-members</th>
<th>member-member-id</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>show system virtual-memory</td>
<td>Displays the usage of Junos OS kernel memory, listed first by size of allocation and then by type of usage. Use show system virtual-memory for troubleshooting with JTAC.</td>
<td>Displays information for all members of the Virtual Chassis configuration.</td>
<td>Displays information for the specified member switch.</td>
<td>all-members</td>
</tr>
</tbody>
</table>

Related Documentation

- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
- Understanding EX Series Virtual Chassis Components on page 4460
- Junos OS System Basics and Services Command Reference

Verifying the Member ID, Role, and Neighbor Member Connections of an EX Series Virtual Chassis Member

**Purpose**
You can designate the role that a member performs within a Virtual Chassis or you can allow the role to be assigned by default. You can designate the member ID that is assigned to a specific switch by creating a permanent association between the switch's serial number and a member ID, using a preprovisioned configuration. Or you can let the member ID be assigned by the master, based on the sequence in which the member switch is powered on and on which member IDs are currently available.

The role and member ID of the member switch are displayed on the front-panel LCD.

Each member switch can be cabled to one or two other member switches, using either the dedicated Virtual Chassis ports (VCPs) on the rear panel, an uplink port that has been configured as a VCP, or an optical port that has been configured as a VCP. The members that are cabled together are considered neighbor members.

**Action**
To display the role and member ID assignments using the CLI:

```
user@switch> show virtual-chassis
```

Virtual Chassis ID: 0000.e255.00e0

<table>
<thead>
<tr>
<th>Member ID</th>
<th>Status</th>
<th>Serial No</th>
<th>Model</th>
<th>Mastership Priority</th>
<th>Role</th>
<th>Neighbor List ID, Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (FPC 0)</td>
<td>Prsnt</td>
<td>abc123</td>
<td>ex4200-48p</td>
<td>255 Master*</td>
<td></td>
<td>1 vcp-0 2 vcp-1</td>
</tr>
<tr>
<td>1 (FPC 1)</td>
<td>Prsnt</td>
<td>def456</td>
<td>ex4200-24t</td>
<td>255 Backup</td>
<td></td>
<td>2 vcp-0</td>
</tr>
</tbody>
</table>
### Meaning
This output verifies that three EX4200 switches have been interconnected as a Virtual Chassis configuration through their dedicated VCPs to create an EX4200 Virtual Chassis. The display shows which of the VCPs is connected to which neighbor. The first port (vcp-0) of member 0 is connected to member 1 and the second port of member 0 (vcp-1) is connected to member 2. The FPC slots for the switches are the same as the member IDs.

The Mastership Priority values indicate that the master and backup members have been explicitly configured, because they are not using the default value (128).

### Related Documentation
- Configuring Mastership of an EX Series Virtual Chassis (CLI Procedure) on page 4495
- Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
- Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)
- Configuring a Mixed Virtual Chassis with EX4200, EX4500, and EX4550 Member Switches (CLI Procedure)
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537

### Verifying That Virtual Chassis Ports on an EX Series Switch Are Operational

**Purpose**
Display the status of Virtual Chassis ports (VCPs) in a Virtual Chassis.

**Action**
Display the VCPs:

```
user@switch> show virtual-chassis vc-port all-members
```

```plaintext
fpc0:
--- Interface or PIC / Port Type  Trunk Status  Speed (mbps)  Neighbor ID Interface
  vcp-0  Dedicated  1  Up  32000  1  vcp-0
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Up</td>
<td>32000</td>
<td>0</td>
<td>vcp-0</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Up</td>
<td>32000</td>
<td>0</td>
<td>vcp-1</td>
</tr>
<tr>
<td>1/0</td>
<td>Configured</td>
<td>3</td>
<td>Up</td>
<td>10000</td>
<td>3</td>
<td>vcp-255/1/0</td>
</tr>
<tr>
<td>1/1</td>
<td>Configured</td>
<td>3</td>
<td>Up</td>
<td>10000</td>
<td>3</td>
<td>vcp-255/1/1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Up</td>
<td>32000</td>
<td>3</td>
<td>vcp-0</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Up</td>
<td>32000</td>
<td>3</td>
<td>vcp-1</td>
</tr>
<tr>
<td>1/0</td>
<td>Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-255/1/0</td>
</tr>
<tr>
<td>1/1</td>
<td>Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-255/1/1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Down</td>
<td>1000</td>
<td>2</td>
<td>vcp-0</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Down</td>
<td>1000</td>
<td>2</td>
<td>vcp-1</td>
</tr>
<tr>
<td>1/0</td>
<td>Configured</td>
<td>3</td>
<td>Up</td>
<td>10000</td>
<td>1</td>
<td>vcp-255/1/0</td>
</tr>
<tr>
<td>1/1</td>
<td>Configured</td>
<td>3</td>
<td>Up</td>
<td>10000</td>
<td>1</td>
<td>vcp-255/1/1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Down</td>
<td>32000</td>
<td>0</td>
<td>vcp-255/1/2</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Down</td>
<td>32000</td>
<td>0</td>
<td>vcp-255/1/3</td>
</tr>
</tbody>
</table>

Meaning

The dedicated VCPs are displayed as vcp-0 and vcp-1. The uplink interfaces that have been set as uplink VCPs are displayed as 1/0, 1/1, 1/2, and 1/3. The network interfaces that have been set as VCPs are displayed as 0/20 and 0/21. The neighbor interface names of uplink and network VCPs are of the form vcp-255/pic/port—for example, vcp-255/1/0. In that name, vcp-255 indicates that the interface is a VCP, 1 is the uplink PIC number, and 0 is the port number. The fpc number is the same as the member ID. The trunk ID is a positive number ID assigned to the link aggregation group (LAG) formed by the Virtual Chassis. If no LAG is formed, the value is –1.
NOTE: This example uses output from an EX4200 Virtual Chassis. The output would be identical on all other types of Virtual Chassis.

Related Documentation

- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
  - Configuring an EX3300 Virtual Chassis (CLI Procedure)
  - Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
  - Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)
  - Configuring a Mixed Virtual Chassis with EX4200, EX4500, and EX4550 Member Switches (CLI Procedure)

Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis

Purpose

Use the monitoring functionality to view the following information about the switches and the ports on EX2200, EX3300, EX4200, EX4300, EX4500, EX4550, and EX8200 switches that are members of a Virtual Chassis:

- Member details and how members are connected with each other
- Traffic statistics for Virtual Chassis ports (VCPs) of the selected members
- Details of the VCP packet counters

Action

To view Virtual Chassis monitoring details in the J-Web interface for a Virtual Chassis, select Monitor > Virtual Chassis.

NOTE: Virtual Chassis monitoring is supported on J-Web, on all Virtual Chassis platforms except EX3200 and EX6210.

To view member details for all members in the CLI, enter the following command:

```
user@switch> show virtual-chassis
```

To view VCP traffic statistics for a specific member in the CLI, enter the following command:

```
user@switch> show virtual-chassis vc-port statistics member member-id
```

To view the path a packet takes when going from a source interface to a destination interface in a Virtual Chassis configuration using the CLI, enter the following command:

```
user@switch> show virtual-chassis vc-path
```

Meaning

In the J-Web interface, the top half of the screen displays details of the Virtual Chassis configuration, such as:
Click the **Stop** button to stop fetching values from the switch, and click the **Start** button to start plotting data again from the point where it was stopped.

To view a graph of the statistics for the selected VCP of the member, click **Show Graph**.

**Refresh Interval (sec)**—Displays the time interval you have set for page refresh.

Click **Clear Statistics** to clear the monitoring statistics for the selected member switch.

You can specify the interval at which the member details and statistics must be refreshed.

The bottom half of the screen displays a chart of the Virtual Chassis statistics and the port packet counters.

For details about the output from CLI commands, see the `show virtual-chassis` and `show virtual-chassis vc-port statistics` command summaries.

### Related Documentation

- Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
- Configuring an EX8200 Virtual Chassis (CLI Procedure)
- Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)
- Configuring a Mixed Virtual Chassis with EX4200, EX4500, and EX4550 Member Switches (CLI Procedure)
- Verifying the Member ID, Role, and Neighbor Member Connections of an EX Series Virtual Chassis Member on page 4534

### Verifying That Graceful Routing Engine Switchover Is Working in the Virtual Chassis

**Purpose**

Verify that a Graceful Routing Engine switchover (GRES) between two member switches acting as the master and backup routing engines in a Virtual Chassis has occurred.

**Action**

On the master switch, verify the member ID of the backup Routing Engine:

```shell
{master:0}
user@switch> show virtual-chassis
Virtual Chassis ID: 5efa.4b7a.aae6
Mastership Neighbor List
Member ID Status Serial No Model priority Role ID  Interface
0 (FPC 0) Prsnt BM0208105281 ex4200-24t 255 Master* 1 vcp-0
```
1 (FPC 1) Prsnt BP0208192350 ex4200-48t 255 Backup 0 vcp-0

Member ID for next new member: 2 (FPC 2)

1. Connect to the backup Routing Engine:

   {master:0}
   user@switch> request session member 1

   {backup:1}
   user@switch>

2. Verify that the backup Routing Engine is ready for switchover on member ID 1:

   {backup:1}
   user@switch> show system switchover

   Graceful switchover: On
   Configuration database: Ready
   Kernel database: Ready
   Peer state: Steady State

3. Switch the current backup Routing Engine to master Routing Engine:

   NOTE: You must wait a minimum of two minutes between Routing Engine failovers for the Routing Engines to synchronize.

   {backup:1}
   user@switch> request chassis routing-engine master acquire

4. Verify that the master and backup Routing Engines have switched roles:

   NOTE: Member ID 1 is now the master and member ID 0 is now the backup.

   {master:1}
   user@switch> show virtual-chassis

   Virtual Chassis ID: 5efa.4b7a.aee6
   Mastership         Neighbor List
   Member ID  Status  Serial No Model  priority  Role  ID  Interface
   0 (FPC 0)  Prsnt  BM0208105281 ex4200-24t 255  Backup 1  vcp-0
   1 (FPC 1)  Prsnt  BP0208192350 ex4200-48t 255  Master* 0  vcp-0

Member ID for next new member: 2 (FPC 2)

Meaning: With graceful Routing Engine switchover enabled, when you initiated a switchover from the backup Routing Engine, the backup Routing Engine became the master and the master Routing Engine became the backup.
Related Documentation

• Configuring Graceful Routing Engine Switchover in a Virtual Chassis (CLI Procedure) on page 4504

Operational Commands
**clear virtual-chassis vc-port statistics**

**Syntax**
clear virtual-chassis vc-port statistics
<all-members>
</interface-name>
<local>
<member member-id>

**Release Information**
Command introduced in Junos OS Release 9.0 for EX Series switches. The options all-members and local were added in Junos OS Release 9.3 for EX Series switches.

**Description**
Clear—reset to zero (0)—the traffic statistics counters on Virtual Chassis ports (VCPs).

**Options**
none—Clear traffic statistics for VCPs of all members of a Virtual Chassis configuration.

all-members—(Optional) Clear traffic statistics for VCPs of all members of a Virtual Chassis configuration.

interface-name—(Optional) Clear traffic statistics for the specified VCP.

local—(Optional) Clear traffic statistics for VCPs from the switch or external Routing Engine on which this command is entered.

member member-id—(Optional) Clear traffic statistics for VCPs from the specified member of a Virtual Chassis configuration.

**Required Privilege**
clear

**Level**

**Related Documentation**
- show virtual-chassis vc-port statistics on page 4597
- show virtual-chassis vc-port on page 4579
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537

**List of Sample Output**
clear virtual-chassis vc-port statistics (EX4200 Virtual Chassis) on page 4541
clear virtual-chassis vc-port statistics (EX8200 Virtual Chassis) on page 4541
clear virtual-chassis vc-port statistics member 3 on page 4542

**Sample Output**
clear virtual-chassis vc-port statistics (EX4200 Virtual Chassis)

```
user@switch> clear virtual-chassis vc-port statistics
fpc0:
----------------------------------------------------------------------------
Statistics cleared
```

clear virtual-chassis vc-port statistics (EX8200 Virtual Chassis)

```
user@external-routing-engine> clear virtual-chassis vc-port statistics
```
Statistics cleared

Statistics cleared

Statistics cleared

Statistics cleared

Statistics cleared

clear virtual-chassis vc-port statistics member 3

user@switch> clear virtual-chassis vc-port statistics member 3
Cleared statistics on member 3
request session member

Syntax  
request session member member-id

Release Information  Command introduced in Junos OS Release 9.0 for EX Series switches.

Description  Start a session with the specified member of a Virtual Chassis configuration.

Options  
member-id—Member ID for the specific member of the Virtual Chassis configuration.

Required Privilege  maintenance

Related Documentation  
- member on page 4515
- Understanding EX Series Virtual Chassis Components on page 4460
**request virtual-chassis recycle**

**Syntax**

request virtual-chassis recycle member-id member-id

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Make a previously used member ID available for reassignment.

When you remove a member switch from the Virtual Chassis configuration, the master reserves that member ID. To make the member ID available for reassignment, you must use this command.

**NOTE:** You must run this command from the Virtual Chassis member in the master role.

**Options**

- **member-id member-id**—Specify the member ID that you want to make available for reassignment to a different member.

**Required Privilege Level**

system-control

**Related Documentation**

- request virtual-chassis renumber on page 4545
- Replacing a Member Switch of an EX Series Virtual Chassis Configuration (CLI Procedure) on page 4492
- Adding or Replacing a Member Switch or an External Routing Engine in an EX8200 Virtual Chassis (CLI Procedure)

**List of Sample Output**

- request virtual-chassis recycle member-id 3 on page 4544
- request virtual-chassis recycle member-id 1 on page 4544

**Sample Output**

request virtual-chassis recycle member-id 3

user@switch> request virtual-chassis recycle member-id 3

Sample Output

request virtual-chassis recycle member-id 1

user@external-routing-engine> request virtual-chassis recycle member-id 1
**request virtual-chassis renumber**

**Syntax**

```
request virtual-chassis renumber member-id old-member-id new-member-id new-member-id
```

**Release Information**

Command introduced in Junos OS Release 9.0 for EX Series switches.

**Description**

Renumber a member of a Virtual Chassis configuration.

**NOTE:** You must run this command from the Virtual Chassis member in the master role.

**Options**

- `member-id old-member-id`—Specify the ID of the member that you wish to renumber.
- `new-member-id new-member-id`—Specify an unassigned member ID.

**Required Privilege Level**

system-control

**Related Documentation**

- request virtual-chassis recycle on page 4544
- Replacing a Member Switch of an EX Series Virtual Chassis Configuration (CLI Procedure) on page 4492
- Adding or Replacing a Member Switch or an External Routing Engine in an EX8200 Virtual Chassis (CLI Procedure)

**List of Sample Output**

request virtual-chassis renumber member-id 5 new-member-id 4 on page 4545
request virtual-chassis renumber member-id 1 new-member-id 0 on page 4545

**Sample Output**

request virtual-chassis renumber member-id 5 new-member-id 4

```
user@switch> request virtual-chassis renumber member-id 5 new-member-id 4
```

request virtual-chassis renumber member-id 1 new-member-id 0

```
user@external-routing-engine> request virtual-chassis renumber member-id 1 new-member-id 0
```
request virtual-chassis vc-port

Syntax

request virtual-chassis vc-port set | delete <fpc-slot fpc-slot> pic-slot pic-slot port port-number <member member-id>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches. 
Option fpc-slot introduced in Junos OS Release 10.4 for EX Series switches.

Description

Enable or disable an uplink port (on an SFP, SFP+, or XFP uplink interface) or an SFP network port as a Virtual Chassis port (VCP).

If you omit member member-id, this command defaults to enabling or disabling the uplink VCP or SFP network port configured as a VCP on the switch where the command is issued.

On an EX3300 switch, uplink ports 2 and 3 are configured as VCPs by default. No other uplink ports on any other EX Series switches are configured as VCPs by default.

You might experience a temporary traffic disruption immediately after creating or deleting a user-configured VCP in an EX8200 Virtual Chassis.

Options

pic-slot pic-slot—Number of the PIC slot for the uplink port or SFP network port on the switch.

port port-number—Number of the uplink port or SFP network port that is to be enabled or disabled as a VCP.

member member-id—(Optional) Enable or disable the specified VCP on the specified member of the Virtual Chassis configuration.

Required Privilege

Level system-control

Related Documentation

• request virtual-chassis vc-port (dedicated port)
  • show virtual-chassis vc-port on page 4579
  • show virtual-chassis vc-port statistics on page 4597
  • clear virtual-chassis vc-port statistics on page 4541
  • Virtual Chassis Port (VCP) Interface Names in an EX8200 Virtual Chassis
  • Understanding EX Series Virtual Chassis Components on page 4460

List of Sample Output

request virtual-chassis vc-port set pic-slot 1 port 0 on page 4546
request virtual-chassis vc-port set pic-slot 1 port 1 member 3 on page 4547
request virtual-chassis vc-port delete pic-slot 1 port 1 member 3 on page 4547

Sample Output

request virtual-chassis vc-port set pic-slot 1 port 0

user@switch> request virtual-chassis vc-port set pic-slot 1 port 0
To check the results of this command, use the `show virtual-chassis vc-port` command.

```plaintext
request virtual-chassis vc-port set pic-slot 1 port 1 member 3
  user@switch> request virtual-chassis vc-port set pic-slot 1 port 1 member 3
To check the results of this command, use the `show virtual-chassis vc-port` command.

request virtual-chassis vc-port delete pic-slot 1 port 1 member 3
  user@switch> request virtual-chassis vc-port delete pic-slot 1 port 1 member 3
To check the results of this command, use the `show virtual-chassis vc-port` command.
```
**request virtual-chassis vc-port diagnostics optics**

**Syntax**

`request virtual-chassis vc-port diagnostics optics`

**Release Information**

Command introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

**Description**

Run a digital optical monitoring (DOM) scan on the optical ports configured as Virtual Chassis ports (VCPs).

Enter the `show virtual-chassis vc-port diagnostics optics` command to view the results of the diagnostic scan.

On certain EX Series switches, the `request virtual-chassis vc-port diagnostics optics` command must be entered to run a diagnostic scan before you can gather the `show virtual-chassis vc-port diagnostics optics` output.

**Required Privilege Level**

`system-control`

**Related Documentation**

- `show virtual-chassis vc-port diagnostics optics` on page 4583

**Sample Output**

```
request virtual-chassis vc-port diagnostics optics
user@switch> request virtual-chassis vc-port diagnostics optics
fpc0:
--------------------------------------------------------------------------
vc-port Diagnostics Optics Done
```
show system uptime

Syntax  show system uptime (all-members | member member-id)

Release Information  Command introduced in Junos OS Release 9.0 for EX Series switches.

Description  Display the current time and information about how long the Virtual Chassis, the Junos OS software, and routing protocols have been running.

Options

- **all-members**—Display the current time and information about how long the Virtual Chassis, the Junos OS software, and routing protocols have been running for all the member switches of the Virtual Chassis configuration.

- **member member-id**—Display the current time and information about how long the Virtual Chassis, the Junos OS software, and routing protocols have been running for the specific member of the Virtual Chassis configuration.

Required Privilege  view

Related Documentation

- virtual-chassis on page 4527
- Monitoring System Properties on page 714

List of Sample Output  show system uptime member 0 on page 4550

Output Fields  Table 559 on page 4549 lists the output fields for the show system uptime command. Output fields are listed in the approximate order in which they appear.

Table 559: show system uptime Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current time</td>
<td>Current system time in UTC.</td>
</tr>
<tr>
<td>System booted</td>
<td>Date and time when the switch was last booted and how long it has been running.</td>
</tr>
<tr>
<td>Protocols started</td>
<td>Date and time when the routing protocols were last started and how long they have been running.</td>
</tr>
<tr>
<td>Last configured</td>
<td>Date and time when a configuration was last committed. Also shows the name of the user who issued the last commit command.</td>
</tr>
<tr>
<td>Time and up</td>
<td>Current time, in the local time zone, and how long the switch has been operational.</td>
</tr>
<tr>
<td>Users</td>
<td>Number of users logged into the switch.</td>
</tr>
<tr>
<td>Load averages</td>
<td>Load averages for the last 1 minute, 5 minutes, and 15 minutes.</td>
</tr>
</tbody>
</table>
Sample Output

show system uptime member 0

user@switch>show system uptime member 0
fpc0:
------------------------------------------------------------------------
Current time: 2008-02-06 05:24:20 UTC
System booted: 2008-01-31 08:26:54 UTC (5d 20:57 ago)
Protocols started: 2008-01-31 08:27:56 UTC (5d 20:56 ago)
Last configured: 2008-02-05 03:26:43 UTC (1d 01:57 ago) by root
5:24AM up 5 days, 20:57, 1 user, load averages: 0.14, 0.06, 0.01
show virtual-chassis active-topology

Syntax

show virtual-chassis active-topology
   <all-members>
   <local>
   <member member-id>

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.

Description

Display the active topology of the Virtual Chassis configuration with next-hop reachability information.

Options

none—Display the active topology of the member switch where the command is issued.

all-members—(Optional) Display the active topology of all members of the Virtual Chassis configuration.

local—(Optional) Display the active topology of the switch or external Routing Engine on which this command is entered.

member member-id—(Optional) Display the active topology of the specified member of the Virtual Chassis configuration.

Required Privilege

Level view

Related Documentation

• Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537

• Understanding EX Series Virtual Chassis Configuration on page 4475

List of Sample Output

show virtual-chassis active-topology (EX4200 Virtual Chassis) on page 4551
show virtual-chassis active-topology (EX8200 Virtual Chassis) on page 4552

Output Fields

Table 560 on page 4551 lists the output fields for the show virtual-chassis active-topology command. Output fields are listed in the approximate order in which they appear.

Table 560: show virtual-chassis active-topology Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination ID</td>
<td>Specifies the member ID of the destination.</td>
</tr>
<tr>
<td>Next-hop</td>
<td>Specifies the member ID and Virtual Chassis port (VCP) of the next hop to which packets for the destination ID are forwarded.</td>
</tr>
</tbody>
</table>

Sample Output

show virtual-chassis active-topology (EX4200 Virtual Chassis)

   user@switch> show virtual-chassis active-topology
show virtual-chassis active-topology (EX8200 Virtual Chassis)

user@external-routing-engine> show virtual-chassis active-topology
member0:

<table>
<thead>
<tr>
<th>Destination ID</th>
<th>Next-hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1(vcp-4/0/4.32768)</td>
</tr>
<tr>
<td>8</td>
<td>8(vcp-0/0.32768)</td>
</tr>
<tr>
<td>9</td>
<td>8(vcp-0/0.32768)</td>
</tr>
</tbody>
</table>

member1:

<table>
<thead>
<tr>
<th>Destination ID</th>
<th>Next-hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0(vcp-3/0/4.32768)</td>
</tr>
<tr>
<td>8</td>
<td>8(vcp-0/0.32768)</td>
</tr>
<tr>
<td>9</td>
<td>8(vcp-0/0.32768)</td>
</tr>
</tbody>
</table>

member8:

<table>
<thead>
<tr>
<th>Destination ID</th>
<th>Next-hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0(vcp-1/1.32768)</td>
</tr>
<tr>
<td>Destination ID</td>
<td>Next-hop</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>0</td>
<td>8(vcp-1/2.32768)</td>
</tr>
<tr>
<td>1</td>
<td>8(vcp-1/2.32768)</td>
</tr>
<tr>
<td>8</td>
<td>8(vcp-1/2.32768)</td>
</tr>
</tbody>
</table>
show virtual-chassis device-topology

Syntax

show virtual-chassis device-topology
<all-members>
<local>
<member member-id>

Release Information
Command introduced in Junos OS Release 10.4 for EX Series switches.

Description
Display the device topology—the member and system IDs, the VCP numbers, and device status—for all hardware devices in the Virtual Chassis.

Options
none—Display the Virtual Chassis device topology for all members of the Virtual Chassis.

all-members—(Optional) Display the Virtual Chassis device topology for all members of the Virtual Chassis.

local—(Optional) Display the Virtual Chassis device topology for the switch or external Routing Engine on which this command is entered.

member member-id—(Optional) Display the Virtual Chassis device topology for the specified member of the Virtual Chassis.

Required Privilege
Level
clear

Related Documentation
• Understanding EX Series Virtual Chassis Port Link Aggregation on page 4472
• Understanding EX8200 Virtual Chassis Topologies

Output Fields
Table 561 on page 4554 lists the output fields for the show virtual-chassis device-topology command. Output fields are listed in the approximate order in which they appear.

Table 561: show virtual-chassis device-topology Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
<td>Assigned member ID.</td>
</tr>
<tr>
<td>Device</td>
<td>Assigned device ID.</td>
</tr>
<tr>
<td></td>
<td>For an EX8200 Virtual Chassis, the member ID and the device ID are always identical.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the device within the Virtual Chassis. Outputs include:</td>
</tr>
<tr>
<td></td>
<td>* Prsnt—Device is currently connected to and participating in the Virtual Chassis configuration.</td>
</tr>
<tr>
<td></td>
<td>* NotPrsnt—Device is assigned but is not currently connected.</td>
</tr>
<tr>
<td>System ID</td>
<td>System ID of the device.</td>
</tr>
<tr>
<td></td>
<td>The system ID of the device is the device's MAC address.</td>
</tr>
</tbody>
</table>
Table 561: show virtual-chassis device-topology Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member (Neighbor List)</td>
<td>Assigned member ID of the neighbor device.</td>
</tr>
<tr>
<td>Device (Neighbor List)</td>
<td>Assigned device ID of the neighbor device.</td>
</tr>
<tr>
<td></td>
<td>For an EX8200 Virtual Chassis, the member ID and the device ID are always identical.</td>
</tr>
<tr>
<td>Interface (Neighbor List)</td>
<td>The interface connecting the device to the neighbor.</td>
</tr>
</tbody>
</table>

Sample Output

show virtual-chassis device-topology

```
user@switch> show virtual-chassis device-topology
member0:
------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Member</th>
<th>Device</th>
<th>Status</th>
<th>System ID</th>
<th>Neighbor List</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Prsnt</td>
<td>0021.59f7.d000</td>
<td>8 8</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Prsnt</td>
<td>0026.888d.6800</td>
<td>1 1</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>Prsnt</td>
<td>0000.4a75.9b7c</td>
<td>0 0</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>Prsnt</td>
<td>0000.73e9.9a57</td>
<td>0 0</td>
</tr>
</tbody>
</table>

member1:
------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Member</th>
<th>Device</th>
<th>Status</th>
<th>System ID</th>
<th>Neighbor List</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Prsnt</td>
<td>0021.59f7.d000</td>
<td>8 8</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Prsnt</td>
<td>0026.888d.6800</td>
<td>1 1</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>Prsnt</td>
<td>0000.4a75.9b7c</td>
<td>0 0</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>Prsnt</td>
<td>0000.73e9.9a57</td>
<td>0 0</td>
</tr>
</tbody>
</table>

member8:
------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Member</th>
<th>Device</th>
<th>Status</th>
<th>System ID</th>
<th>Neighbor List</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Prsnt</td>
<td>0021.59f7.d000</td>
<td>8 8</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Prsnt</td>
<td>0026.888d.6800</td>
<td>1 1</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Member</th>
<th>Device</th>
<th>Status</th>
<th>System ID</th>
<th>Neighbor List</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Prsnt</td>
<td>0021.59f7.d000</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Prsnt</td>
<td>0026.888d.6800</td>
<td>8 8 vcp-0/0</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>Prsnt</td>
<td>0000.4a75.9b7c</td>
<td>9 9 vcp-1/0</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>Prsnt</td>
<td>0000.73e9.9a57</td>
<td>8 8 vcp-1/0</td>
</tr>
</tbody>
</table>

Copyright © 2013, Juniper Networks, Inc.
### show virtual-chassis login

<table>
<thead>
<tr>
<th>Syntax</th>
<th>show virtual-chassis login</th>
</tr>
</thead>
</table>

**Release Information**  
Command introduced in Junos OS Release 9.3 for EX Series switches.

**Description**  
Supply the address of the host that logged into the Virtual Chassis, or identify the location of the member switch that redirected the current session to a different Virtual Chassis member switch.

You might need this information for tracing or troubleshooting purposes.

**Required Privilege Level**  
view

**Related Documentation**
- request session member on page 4543
- Understanding Global Management of an EX Series Virtual Chassis on page 4469

**List of Sample Output**
- show virtual-chassis login (Direct Login to the Master Console Port) on page 4557
- show virtual-chassis login (Backup Console Session Redirected to the Master Console Port) on page 4557

**Sample Output**

**show virtual-chassis login (Direct Login to the Master Console Port)**

```
user@switch> show virtual-chassis login
Current login session initiated from host 248.1.2.3
```

**show virtual-chassis login (Backup Console Session Redirected to the Master Console Port)**

```
user@switch> show virtual-chassis login
Current login session initiated from host backup
```
show virtual-chassis protocol adjacency

Syntax

```
show virtual-chassis protocol adjacency
  <brief | detail | extensive>
  <all-members>
  <local>
  <member member-id>
  <system-id>
```

Release Information

Command introduced in Junos OS Release 10.4 for EX Series switches.

Description

Display the Virtual Chassis Control Protocol (VCCP) adjacency statistics in the Virtual Chassis for all hardware devices.

Options

- **none**—Display VCCP adjacency statistics in brief form for all members of the Virtual Chassis.
- **brief | detail | extensive**—(Optional) Display the specified level of output. Using the **brief** option is equivalent to entering the command with no options (the default). The **detail** and **extensive** options provide identical displays.
- **all-members**—(Optional) Display VCCP adjacency statistics in brief form for all members of the Virtual Chassis.
- **local**—(Optional) Display VCCP adjacency statistics for the switch or external Routing Engine on which this command is entered.
- **member member-id**—(Optional) Display VCCP adjacency statistics for the specified member of the Virtual Chassis.
- **system-id**—(Optional) Display VCCP adjacency statistics for the specified member of the Virtual Chassis.

Required Privilege

- **clear**

Related Documentation

- Understanding EX Series Virtual Chassis Port Link Aggregation on page 4472
- Understanding the Virtual Chassis Control Protocol in an EX8200 Virtual Chassis

List of Sample Output

- `show virtual-chassis protocol adjacency` on page 4559
- `show virtual-chassis protocol adjacency detail` on page 4560

Output Fields

Table 562 on page 4558 lists the output fields for the `show virtual-chassis protocol adjacency` command. Output fields are listed in the approximate order in which they appear.

Table 562: show virtual-chassis protocol adjacency Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the Virtual Chassis port (VCP) interface.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
Table 562: show virtual-chassis protocol adjacency Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>The MAC address of the device on the receiving side of the VCP link.</td>
<td>All levels</td>
</tr>
<tr>
<td>State</td>
<td>State of the link. Outputs include:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• Up—The link is up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Down—The link is down.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• New—The link is new.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• One-way—The link is transmitting traffic in one direction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Initializing—The link is initializing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Rejected—The link is rejected.</td>
<td></td>
</tr>
<tr>
<td>Hold, Expires in</td>
<td>Remaining holdtime of the adjacency.</td>
<td>All levels</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority to become the designated intermediary system.</td>
<td>detail</td>
</tr>
<tr>
<td>Up/Down Transitions</td>
<td>Count of adjacency status transition changes from up to down or down to up.</td>
<td>detail</td>
</tr>
<tr>
<td>Last transition</td>
<td>Time of the last up/down transition.</td>
<td>detail</td>
</tr>
</tbody>
</table>

Sample Output

show virtual-chassis protocol adjacency

user@switch> show virtual-chassis protocol adjacency

member0:

<table>
<thead>
<tr>
<th>Interface</th>
<th>System</th>
<th>State</th>
<th>Hold (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0/0.32768</td>
<td>0000.4a75.9b7c</td>
<td>Up</td>
<td>57</td>
</tr>
<tr>
<td>vcp-0/1.32768</td>
<td>0000.4a75.9b7c</td>
<td>Up</td>
<td>59</td>
</tr>
<tr>
<td>vcp-4/0/1.32768</td>
<td>0026.888d.6800</td>
<td>Up</td>
<td>57</td>
</tr>
</tbody>
</table>

member1:

<table>
<thead>
<tr>
<th>Interface</th>
<th>System</th>
<th>State</th>
<th>Hold (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0/0.32768</td>
<td>0000.4a75.9b7c</td>
<td>Up</td>
<td>58</td>
</tr>
<tr>
<td>vcp-0/1.32768</td>
<td>0000.73e9.9a57</td>
<td>Up</td>
<td>59</td>
</tr>
<tr>
<td>vcp-3/0/4.32768</td>
<td>0021.59f7.d000</td>
<td>Up</td>
<td>58</td>
</tr>
</tbody>
</table>

member8:

<table>
<thead>
<tr>
<th>Interface</th>
<th>System</th>
<th>State</th>
<th>Hold (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-1/0.32768</td>
<td>0000.73e9.9a57</td>
<td>Up</td>
<td>58</td>
</tr>
<tr>
<td>vcp-1/1.32768</td>
<td>0021.59f7.d000</td>
<td>Up</td>
<td>58</td>
</tr>
<tr>
<td>vcp-1/2.32768</td>
<td>0026.888d.6800</td>
<td>Up</td>
<td>59</td>
</tr>
<tr>
<td>vcp-2/0.32768</td>
<td>0021.59f7.d000</td>
<td>Up</td>
<td>59</td>
</tr>
</tbody>
</table>

member9:

<table>
<thead>
<tr>
<th>Interface</th>
<th>System</th>
<th>State</th>
<th>Hold (secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-1/0.32768</td>
<td>0000.4a75.9b7c</td>
<td>Up</td>
<td>58</td>
</tr>
<tr>
<td>vcp-1/1.32768</td>
<td>0026.888d.6800</td>
<td>Up</td>
<td>59</td>
</tr>
</tbody>
</table>
show virtual-chassis protocol adjacency detail

user@switch> show virtual-chassis protocol adjacency detail
member0:
--------------------------------------------------------------------------
0000.4a75.9b7c
   interface-name: vcp-0/0.32768, State: Up, Expires in 57 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:37 ago

0000.4a75.9b7c
   interface-name: vcp-0/1.32768, State: Up, Expires in 59 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:37 ago

0026.888d.6800
   interface-name: vcp-4/0/1.32768, State: Up, Expires in 59 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 22:06:39 ago

member1:
--------------------------------------------------------------------------
0000.4a75.9b7c
   interface-name: vcp-0/0.32768, State: Up, Expires in 59 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:38 ago

0000.73e9.9a57
   interface-name: vcp-0/1.32768, State: Up, Expires in 58 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 22:17:36 ago

0021.59f7.d000
   interface-name: vcp-3/0/4.32768, State: Up, Expires in 58 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 22:06:39 ago

member8:
--------------------------------------------------------------------------
0000.73e9.9a57
   interface-name: vcp-1/0.32768, State: Up, Expires in 58 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:38 ago

0021.59f7.d000
   interface-name: vcp-1/1.32768, State: Up, Expires in 59 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:38 ago

0026.888d.6800
   interface-name: vcp-1/2.32768, State: Up, Expires in 59 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:38 ago

0021.59f7.d000
   interface-name: vcp-2/0.32768, State: Up, Expires in 57 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:38 ago

member9:
--------------------------------------------------------------------------
0000.4a75.9b7c
   interface-name: vcp-1/0.32768, State: Up, Expires in 59 secs
   Priority: 0, Up/Down transitions: 1, Last transition: 19:26:38 ago

0026.888d.6800
interface-name: vcp-1/1.32768, State: Up, Expires in 58 secs
Priority: 0, Up/Down transitions: 1, Last transition: 22:17:36 ago
**show virtual-chassis protocol database**

**Syntax**
```
show virtual-chassis protocol database
  <brief | detail | extensive>
  <all-members>
  <local>
  <member member-id>
```

**Release Information**
Command introduced in Junos OS Release 10.4 for EX Series switches.

**Description**
Display the Virtual Chassis Control Protocol (VCCP) database statistics for all hardware devices within the Virtual Chassis.

**Options**
- **none**—Display VCCP database statistics in brief form for all members of the Virtual Chassis.
- **brief | detail | extensive**—(Optional) Display the specified level of output. Using the `brief` option is equivalent to entering the command with no options (the default). The `detail` option provides more output than the `brief` option. The `extensive` option provides all output and is most useful for customer support personnel.
- **all-members**—(Optional) Display VCCP database statistics in brief form for all members of the Virtual Chassis.
- **local**—(Optional) Display VCCP database statistics for the switch or external Routing Engine on which this command is entered.
- **member member-id**—(Optional) Display VCCP database statistics for the specified member of the Virtual Chassis.

**Required Privilege**
- clear

**Related Documentation**
- "Understanding the Virtual Chassis Control Protocol in an EX8200 Virtual Chassis"

**List of Sample Output**
- `show virtual-chassis protocol database` on page 4563
- `show virtual-chassis protocol database detail` on page 4564

**Output Fields**
Table 563 on page 4562 lists the output fields for the `show virtual-chassis protocol database` command. Output fields are listed in the approximate order in which they appear.

**Table 563: show virtual-chassis protocol database Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP ID</td>
<td>Link-state protocol (LSP) data unit identifier.</td>
<td>All levels</td>
</tr>
<tr>
<td>Sequence</td>
<td>Sequence number of the LSP.</td>
<td>All levels</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum value of the LSP.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 563: show virtual-chassis protocol database Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifetime</td>
<td>Remaining lifetime of the LSP, in seconds.</td>
<td>All levels</td>
</tr>
<tr>
<td>Neighbor</td>
<td>MAC address of the neighbor on the advertising system.</td>
<td>detail</td>
</tr>
<tr>
<td>Interface</td>
<td>Virtual Chassis port (VCP) interface name.</td>
<td>detail</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric of the prefix or neighbor.</td>
<td>detail</td>
</tr>
</tbody>
</table>

The **extensive** output was omitted from this list. The **extensive** output is useful for customer support personnel only.

### Sample Output

**show virtual-chassis protocol database**

```plaintext
user@switch> show virtual-chassis protocol database
member0:

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c.00-00</td>
<td>0x1dd80</td>
<td>0xc2e3</td>
<td>116</td>
</tr>
<tr>
<td>0000.73e9.9a57.00-00</td>
<td>0xf361</td>
<td>0x27e8</td>
<td>113</td>
</tr>
<tr>
<td>0021.59f7.d000.00-00</td>
<td>0x16882</td>
<td>0x3993</td>
<td>118</td>
</tr>
<tr>
<td>0026.888d.6800.00-00</td>
<td>0x1691f</td>
<td>0x82b7</td>
<td>116</td>
</tr>
<tr>
<td>4 LSPs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

member1:

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c.00-00</td>
<td>0x1dd80</td>
<td>0xc2e3</td>
<td>116</td>
</tr>
<tr>
<td>0000.73e9.9a57.00-00</td>
<td>0xf361</td>
<td>0x27e8</td>
<td>114</td>
</tr>
<tr>
<td>0021.59f7.d000.00-00</td>
<td>0x16883</td>
<td>0x289</td>
<td>116</td>
</tr>
<tr>
<td>0026.888d.6800.00-00</td>
<td>0x1691f</td>
<td>0x82b7</td>
<td>118</td>
</tr>
<tr>
<td>4 LSPs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

member8:

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c.00-00</td>
<td>0x1dd80</td>
<td>0xc2e3</td>
<td>118</td>
</tr>
<tr>
<td>0000.73e9.9a57.00-00</td>
<td>0xf361</td>
<td>0x27e8</td>
<td>114</td>
</tr>
<tr>
<td>0021.59f7.d000.00-00</td>
<td>0x16883</td>
<td>0x289</td>
<td>116</td>
</tr>
<tr>
<td>0026.888d.6800.00-00</td>
<td>0x16920</td>
<td>0xa335</td>
<td>116</td>
</tr>
<tr>
<td>4 LSPs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

member9:

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c.00-00</td>
<td>0x1dd80</td>
<td>0xc2e3</td>
<td>116</td>
</tr>
<tr>
<td>0000.73e9.9a57.00-00</td>
<td>0xf361</td>
<td>0x27e8</td>
<td>116</td>
</tr>
<tr>
<td>0021.59f7.d000.00-00</td>
<td>0x16883</td>
<td>0x289</td>
<td>114</td>
</tr>
<tr>
<td>0026.888d.6800.00-00</td>
<td>0x16920</td>
<td>0xa335</td>
<td>116</td>
</tr>
<tr>
<td>4 LSPs</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
show virtual-chassis protocol database detail

user@switch> show virtual-chassis protocol database detail

member0:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1ddbc</td>
<td>0x3111</td>
<td>115 secs</td>
</tr>
<tr>
<td>0xf381</td>
<td>0xe065</td>
<td>114 secs</td>
</tr>
<tr>
<td>0x168af</td>
<td>0xca97</td>
<td>115 secs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Interface</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c.00</td>
<td>vcp-1/0.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.73e9.9a57.00</td>
<td>vcp-1/1.32768</td>
<td>150</td>
</tr>
<tr>
<td>0026.888d.6800.00</td>
<td>vcp-1/2.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.4a75.9b7c.00</td>
<td>vcp-0/0.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.73e9.9a57.00</td>
<td>vcp-0/1.32768</td>
<td>150</td>
</tr>
<tr>
<td>0021.59f7.d000.00</td>
<td>vcp-3/0.32768</td>
<td>15</td>
</tr>
</tbody>
</table>

member1:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1ddbc</td>
<td>0x3111</td>
<td>115 secs</td>
</tr>
<tr>
<td>0xf381</td>
<td>0xe065</td>
<td>116 secs</td>
</tr>
<tr>
<td>0x168af</td>
<td>0xca97</td>
<td>115 secs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Interface</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c.00</td>
<td>vcp-1/0.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.73e9.9a57.00</td>
<td>vcp-1/1.32768</td>
<td>150</td>
</tr>
<tr>
<td>0026.888d.6800.00</td>
<td>vcp-1/2.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.4a75.9b7c.00</td>
<td>vcp-0/0.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.73e9.9a57.00</td>
<td>vcp-0/1.32768</td>
<td>150</td>
</tr>
<tr>
<td>0021.59f7.d000.00</td>
<td>vcp-3/0.32768</td>
<td>15</td>
</tr>
</tbody>
</table>

member8:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1ddbd</td>
<td>0xfd83</td>
<td>118 secs</td>
</tr>
<tr>
<td>0xf381</td>
<td>0xe065</td>
<td>116 secs</td>
</tr>
<tr>
<td>0x168af</td>
<td>0xca97</td>
<td>117 secs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Interface</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c.00</td>
<td>vcp-1/0.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.73e9.9a57.00</td>
<td>vcp-1/1.32768</td>
<td>150</td>
</tr>
<tr>
<td>0026.888d.6800.00</td>
<td>vcp-1/2.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.4a75.9b7c.00</td>
<td>vcp-0/0.32768</td>
<td>150</td>
</tr>
<tr>
<td>0000.73e9.9a57.00</td>
<td>vcp-0/1.32768</td>
<td>150</td>
</tr>
<tr>
<td>0021.59f7.d000.00</td>
<td>vcp-3/0.32768</td>
<td>15</td>
</tr>
</tbody>
</table>
0026.888d.6800.00-00 Sequence: 0x1694e, Checksum: 0xca97, Lifetime: 115 secs
Neighbor: 0000.4a75.9b7c.00 Interface: vcp-0/0.32768 Metric: 150
Neighbor: 0000.73e9.9a57.00 Interface: vcp-0/1.32768 Metric: 150
Neighbor: 0021.59f7.d000.00 Interface: vcp-0/3/0/4.32768 Metric: 15

member9:
--------------------------------------------------------------------------
0000.4a75.9b7c.00-00 Sequence: 0x1ddbd, Checksum: 0xfd83, Lifetime: 116 secs
Neighbor: 0000.73e9.9a57.00 Interface: vcp-1/0.32768 Metric: 150
Neighbor: 0021.59f7.d000.00 Interface: vcp-1/1.32768 Metric: 150
Neighbor: 0026.888d.6800.00 Interface: vcp-1/2.32768 Metric: 150

0000.73e9.9a57.00-00 Sequence: 0xf381, Checksum: 0xe065, Lifetime: 117 secs
Neighbor: 0000.4a75.9b7c.00 Interface: vcp-1/0.32768 Metric: 150
Neighbor: 0026.888d.6800.00 Interface: vcp-1/1.32768 Metric: 150

0021.59f7.d000.00-00 Sequence: 0x168af, Checksum: 0x8b0b, Lifetime: 113 secs
Neighbor: 0000.4a75.9b7c.00 Interface: vcp-0/0.32768 Metric: 150
Neighbor: 0026.888d.6800.00 Interface: vcp-0/4/0.32768 Metric: 15

0026.888d.6800.00-00 Sequence: 0x1694f, Checksum: 0xa61a, Lifetime: 116 secs
Neighbor: 0000.4a75.9b7c.00 Interface: vcp-0/0.32768 Metric: 150
Neighbor: 0000.73e9.9a57.00 Interface: vcp-0/1.32768 Metric: 150
Neighbor: 0021.59f7.d000.00 Interface: vcp-3/0/4.32768 Metric: 15
show virtual-chassis protocol interface

Syntax

```
show virtual-chassis protocol interface
  <brief | detail>
  <all-members>
  <interface-name>
  <local>
  <member member-id>
```

Release Information

Command introduced in Junos OS Release 10.4 for EX Series switches.

Description

Display information about Virtual Chassis Control Protocol (VCCP) statistics for VCCP-enabled interfaces within the Virtual Chassis.

Options

- **none**—Display the VCCP interface statistics in brief form for all members of the Virtual Chassis.
- **brief | detail**—(Optional) Display the specified level of output. Using the **brief** option is equivalent to entering the command with no options (the default). The **detail** option provides more output than the **brief** option.
- **all-members**—(Optional) Display VCCP interface statistics for all members of the Virtual Chassis.
- **interface-name**—(Optional) Display VCCP interface statistics for the specified interface.
- **local**—(Optional) Display VCCP interface statistics for the switch or external Routing Engine on which this command is entered.
- **member member-id**—(Optional) Display VCCP interface statistics for the specified member of the Virtual Chassis.

Required Privilege

```
clear
```

Related Documentation

- [EX Series Virtual Chassis Overview](#)
- [Understanding Virtual Chassis Ports in an EX8200 Virtual Chassis](#)
- [Understanding the Virtual Chassis Control Protocol in an EX8200 Virtual Chassis](#)

List of Sample Output

```
show virtual-chassis protocol interface on page 4567
```

Output Fields

Table 564 on page 4566 lists the output fields for the `show virtual-chassis protocol interface` command. Output fields are listed in the approximate order in which they appear.

Table 564: show virtual-chassis protocol interface Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the VCP.</td>
<td>All levels</td>
</tr>
</tbody>
</table>
### Table 564: show virtual-chassis protocol interface Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the link. Outputs include:</td>
<td>All levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Up</strong>—The link is up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>Down</strong>—The link is down.</td>
<td></td>
</tr>
<tr>
<td>Metric</td>
<td>Metric of the prefix or neighbor.</td>
<td>All levels</td>
</tr>
</tbody>
</table>

### Sample Output

**show virtual-chassis protocol interface**

```plaintext
user@switch> show virtual-chassis protocol interface
member0:

<table>
<thead>
<tr>
<th>IS-IS interface database:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>State</td>
<td>Metric</td>
</tr>
<tr>
<td>vcp-0/0.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-0/1.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-4/0/1.32768</td>
<td>Up</td>
<td>15</td>
</tr>
<tr>
<td>vcp-4/0/7.32768</td>
<td>Down</td>
<td>15</td>
</tr>
</tbody>
</table>

member1:

<table>
<thead>
<tr>
<th>IS-IS interface database:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>State</td>
<td>Metric</td>
</tr>
<tr>
<td>vcp-0/0.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-0/1.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-3/0/4.32768</td>
<td>Up</td>
<td>15</td>
</tr>
</tbody>
</table>

member8:

<table>
<thead>
<tr>
<th>IS-IS interface database:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>State</td>
<td>Metric</td>
</tr>
<tr>
<td>vcp-0/0.32768</td>
<td>Down</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/0.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/1.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/2.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/3.32768</td>
<td>Down</td>
<td>150</td>
</tr>
<tr>
<td>vcp-2/0.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-2/1.32768</td>
<td>Down</td>
<td>150</td>
</tr>
<tr>
<td>vcp-2/2.32768</td>
<td>Down</td>
<td>150</td>
</tr>
<tr>
<td>vcp-2/3.32768</td>
<td>Down</td>
<td>150</td>
</tr>
</tbody>
</table>

member9:

<table>
<thead>
<tr>
<th>IS-IS interface database:</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>State</td>
<td>Metric</td>
</tr>
<tr>
<td>vcp-0/0.32768</td>
<td>Down</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/0.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/1.32768</td>
<td>Up</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/2.32768</td>
<td>Down</td>
<td>150</td>
</tr>
<tr>
<td>vcp-1/3.32768</td>
<td>Down</td>
<td>150</td>
</tr>
</tbody>
</table>
```
show virtual-chassis protocol route

**Syntax**

```
show virtual-chassis protocol route
<all-members>
<destination-id>
<local>
<member member-id>
```

**Release Information**

Command introduced in Junos OS Release 10.4 for EX Series switches.

**Description**

Display the unicast and multicast Virtual Chassis Control Protocol (VCCP) routing tables within the Virtual Chassis.

**Options**

- **none**—Display the unicast and multicast routing tables for all members of the Virtual Chassis.

- **all-members**—(Optional) Display the unicast and multicast routing tables for all members of the Virtual Chassis.

- **destination-id**—(Optional) Display the unicast and multicast routing tables to the specified destination member ID for each member of the Virtual Chassis.

- **local**—(Optional) Display the unicast and multicast routing tables on the device where this command is entered.

- **member member-id**—(Optional) Display the unicast and multicast routing tables for the specified member of the Virtual Chassis.

**Required Privilege**

- **clear**

**Related Documentation**

- *Understanding the Virtual Chassis Control Protocol in an EX8200 Virtual Chassis*

**List of Sample Output**

show virtual-chassis protocol route on page 4569

**Output Fields**

Table 565 on page 4568 lists the output fields for the `show virtual-chassis protocol route` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dev</td>
<td>MAC address of the member storing the VCCP routing table.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the shortest-path-first algorithm that generated the routing table.</td>
</tr>
<tr>
<td>System ID</td>
<td>MAC address of the device.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the shortest-path-first (SPF) algorithm that generated the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric number to get to that device.</td>
</tr>
</tbody>
</table>
Table 565: show virtual-chassis protocol route Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the Virtual Chassis port (VCP) interface connecting the devices.</td>
</tr>
<tr>
<td>Via</td>
<td>MAC address of the next-hop device, if applicable.</td>
</tr>
</tbody>
</table>

Sample Output

show virtual-chassis protocol route

```
user@switch> show virtual-chassis protocol route
member0:
--------------------------------------------------------------------------
Dev 0021.59f7.d000 ucast routing table  Current version: 21
--------------------------------------
System ID  Version  Metric  Interface     Via
0000.4a75.9b7c  21     150  vcp-0/1.32768 0000.4a75.9b7c
0000.73e9.9a57  21     165  vcp-4/0/1.32768 0026.888d.6800
0021.59f7.d000  21      0  vcp-4/0/1.32768 0026.888d.6800
0026.888d.6800  21     15  vcp-4/0/1.32768 0026.888d.6800

Dev 0021.59f7.d000 mcast routing table  Current version: 21
--------------------------------------
System ID  Version  Metric  Interface     Via
0000.4a75.9b7c  21
0000.73e9.9a57  21     vcp-3/0/4.32768 0021.59f7.d000
0021.59f7.d000  21     vcp-0/1.32768
0026.888d.6800  21

member1:
--------------------------------------------------------------------------
Dev 0026.888d.6800 ucast routing table  Current version: 25
--------------------------------------
System ID  Version  Metric  Interface     Via
0000.4a75.9b7c  25     150  vcp-0/0.32768 0000.4a75.9b7c
0000.73e9.9a57  25     150  vcp-0/1.32768 0000.73e9.9a57
0021.59f7.d000  25      15  vcp-3/0/4.32768 0021.59f7.d000
0026.888d.6800  25      0  vcp-0/0.32768

Dev 0026.888d.6800 mcast routing table  Current version: 25
--------------------------------------
System ID  Version  Metric  Interface     Via
0000.4a75.9b7c  25
0000.73e9.9a57  25     vcp-3/0/4.32768
0021.59f7.d000  25     vcp-0/1.32768
0026.888d.6800  25     vcp-3/0/4.32768
              vcp-0/0.32768
              vcp-0/1.32768

member8:
--------------------------------------------------------------------------
Dev 0000.4a75.9b7c ucast routing table  Current version: 39
--------------------------------------
System ID  Version  Metric  Interface     Via
0000.4a75.9b7c  25
0000.73e9.9a57  25     vcp-3/0/4.32768
0021.59f7.d000  25     vcp-0/1.32768
0026.888d.6800  25     vcp-3/0/4.32768
```

Copyright © 2013, Juniper Networks, Inc.
<table>
<thead>
<tr>
<th>System ID</th>
<th>Version</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c</td>
<td>39</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0000.73e9.9a57</td>
<td>39</td>
<td>150</td>
<td>vcp-1/0.32768</td>
<td>0000.73e9.9a57</td>
</tr>
<tr>
<td>0021.59f7.d000</td>
<td>39</td>
<td>150</td>
<td>vcp-2/0.32768</td>
<td>0021.59f7.d000</td>
</tr>
<tr>
<td>0026.888d.6800</td>
<td>39</td>
<td>150</td>
<td>vcp-1/2.32768</td>
<td>0026.888d.6800</td>
</tr>
</tbody>
</table>

Dev 0000.4a75.9b7c mcast routing table
Current version: 39

<table>
<thead>
<tr>
<th>System ID</th>
<th>Version</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c</td>
<td>39</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0000.73e9.9a57</td>
<td>39</td>
<td>150</td>
<td>vcp-1/0.32768</td>
<td>0000.73e9.9a57</td>
</tr>
<tr>
<td>0021.59f7.d000</td>
<td>39</td>
<td>150</td>
<td>vcp-1/0.32768</td>
<td>0021.59f7.d000</td>
</tr>
<tr>
<td>0026.888d.6800</td>
<td>39</td>
<td>150</td>
<td>vcp-1/2.32768</td>
<td>0026.888d.6800</td>
</tr>
</tbody>
</table>

Dev 0000.73e9.9a57 ucast routing table
Current version: 31

<table>
<thead>
<tr>
<th>System ID</th>
<th>Version</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c</td>
<td>31</td>
<td>150</td>
<td>vcp-1/0.32768</td>
<td>0000.4a75.9b7c</td>
</tr>
<tr>
<td>0000.73e9.9a57</td>
<td>31</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0021.59f7.d000</td>
<td>31</td>
<td>165</td>
<td>vcp-1/1.32768</td>
<td>0026.888d.6800</td>
</tr>
<tr>
<td>0026.888d.6800</td>
<td>31</td>
<td>150</td>
<td>vcp-1/1.32768</td>
<td>0026.888d.6800</td>
</tr>
</tbody>
</table>

Dev 0000.73e9.9a57 mcast routing table
Current version: 31

<table>
<thead>
<tr>
<th>System ID</th>
<th>Version</th>
<th>Metric</th>
<th>Interface</th>
<th>Via</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.4a75.9b7c</td>
<td>31</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0000.73e9.9a57</td>
<td>31</td>
<td>150</td>
<td>vcp-1/0.32768</td>
<td>0000.73e9.9a57</td>
</tr>
<tr>
<td>0021.59f7.d000</td>
<td>31</td>
<td>150</td>
<td>vcp-1/1.32768</td>
<td>0021.59f7.d000</td>
</tr>
<tr>
<td>0026.888d.6800</td>
<td>31</td>
<td>150</td>
<td>vcp-1/1.32768</td>
<td>0026.888d.6800</td>
</tr>
</tbody>
</table>
show virtual-chassis protocol statistics

Syntax

```
show virtual-chassis protocol statistics
<all-members>
<interface-name>
<local>
<member member-id>
```

Release Information

Command introduced in Junos OS Release 10.4 for EX Series switches.

Description

Display the Virtual Chassis Control Protocol (VCCP) statistics for all hardware devices within the Virtual Chassis.

Options

- **none**—Display VCCP statistics for all members of the Virtual Chassis.
- **all-members**—(Optional) Display VCCP statistics for all members of the Virtual Chassis.
- **interface-name**—(Optional) Display VCCP statistics for the specified interface.
- **local**—(Optional) Display VCCP statistics for the switch or external Routing Engine on which this command is entered.
- **member member-id**—(Optional) Display VCCP statistics for the specified member of the Virtual Chassis.

Required Privilege Level

clear

Related Documentation

- Understanding the Virtual Chassis Control Protocol in an EX8200 Virtual Chassis

List of Sample Output

```text
show virtual-chassis protocol statistics on page 4572
```

Output Fields

Table 566 on page 4571 lists the output fields for the `show virtual-chassis protocol interface` command. Output fields are listed in the approximate order in which they appear.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDU type</td>
<td>Protocol data unit type.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of PDUs received since VCCP started or since the statistics were set to zero.</td>
</tr>
<tr>
<td>Processed</td>
<td>Number of PDUs received minus the number of PDUs dropped.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of PDUs dropped.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of PDUs transmitted since VCCP started or since the statistics were set to zero.</td>
</tr>
<tr>
<td>Rexmit</td>
<td>Number of PDUs retransmitted since VCCP started or since the statistics were set to zero.</td>
</tr>
</tbody>
</table>
Table 566: show virtual-chassis protocol statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Packets Received</td>
<td>Number of PDUs received since VCCP started or since the statistics were set to zero.</td>
</tr>
<tr>
<td>Total Packets Sent</td>
<td>Number of PDUs sent since VCCP started or since the statistics were set to zero.</td>
</tr>
<tr>
<td>LSP queue length</td>
<td>Number of link-state PDUs waiting in the queue for processing. This value is almost always 0.</td>
</tr>
<tr>
<td>SPF runs</td>
<td>Number of shortest-path-first (SPF) calculations that have been performed.</td>
</tr>
<tr>
<td>Fragments Rebuilt</td>
<td>Number of link-state PDU fragments that the local system has computed.</td>
</tr>
<tr>
<td>LSP Regenerations</td>
<td>Number of link-state PDUs that have been regenerated. A link-state PDU is regenerated when it is nearing the end of its lifetime and it has not changed.</td>
</tr>
<tr>
<td>Purges initiated</td>
<td>Number of purges that the system initiated. A purge is initiated if the software determines that a link-state PDU must be removed from the network.</td>
</tr>
</tbody>
</table>

Sample Output

show virtual-chassis protocol statistics

user@switch> show virtual-chassis protocol statistics
member0:
-------------------------------------------------------------------------
IS-IS statistics for 0021.59f7.d000:
PDU type    Received  Processed  Drops  Sent  Rexmit
LSP         8166      8166       0     4551   0
HELLO       1659      1659       0     1693   0
CSNP         2         2         0     3      0
PSNP        1909      1909       0     2293   0
Unknown     0         0         0      0      0
Totals      11736     11736      0     8540   0
-------------------------------------------------------------------------
Total packets received: 11736 Sent: 8540
LSP queue length: 0 Drops: 0
SPF runs: 9
Fragments rebuilt: 1640
LSP regenerations: 1
Purges initiated: 0

member1:
-------------------------------------------------------------------------
IS-IS statistics for 0026.888d.6800:
PDU type    Received  Processed  Drops  Sent  Rexmit
LSP         10909     10909      0     12088  0
HELLO       1877      1877       0     2251   0
CSNP         3         3         0     3      0
PSNP        3846      3846       0     3732   0
Unknown     0         0         0      0      0
Totals      16635     16635      0     18074  0
-------------------------------------------------------------------------
Total packets received: 16635  Sent: 18074
LSP queue length: 0  Drops: 0
SPF runs: 13
Fragments rebuilt: 1871
LSP regenerations: 2
Purges initiated: 0

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Reemit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>7935</td>
<td>7935</td>
<td>0</td>
<td>14865</td>
<td>0</td>
</tr>
<tr>
<td>HELLO</td>
<td>2695</td>
<td>2695</td>
<td>0</td>
<td>7124</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>4398</td>
<td>4398</td>
<td>0</td>
<td>3666</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>15032</td>
<td>15032</td>
<td>0</td>
<td>25659</td>
<td>0</td>
</tr>
</tbody>
</table>

Total packets received: 15032  Sent: 25659
LSP queue length: 0  Drops: 0
SPF runs: 26
Fragments rebuilt: 2666
LSP regenerations: 4
Purges initiated: 0

<table>
<thead>
<tr>
<th>PDU type</th>
<th>Received</th>
<th>Processed</th>
<th>Drops</th>
<th>Sent</th>
<th>Reemit</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>10800</td>
<td>10800</td>
<td>0</td>
<td>6327</td>
<td>0</td>
</tr>
<tr>
<td>HELLO</td>
<td>1492</td>
<td>1492</td>
<td>0</td>
<td>2356</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>2683</td>
<td>2683</td>
<td>0</td>
<td>3149</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Totals</td>
<td>14977</td>
<td>14977</td>
<td>0</td>
<td>11834</td>
<td>0</td>
</tr>
</tbody>
</table>

Total packets received: 14977  Sent: 11834
LSP queue length: 0  Drops: 0
SPF runs: 19
Fragments rebuilt: 1510
LSP regenerations: 6
Purges initiated: 0
**show virtual-chassis**

**Syntax**

```plaintext
show virtual-chassis
<status>
```

**Release Information**

Command introduced in Junos OS Release 9.2 for EX Series switches.

**Description**

Display information about all members of the Virtual Chassis configuration.

**Options**

- `none`—Display information about all Virtual Chassis members.
- `status`—Same output as for `show virtual-chassis`.

**Required Privilege Level**

view

**Related Documentation**

- show virtual-chassis active-topology on page 4551
- show virtual-chassis protocol adjacency on page 4558
- show virtual-chassis vc-path on page 4577

**List of Sample Output**

show virtual-chassis (EX4200 Virtual Chassis) on page 4575
show virtual-chassis (EX8200 Virtual Chassis) on page 4576

**Output Fields**

Table 567 on page 4574 lists the output fields for the `show virtual-chassis` command. Output fields are listed in the approximate order in which they appear.

**Table 567: show virtual-chassis Output Fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Chassis ID</td>
<td>Assigned ID that applies to the entire Virtual Chassis configuration.</td>
</tr>
<tr>
<td>Virtual Chassis Mode</td>
<td>Mode of the Virtual Chassis: Enabled, Disabled, or Mixed.</td>
</tr>
<tr>
<td>Member ID</td>
<td>Assigned member ID and FPC:</td>
</tr>
<tr>
<td></td>
<td>• On EX2200 Virtual Chassis and EX3300, EX4200, and EX4500 Virtual Chassis, member IDs are numbered 0 through 9. The FPC number refers to the member ID assigned to the switch.</td>
</tr>
<tr>
<td></td>
<td>• On EX8200 Virtual Chassis, member IDs are numbered 0 through 9. The FPC number indicates the slot number of the line card within the Virtual Chassis. The FPC number on member 0 is always 0 through 15. The FPC number on member 1 is always 16 through 31. The FPC number on member 2 is always 32 through 47, and so on for the members.</td>
</tr>
</tbody>
</table>
Table 567: show virtual-chassis Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
</table>
| **Status** | For a nonprovisioned configuration:  
  • **Prsnt** for a member that is currently connected to the Virtual Chassis configuration  
  • **NotPrsnt** for a member ID that has been assigned but is not currently connected  
  For a preprovisioned configuration:  
  • **Prsnt** for a member that is specified in the preprovisioned configuration file and is currently connected to the Virtual Chassis configuration  
  • **Unprvsn** for a member that is interconnected with the Virtual Chassis configuration but is not specified in the preprovisioned configuration file |
| **Serial No** | Serial number of the member switch or external Routing Engine. |
| **Model** | Model number of the member switch. |
| **Mastership Priority** | Mastership priority value of the member switch. |
| **Role** | Role of the member switch: Master, Backup, or Linecard. |
| **Mixed Mode** | (EX4200, EX4500, and EX4550 switches) Mixed mode configuration status:  
  • **Y** for a member switch configured in mixed mode.  
  • **N** for a member switch not configured in mixed mode.  
  • **NA** for a member switch that cannot be configured in mixed mode. |
| **Location** | Location of the member device.  
  If this field is empty, the location field was not set for the device. |
| **Neighbor List** | Member ID of the neighbor member to which this member’s Virtual Chassis port (VCP) is connected. |

Sample Output

show virtual-chassis (EX4200 Virtual Chassis)

```
user@switch> show virtual-chassis
Virtual Chassis ID: 0019.e250.47a0
Virtual Chassis Mode: Enabled

Member ID  Status  Serial No    Model      Mastership Priority  Role  Mode  ID  Interface
0 (FPC 0)  Prsnt   AK0207360276 ex4200-24t  249   Master*    N   8   vcp-0
1   vcp-1
1 (FPC 1)  Prsnt   AK0207360281 ex4200-24t  248   Backup     N   0   vcp-0
2   vcp-1
2 (FPC 2)  Prsnt   AJ0207391130 ex4200-48p  247   Linecard   N   1   vcp-0
```
show virtual-chassis (EX8200 Virtual Chassis)

user@external-routing-engine> show virtual-chassis
Virtual Chassis ID: c806.0842.de51
Virtual Chassis Mode: Enabled

<table>
<thead>
<tr>
<th>Member ID</th>
<th>Status</th>
<th>Serial No</th>
<th>Model</th>
<th>priority</th>
<th>Role</th>
<th>ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (FPC 0-15)</td>
<td>Prsnt</td>
<td>BA0908380001 ex8216</td>
<td>0 Linecard</td>
<td>0</td>
<td></td>
<td>8</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>1 (FPC 16-31)</td>
<td>Prsnt</td>
<td>BT0909411634 ex8208</td>
<td>0 Linecard</td>
<td>0</td>
<td></td>
<td>8</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>8 (FPC 128-143)</td>
<td>Prsnt</td>
<td>062009000021 ex-xre</td>
<td>128 Master</td>
<td>9</td>
<td></td>
<td>9</td>
<td>vcp-0/1</td>
</tr>
<tr>
<td>9 (FPC 144-159)</td>
<td>Prsnt</td>
<td>062009000022 ex-xre</td>
<td>128 Backup</td>
<td>8</td>
<td></td>
<td>9</td>
<td>vcp-0/1</td>
</tr>
</tbody>
</table>

Member ID for next new member: 9 (FPC 9)
show virtual-chassis vc-path

Syntax

show virtual-chassis vc-path source-interface interface-name destination-interface interface-name

Release Information

Command introduced in Junos OS Release 9.6 for EX Series switches.

Description

Show the path a packet takes when going from a source interface to a destination interface in a Virtual Chassis configuration.

Options

source-interface interface-name — Name of the interface from which the packet originates

destination-interface interface-name — Name of the interface to which the packet is delivered

Required Privilege

Level view

Related Documentation

• Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
• Understanding EX Series Virtual Chassis Configuration on page 4475
• EX8200 Virtual Chassis Overview

List of Sample Output

show virtual-chassis vc-path source-interface destination-interface on page 4578

Output Fields

Table 568 on page 4577 lists the output fields for the show virtual-chassis vc-path command. Output fields are listed in the approximate order in which they appear.

Table 568: show virtual-chassis vc-path Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop</td>
<td>The number of hops between the source and destination interfaces.</td>
</tr>
<tr>
<td>Member</td>
<td>The Virtual Chassis ID of the member switch that contains the Packet Forwarding Engine for each intermediate hop.</td>
</tr>
<tr>
<td>PFE-Device</td>
<td>The number of the Packet Forwarding Engine in each Virtual Chassis member through which a packet passes. Each Packet Forwarding Engine is the next hop of the preceding Packet Forwarding Engine.</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the interface through which the Packet Forwarding Engines are connected. The interface for the first hop is always the source interface and the interface for the last hop is always the destination interface. For intermediate hops, the <strong>Interface</strong> field denotes the Packet Forwarding Engines through which the packet passes on its way to the next hop.</td>
</tr>
</tbody>
</table>
Sample Output

show virtual-chassis vc-path source-interface destination-interface

```
show virtual-chassis vc-path source-interface ge-0/0/0 destination-interface ge-1/0/1
```

<table>
<thead>
<tr>
<th>Hop</th>
<th>Member</th>
<th>PFE-Device</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>ge-0/0/0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>internal-1/24</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
<td>vcp-0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>4</td>
<td>ge-1/0/1</td>
</tr>
</tbody>
</table>
show virtual-chassis vc-port

Syntax
show virtual-chassis vc-port
<all-members>
<local>
<member member-id>

Release Information
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description
Display the status of the Virtual Chassis ports (VCPs), including both the dedicated VCPs and the uplink ports configured as VCPs.

Options
none—Display the operational status of all VCPs of the member switch where the command is issued.

all-members—(Optional) Display the operational status of all VCPs on all members of the Virtual Chassis configuration.

local—(Optional) Display the operational status of the switch or external Routing Engine on which this command is entered.

member member-id—(Optional) Display the operational status of all VCPs for the specified member of the Virtual Chassis configuration.

Required Privilege
view

Related Documentation
- show virtual-chassis vc-port statistics on page 4597
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
- Verifying Virtual Chassis Ports in an EX8200 Virtual Chassis

List of Sample Output
show virtual-chassis vc-port (EX4200 Virtual Chassis) on page 4580
show virtual-chassis vc-port (EX8200 Virtual Chassis) on page 4581
show virtual-chassis vc-port all-members on page 4582

Output Fields
Table 569 on page 4579 lists the output fields for the show virtual-chassis vc-port command. Output fields are listed in the approximate order in which they appear.

Table 569: show virtual-chassis vc-port Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fpcnumber</td>
<td>The FPC number is the same as the member ID.</td>
</tr>
</tbody>
</table>
### Table 569: show virtual-chassis vc-port Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface or PIC/Port</td>
<td>VCP name.</td>
</tr>
<tr>
<td></td>
<td>• The dedicated VCPs in an EX4200, EX4500, or EX4550 Virtual Chassis are vcp-0 and vcp-1.</td>
</tr>
<tr>
<td></td>
<td>• The uplink module ports set as VCPs in an EX2200 Virtual Chassis or in an EX3300 or EX4200 Virtual Chassis are named 1/0 and 1/1, representing the PIC number and the port number.</td>
</tr>
<tr>
<td></td>
<td>• The native VCP (port 0) on an XRE200 External Routing Engine in an EX8200 Virtual Chassis is named vcp-0.</td>
</tr>
<tr>
<td></td>
<td>• The VCPs on each Virtual Chassis Control Interface (VCCI) module in an XRE200 External Routing Engine are named using the vcp-slot-number/port-number convention; for instance, vcp-1/0.</td>
</tr>
<tr>
<td></td>
<td>• The VCPs on EX8200 member switches are named using the vcp-slot-number/pic-number/interface-number convention; for instance, vcp-3/0/2.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of VCP:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Dedicated</strong>—The rear panel VCP on an EX4200, EX4500, or EX4550 switch, or any VCP link connected to an XRE200 External Routing Engine in an EX8200 Virtual Chassis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Configured</strong>—Optical port configured as a VCP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto-Configured</strong>—Optical port autoconfigured as a VCP.</td>
</tr>
<tr>
<td></td>
<td>See “Setting an Uplink Port on an EX Series Switch as a Virtual Chassis Port (CLI Procedure)” on page 4497 or Setting a 10-Gigabit Ethernet Port as a Virtual Chassis Port in an EX8200 Virtual Chassis (CLI Procedure) for information about configuring VCPs.</td>
</tr>
<tr>
<td>Trunk ID</td>
<td>A positive-number ID assigned to a link aggregation group (LAG) formed by the Virtual Chassis. The trunk ID value is −1 if no trunk is formed. A LAG between uplink VCPs requires that the link speed be the same on connected interfaces and that at least two VCPs on one member be connected to at least two VCPs on the other member in an EX4200 or EX4500 Virtual Chassis.</td>
</tr>
<tr>
<td></td>
<td>Dedicated VCP LAGs are assigned trunk IDs 1 and 2. Trunk IDs for LAGs formed with uplink VCPs therefore have values of 3 or greater.</td>
</tr>
<tr>
<td></td>
<td>The trunk ID value changes if the link-adjacency state between LAG members changes; trunk membership is then allocated or deallocated.</td>
</tr>
<tr>
<td>Status</td>
<td>Interface status:</td>
</tr>
<tr>
<td></td>
<td>• <strong>absent</strong>—Interface is not a VCP link.</td>
</tr>
<tr>
<td></td>
<td>• <strong>down</strong>—VCP link is down.</td>
</tr>
<tr>
<td></td>
<td>• <strong>up</strong>—VCP link is up.</td>
</tr>
<tr>
<td>Speed (mbps)</td>
<td>Speed of the interface in megabits per second.</td>
</tr>
<tr>
<td>NeighborID/Interface</td>
<td>The Virtual Chassis member ID and interface of a VCP on a member that is connected to the interface or PIC/Port field in the same row as this interface.</td>
</tr>
</tbody>
</table>

### Sample Output

**show virtual-chassis vc-port (EX4200 Virtual Chassis)**

```bash
user@switch> show virtual-chassis vc-port
fpc0:
```
### show virtual-chassis vc-port (EX8200 Virtual Chassis)

**user@external-routing-engine> show virtual-chassis vc-port**

#### member0:

<table>
<thead>
<tr>
<th>Interface or Slot/PIC/Port</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>8</td>
<td>vcp-1/1</td>
</tr>
<tr>
<td>vcp-0/1</td>
<td>Dedicated</td>
<td>-1</td>
<td>Down</td>
<td>10000</td>
<td>0</td>
<td>vcp-2/0</td>
</tr>
<tr>
<td>4/0/4</td>
<td>Configured</td>
<td>-1</td>
<td>Up</td>
<td>10000</td>
<td>1</td>
<td>vcp-3/0/4</td>
</tr>
<tr>
<td>4/0/7</td>
<td>Configured</td>
<td>-1</td>
<td>Down</td>
<td>10000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/3</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/2</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/5</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/6</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/1</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/0</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### member1:

<table>
<thead>
<tr>
<th>Interface or Slot/PIC/Port</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>8</td>
<td>vcp-1/2</td>
</tr>
<tr>
<td>3/0/0</td>
<td>Configured</td>
<td>-1</td>
<td>Down</td>
<td>10000</td>
<td>0</td>
<td>vcp-4/0/4</td>
</tr>
<tr>
<td>3/0/1</td>
<td>Configured</td>
<td>-1</td>
<td>Down</td>
<td>10000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3/0/4</td>
<td>Configured</td>
<td>-1</td>
<td>Down</td>
<td>10000</td>
<td>0</td>
<td>vcp-4/0/4</td>
</tr>
<tr>
<td>3/0/5</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/5</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/0/4</td>
<td>Configured</td>
<td>Absent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### member8:

<table>
<thead>
<tr>
<th>Interface or Slot/PIC/Port</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Down</td>
<td>1000</td>
<td>9</td>
<td>vcp-1/0</td>
</tr>
<tr>
<td>vcp-1/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>vcp-1/1</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>vcp-1/2</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>1</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>vcp-1/3</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>9</td>
<td>vcp-1/3</td>
</tr>
<tr>
<td>vcp-2/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-0/1</td>
</tr>
<tr>
<td>vcp-2/1</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>9</td>
<td>vcp-1/2</td>
</tr>
<tr>
<td>vcp-2/2</td>
<td>Dedicated</td>
<td>-1</td>
<td>Down</td>
<td>1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vcp-2/3</td>
<td>Dedicated</td>
<td>-1</td>
<td>Down</td>
<td>1000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### member9:

<table>
<thead>
<tr>
<th>Interface or Slot/PIC/Port</th>
<th>Type</th>
<th>Trunk ID</th>
<th>Status</th>
<th>Speed (mbps)</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Down</td>
<td>1000</td>
<td>9</td>
<td>vcp-1/2</td>
</tr>
<tr>
<td>vcp-1/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>vcp-1/1</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>vcp-1/2</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>1</td>
<td>vcp-0/0</td>
</tr>
<tr>
<td>vcp-1/3</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>9</td>
<td>vcp-1/3</td>
</tr>
<tr>
<td>vcp-2/0</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-0/1</td>
</tr>
<tr>
<td>vcp-2/1</td>
<td>Dedicated</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>9</td>
<td>vcp-1/2</td>
</tr>
<tr>
<td>vcp-2/2</td>
<td>Dedicated</td>
<td>-1</td>
<td>Down</td>
<td>1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vcp-2/3</td>
<td>Dedicated</td>
<td>-1</td>
<td>Down</td>
<td>1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIC / Port</td>
<td>Type</td>
<td>Trunk</td>
<td>Status</td>
<td>Speed</td>
<td>Neighbor ID</td>
<td>Interface</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>-------</td>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Up</td>
<td>32000</td>
<td>1</td>
<td>vcp-1</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Up</td>
<td>32000</td>
<td>0</td>
<td>vcp-0</td>
</tr>
<tr>
<td>1/0</td>
<td>Auto-Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>2</td>
<td>vcp-255/1/0</td>
</tr>
<tr>
<td>1/1</td>
<td>Auto-Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>2</td>
<td>vcp-255/1/1</td>
</tr>
</tbody>
</table>

show virtual-chassis vc-port all-members

user@switch> show virtual-chassis vc-port all-members

fpc0:

<table>
<thead>
<tr>
<th>PIC / Port</th>
<th>Type</th>
<th>Trunk</th>
<th>Status</th>
<th>Speed</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Up</td>
<td>32000</td>
<td>1</td>
<td>vcp-1</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Up</td>
<td>32000</td>
<td>0</td>
<td>vcp-0</td>
</tr>
<tr>
<td>1/0</td>
<td>Auto-Configured</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>3</td>
<td>vcp-255/1/0</td>
</tr>
<tr>
<td>1/1</td>
<td>Auto-Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>2</td>
<td>vcp-255/1/0</td>
</tr>
</tbody>
</table>

fpc1:

<table>
<thead>
<tr>
<th>PIC / Port</th>
<th>Type</th>
<th>Trunk</th>
<th>Status</th>
<th>Speed</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Up</td>
<td>32000</td>
<td>0</td>
<td>vcp-1</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Up</td>
<td>32000</td>
<td>3</td>
<td>vcp-0</td>
</tr>
<tr>
<td>1/0</td>
<td>Auto-Configured</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>3</td>
<td>vcp-255/1/0</td>
</tr>
<tr>
<td>1/1</td>
<td>Auto-Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-255/1/0</td>
</tr>
</tbody>
</table>

fpc2:

<table>
<thead>
<tr>
<th>PIC / Port</th>
<th>Type</th>
<th>Trunk</th>
<th>Status</th>
<th>Speed</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Up</td>
<td>32000</td>
<td>3</td>
<td>vcp-1</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Up</td>
<td>32000</td>
<td>3</td>
<td>vcp-0</td>
</tr>
<tr>
<td>1/0</td>
<td>Auto-Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-255/1/0</td>
</tr>
<tr>
<td>1/1</td>
<td>Auto-Configured</td>
<td>3</td>
<td>Up</td>
<td>1000</td>
<td>0</td>
<td>vcp-255/1/0</td>
</tr>
</tbody>
</table>

fpc3:

<table>
<thead>
<tr>
<th>PIC / Port</th>
<th>Type</th>
<th>Trunk</th>
<th>Status</th>
<th>Speed</th>
<th>Neighbor ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>vcp-0</td>
<td>Dedicated</td>
<td>1</td>
<td>Up</td>
<td>32000</td>
<td>2</td>
<td>vcp-0</td>
</tr>
<tr>
<td>vcp-1</td>
<td>Dedicated</td>
<td>2</td>
<td>Up</td>
<td>32000</td>
<td>2</td>
<td>vcp-1</td>
</tr>
<tr>
<td>1/0</td>
<td>Auto-Configured</td>
<td>-1</td>
<td>Up</td>
<td>1000</td>
<td>1</td>
<td>vcp-255/1/0</td>
</tr>
</tbody>
</table>
show virtual-chassis vc-port diagnostics optics

Syntax

show virtual-chassis vc-port diagnostics optics
<all-members>
<interface-name>
<local>
<member member-id>

Release Information

Command introduced in Junos OS Release 12.2 for EX Series switches.

Description

Display diagnostics data and alarms for Ethernet optical transceivers installed in ports configured as Virtual Chassis Ports (VCPs) in an EX Series switches. The information provided by this command is known as digital optical monitoring (DOM) information.

Thresholds that trigger a high alarm, low alarm, high warning, or low warning are set by the transponder vendors. Generally, a high alarm or low alarm indicates that a transceiver is not operating properly. DOM information can be used to diagnose why a transceiver is not working.

On some EX Series switches, the request virtual-chassis vc-port diagnostics optics command must be entered to run a diagnostic scan before you can gather the show virtual-chassis vc-port diagnostics optics output.

Options

none—Display diagnostics information for transceivers installed in VCPs of all members of a Virtual Chassis configuration.

all-members—(Optional) Display diagnostics information for transceivers installed in VCPs of all members of a Virtual Chassis configuration.

interface-name—(Optional) Display diagnostics information for the transceiver installed in a specified VCP.

local—(Optional) Display diagnostics information for transceivers installed in VCPs on the switch or external Routing Engine on which this command is entered.

member member-id—(Optional) Display diagnostics information for transceivers installed in VCPs on a specified member of a Virtual Chassis configuration.

Required Privilege Level

view

Related Documentation

- show virtual-chassis vc-port on page 4579
- Installing a Transceiver in an EX Series Switch
- Removing a Transceiver from an EX Series Switch
- Junos OS Ethernet Interfaces Configuration Guide

List of Sample Output

show virtual-chassis vc-port diagnostics optics on page 4586
show virtual-chassis vc-port diagnostics optics (interface-name) on page 4591
show virtual-chassis vc-port diagnostics optics local on page 4593
**Output Fields**  
Table 570 on page 4584 lists the output fields for the `show virtual-chassis vc-port diagnostics optics` command. Output fields are listed in the approximate order in which they appear.

### Table 570: show virtual-chassis vc-port diagnostics optics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC</td>
<td>Displays the FPC slot number.</td>
</tr>
<tr>
<td>Virtual chassis port</td>
<td>Displays the name of the VCP.</td>
</tr>
<tr>
<td>Laser bias current</td>
<td>Displays the magnitude of the laser bias power setting current, in milliamperes (mA). The laser bias provides direct modulation of laser diodes and modulates currents.</td>
</tr>
<tr>
<td>Laser output power</td>
<td>Displays the laser output power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm).</td>
</tr>
<tr>
<td>Module temperature</td>
<td>Displays the temperature, in Celsius and Fahrenheit.</td>
</tr>
<tr>
<td>Module voltage</td>
<td>Displays the voltage, in Volts.</td>
</tr>
<tr>
<td>Receiver signal average optical power</td>
<td>Displays the receiver signal average optical power, in milliwatts (mW) and decibels referred to 1.0 mW (dBm).</td>
</tr>
<tr>
<td>Laser bias current high alarm</td>
<td>Displays whether the laser bias power setting high alarm is On or Off.</td>
</tr>
<tr>
<td>Laser bias current low alarm</td>
<td>Displays whether the laser bias power setting low alarm is On or Off.</td>
</tr>
<tr>
<td>Laser bias current high warning</td>
<td>Displays whether the laser bias power setting high warning is On or Off.</td>
</tr>
<tr>
<td>Laser bias current low warning</td>
<td>Displays whether the laser bias power setting low warning is On or Off.</td>
</tr>
<tr>
<td>Laser output power high alarm</td>
<td>Displays whether the laser output power high alarm is On or Off.</td>
</tr>
<tr>
<td>Laser output power low alarm</td>
<td>Displays whether the laser output power low alarm is On or Off.</td>
</tr>
<tr>
<td>Laser output power high warning</td>
<td>Displays whether the laser output power high warning is On or Off.</td>
</tr>
<tr>
<td>Laser output power low warning</td>
<td>Displays whether the laser output power low warning is On or Off.</td>
</tr>
<tr>
<td>Module temperature high alarm</td>
<td>Displays whether the module temperature high alarm is On or Off.</td>
</tr>
<tr>
<td>Module temperature low alarm</td>
<td>Displays whether the module temperature low alarm is On or Off.</td>
</tr>
<tr>
<td>Module temperature high warning</td>
<td>Displays whether the module temperature high warning is On or Off.</td>
</tr>
<tr>
<td>Module temperature low warning</td>
<td>Displays whether the module temperature low warning is On or Off.</td>
</tr>
<tr>
<td>Module voltage high alarm</td>
<td>Displays whether the module voltage high alarm is On or Off.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>Module voltage low alarm</td>
<td>Displays whether the module voltage low alarm is On or Off.</td>
</tr>
<tr>
<td>Module voltage high warning</td>
<td>Displays whether the module voltage high warning is On or Off.</td>
</tr>
<tr>
<td>Module voltage low warning</td>
<td>Displays whether the module voltage low warning is On or Off.</td>
</tr>
<tr>
<td>Laser rx power high alarm</td>
<td>Displays whether the receive laser power high alarm is On or Off.</td>
</tr>
<tr>
<td>Laser rx power low alarm</td>
<td>Displays whether the receive laser power low alarm is On or Off.</td>
</tr>
<tr>
<td>Laser rx power high warning</td>
<td>Displays whether the receive laser power high warning is On or Off.</td>
</tr>
<tr>
<td>Laser rx power low warning</td>
<td>Displays whether the receive laser power low warning is On or Off.</td>
</tr>
<tr>
<td>Laser bias current high alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser bias current high alarm.</td>
</tr>
<tr>
<td>Laser bias current low alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser bias current low alarm.</td>
</tr>
<tr>
<td>Laser bias current high warning threshold</td>
<td>Displays the vendor-specified threshold for the laser bias current high warning.</td>
</tr>
<tr>
<td>Laser bias current low warning threshold</td>
<td>Displays the vendor-specified threshold for the laser bias current low warning.</td>
</tr>
<tr>
<td>Laser output power high alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser output power high alarm.</td>
</tr>
<tr>
<td>Laser output power low alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser output power low alarm.</td>
</tr>
<tr>
<td>Laser output power high warning threshold</td>
<td>Displays the vendor-specified threshold for the laser output power high warning.</td>
</tr>
<tr>
<td>Laser output power low warning threshold</td>
<td>Displays the vendor-specified threshold for the laser output power low warning.</td>
</tr>
<tr>
<td>Module temperature high alarm threshold</td>
<td>Displays the vendor-specified threshold for the module temperature high alarm.</td>
</tr>
<tr>
<td>Module temperature low alarm threshold</td>
<td>Displays the vendor-specified threshold for the module temperature low alarm.</td>
</tr>
<tr>
<td>Module temperature high warning threshold</td>
<td>Displays the vendor-specified threshold for the module temperature high warning.</td>
</tr>
<tr>
<td>Module temperature low warning threshold</td>
<td>Displays the vendor-specified threshold for the module temperature low warning.</td>
</tr>
<tr>
<td>Module voltage high alarm threshold</td>
<td>Displays the vendor-specified threshold for the module voltage high alarm.</td>
</tr>
</tbody>
</table>
### Table 570: show virtual-chassis vc-port diagnostics optics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module voltage low alarm threshold</td>
<td>Displays the vendor-specified threshold for the module voltage low alarm.</td>
</tr>
<tr>
<td>Module voltage high warning threshold</td>
<td>Displays the vendor-specified threshold for the module voltage high warning.</td>
</tr>
<tr>
<td>Module voltage low warning threshold</td>
<td>Displays the vendor-specified threshold for the module voltage low warning.</td>
</tr>
<tr>
<td>Laser rx power high alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power high alarm.</td>
</tr>
<tr>
<td>Laser rx power low alarm threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power low alarm.</td>
</tr>
<tr>
<td>Laser rx power high warning threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power high warning.</td>
</tr>
<tr>
<td>Laser rx power low warning threshold</td>
<td>Displays the vendor-specified threshold for the laser rx power low warning.</td>
</tr>
</tbody>
</table>

### Sample Output

**show virtual-chassis vc-port diagnostics optics**

```
user@switch> show virtual-chassis vc-port diagnostics optics
fpc0:
-------------------------------------------------------------------------
Virtual chassis port: vcp-0
  Optical diagnostics : N/A
  Virtual chassis port: vcp-1
    Optical diagnostics : N/A

fpc1:
-------------------------------------------------------------------------
Virtual chassis port: vcp-0
  Optical diagnostics : N/A
  Virtual chassis port: vcp-1
    Optical diagnostics : N/A

fpc2:
-------------------------------------------------------------------------
Virtual chassis port: vcp-2/0
  Optical diagnostics : N/A
  Virtual chassis port: vcp-2/1
    Optical diagnostics : N/A
  Virtual chassis port: vcp-255/0/14
    Optical diagnostics : N/A
  Virtual chassis port: vcp-255/0/15
    Optical diagnostics : N/A
  Virtual chassis port: vcp-255/0/24
    Laser bias current : 4.130 mA
    Laser output power : 0.2450 mW / -6.11 dBm
    Module temperature : 32 degrees C / 90 degrees F
    Module voltage : 3.3530 V
    Receiver signal average optical power : 0.0971 mW / -10.13 dBm
    Laser bias current high alarm : Off
    Laser bias current low alarm : Off
    Laser bias current high warning : Off
    Laser bias current low warning : Off
```
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 14.998 mA
Laser bias current low alarm threshold : 0.998 mA
Laser bias current high warning threshold : 14.000 mA
Laser bias current low warning threshold : 1.198 mA
Laser output power high alarm threshold : 0.7940 mW / -1.00 dBm
Laser output power low alarm threshold : 0.0790 mW / -11.02 dBm
Laser output power high warning threshold : 0.6300 mW / -2.01 dBm
Laser output power low warning threshold : 0.0990 mW / -10.04 dBm
Module temperature high alarm threshold : 85 degrees C / 185 degrees F
Module temperature low alarm threshold : -10 degrees C / 14 degrees F
Module temperature high warning threshold : 80 degrees C / 176 degrees F
Module temperature low warning threshold : -5 degrees C / 23 degrees F
Module voltage high alarm threshold : 3.600 V
Module voltage low alarm threshold : 3.000 V
Module voltage high warning threshold : 3.499 V
Module voltage low warning threshold : 3.099 V
Laser rx power high alarm threshold : 1.5848 mW / 2.00 dBm
Laser rx power low alarm threshold : 0.0100 mW / -20.00 dBm
Laser rx power high warning threshold : 1.2589 mW / 1.00 dBm
Laser rx power low warning threshold : 0.0125 mW / -19.03 dBm
Virtual chassis port: vcp-255/0/3
Laser bias current : 5.428 mA
Laser output power : 0.4760 mW / -3.22 dBm
Module temperature : 28 degrees C / 83 degrees F
Module voltage : 3.3440 V
Receiver signal average optical power : 0.4002 mW / -3.98 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Module temperature high alarm threshold : 75 degrees C / 167 degrees F
Module temperature low alarm threshold : -5 degrees C / 23 degrees F
Module temperature high warning threshold : 70 degrees C / 158 degrees F
Module temperature low warning threshold : 0 degrees C / 32 degrees F
Module voltage high alarm threshold : 3.630 V
Module voltage low alarm threshold : 2.970 V
Module voltage high warning threshold : 3.465 V
Module voltage low warning threshold : 3.135 V
Laser rx power high alarm threshold : 1.5849 mW / 2.00 dBm
Laser rx power low alarm threshold : 0.0407 mW / -13.90 dBm
Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
Laser rx power low warning threshold : 0.1023 mW / -9.90 dBm

fpc3:
--------------------------------------------------------------------------
Virtual chassis port: vcp-255/0/2
Laser bias current : 7.876 mA
Laser output power : 0.5330 mW / -2.73 dBm
Module temperature : 26 degrees C / 78 degrees F
Module voltage : 3.3060 V
Receiver signal average optical power : 0.4885 mW / -3.11 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 14.500 mA
Laser bias current low alarm threshold : 3.500 mA
Laser bias current high warning threshold : 14.500 mA
Laser bias current low warning threshold : 3.500 mA
Laser output power high alarm threshold : 1.8620 mW / 2.70 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7410 mW / -1.30 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Module temperature high alarm threshold : 75 degrees C / 167 degrees F
Module temperature low alarm threshold : -5 degrees C / 23 degrees F
Module temperature high warning threshold : 70 degrees C / 158 degrees F
Module temperature low warning threshold : 0 degrees C / 32 degrees F
Module voltage high alarm threshold : 3.630 V
Module voltage low alarm threshold : 2.970 V
Module voltage high warning threshold : 3.465 V
Module voltage low warning threshold : 3.135 V
Laser rx power high alarm threshold : 1.9952 mW / 3.00 dBm
Laser rx power low alarm threshold : 0.0407 mW / -13.90 dBm
Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
Laser rx power low warning threshold : 0.1023 mW / -9.90 dBm

Virtual chassis port: vcp-255/0/3

Laser bias current : 5.052 mA
Laser output power : 0.5030 mW / -2.98 dBm
Module temperature : 3.2890 V
Module temperature : 24 degrees C / 75 degrees F
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage : 3.2890 V
Module voltage : 0.5030 mW / -2.98 dBm
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm

Virtual chassis port: vcp-255/0/4

Laser bias current : 7.978 mA
Laser output power : 0.5460 mW / -2.63 dBm
Module temperature : 3.3060 V
Module temperature : 24 degrees C / 76 degrees F
Module voltage : 3.3060 V
Module voltage : 0.6305 mW / -2.00 dBm
Receiver signal average optical power : 0.6305 mW / -2.00 dBm
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser bias current high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module voltage low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser rx power high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser rx power low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser rx power high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser rx power low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current high alarm threshold</td>
<td>14.500 mA</td>
</tr>
<tr>
<td>Laser bias current low alarm threshold</td>
<td>3.500 mA</td>
</tr>
<tr>
<td>Laser bias current high warning threshold</td>
<td>14.500 mA</td>
</tr>
<tr>
<td>Laser bias current low warning threshold</td>
<td>3.500 mA</td>
</tr>
<tr>
<td>Laser output power high alarm threshold</td>
<td>1.8620 mW/2.70 dBm</td>
</tr>
<tr>
<td>Laser output power low alarm threshold</td>
<td>0.0740 mW/-11.31 dBm</td>
</tr>
<tr>
<td>Laser output power high warning threshold</td>
<td>0.7410 mW/-1.30 dBm</td>
</tr>
<tr>
<td>Laser output power low warning threshold</td>
<td>0.1860 mW/-7.30 dBm</td>
</tr>
<tr>
<td>Module temperature high alarm threshold</td>
<td>75 degrees C/167 degrees F</td>
</tr>
<tr>
<td>Module temperature low alarm threshold</td>
<td>-5 degrees C/23 degrees F</td>
</tr>
<tr>
<td>Module temperature high warning threshold</td>
<td>70 degrees C/158 degrees F</td>
</tr>
<tr>
<td>Module temperature low warning threshold</td>
<td>0 degrees C/32 degrees F</td>
</tr>
<tr>
<td>Module voltage high alarm threshold</td>
<td>3.630 V</td>
</tr>
<tr>
<td>Module voltage low alarm threshold</td>
<td>2.970 V</td>
</tr>
<tr>
<td>Module voltage high warning threshold</td>
<td>3.465 V</td>
</tr>
<tr>
<td>Module voltage low warning threshold</td>
<td>3.135 V</td>
</tr>
<tr>
<td>Laser rx power high alarm threshold</td>
<td>1.9952 mW/3.00 dBm</td>
</tr>
<tr>
<td>Laser rx power low alarm threshold</td>
<td>0.0407 mW/-13.90 dBm</td>
</tr>
<tr>
<td>Laser rx power high warning threshold</td>
<td>0.7943 mW/-1.00 dBm</td>
</tr>
<tr>
<td>Laser rx power low warning threshold</td>
<td>0.1023 mW/-9.90 dBm</td>
</tr>
</tbody>
</table>

**Virtual chassis port: vcp-0**

Optical diagnostics: N/A

**Virtual chassis port: vcp-1**

Optical diagnostics: N/A

**Virtual chassis port: vcp-255/0/4**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laser bias current</td>
<td>7.860 mA</td>
</tr>
<tr>
<td>Laser output power</td>
<td>0.5370 mW/-2.70 dBm</td>
</tr>
<tr>
<td>Module temperature</td>
<td>24 degrees C/75 degrees F</td>
</tr>
<tr>
<td>Module voltage</td>
<td>3.2920 V</td>
</tr>
<tr>
<td>Receiver signal average optical power</td>
<td>0.6271 mW/-2.03 dBm</td>
</tr>
<tr>
<td>Laser bias current high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser bias current low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power high alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power low alarm</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power high warning</td>
<td>Off</td>
</tr>
<tr>
<td>Laser output power low warning</td>
<td>Off</td>
</tr>
<tr>
<td>Module temperature high alarm</td>
<td>Off</td>
</tr>
</tbody>
</table>

4590
show virtual-chassis vc-port diagnostics optics (interface-name)

user@external-routing-engine> show virtual-chassis vc-port diagnostics optics vcp-255/0/3

fpc0:
--------------------------------------------------------------------------

Virtual chassis port: vcp-255/0/3

  Laser bias current                  :  5.448 mA
  Laser output power                 :  0.4770 mW / -3.21 dBm
  Module temperature                 :  28 degrees C / 82 degrees F
  Module voltage                     :  3.3450 V
  Receiver signal average optical power :  0.3973 mW / -4.01 dBm
  Laser bias current high alarm      :  Off
  Laser bias current low alarm       :  Off
  Laser bias current high warning    :  Off
  Laser bias current low warning     :  Off
  Laser output power high alarm      :  Off
  Laser output power low alarm       :  Off
  Laser output power high warning    :  Off
  Laser output power low warning     :  Off
  Module temperature high alarm      :  Off
  Module temperature low alarm       :  Off
  Module temperature high warning    :  Off
  Module temperature low warning     :  Off

fpc1:
--------------------------------------------------------------------------

fpc2:
--------------------------------------------------------------------------
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Laser output power high alarm threshold : 0.7070 mW / -1.51 dBm
Laser output power low alarm threshold : 0.1860 mW / -7.30 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Module temperature high alarm threshold : 75 degrees C / 167 degrees F
Module temperature low alarm threshold : -5 degrees C / 23 degrees F
Module temperature high warning threshold : 70 degrees C / 158 degrees F
Module temperature low warning threshold : 0 degrees C / 32 degrees F
Module voltage high alarm threshold : 3.630 V
Module voltage low alarm threshold : 2.970 V
Module voltage high warning threshold : 3.465 V
Module voltage low warning threshold : 3.135 V
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA

fpc3:
------------------------------------------------------------------------------------------------
Virtual chassis port: vcp-255/0/3
Laser bias current : 5.040 mA
Laser output power : 0.5020 mW / -2.99 dBm
Module temperature : 32.870 V
Receiver signal average optical power : 0.5073 mW / -2.95 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Module temperature high alarm threshold : 75 degrees C / 167 degrees F
Module temperature low alarm threshold : -5 degrees C / 23 degrees F
Module temperature high warning threshold : 70 degrees C / 158 degrees F
Module temperature low warning threshold : 0 degrees C / 32 degrees F
Module voltage high alarm threshold : 3.630 V
Module voltage low alarm threshold : 2.970 V
Module voltage high warning threshold : 3.465 V
Module voltage low warning threshold : 3.135 V
Laser rx power high alarm threshold : 1.5849 mW / 2.00 dBm
Laser rx power low alarm threshold : 0.0407 mW / -13.90 dBm
Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
Laser rx power low warning threshold : 0.1023 mW / -9.90 dBm

user@switch> show virtual-chassis vc-port diagnostic optics local

Virtual chassis port: vcp-2/0
Optical diagnostics : N/A

Virtual chassis port: vcp-2/1
Optical diagnostics : N/A

Virtual chassis port: vcp-255/0/14
Optical diagnostics : N/A

Virtual chassis port: vcp-255/0/15
Optical diagnostics : N/A

Virtual chassis port: vcp-255/0/24
Laser bias current : 4.130 mA
Laser output power : 0.2450 mW / -6.11 dBm
Module temperature : 32 degrees C / 90 degrees F
Module voltage : 3.3530 V
Receiver signal average optical power : 0.0961 mW / -10.17 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 14.998 mA
Laser bias current low alarm threshold : 0.998 mA
Laser bias current high warning threshold : 14.000 mA
Laser bias current low warning threshold : 1.198 mA
Laser output power high alarm threshold : 0.7940 mW / -1.00 dBm
Laser output power low alarm threshold : 0.0790 mW / -11.02 dBm
Laser output power high warning threshold : 0.6300 mW / -2.01 dBm
Laser output power low warning threshold : 0.0990 mW / -10.04 dBm
Module temperature high alarm threshold : 85 degrees C / 185 degrees F
Module temperature low alarm threshold : -10 degrees C / 14 degrees F
Module temperature high warning threshold : 80 degrees C / 176 degrees F
Module temperature low warning threshold : -5 degrees C / 23 degrees F
Module voltage high alarm threshold : 3.600 V
Module voltage low alarm threshold : 3.000 V
Module voltage high warning threshold : 3.499 V
Module voltage low warning threshold : 3.099 V
Laser rx power high alarm threshold : 1.5849 mW / 2.00 dBm
Laser rx power low alarm threshold : 0.0407 mW / -13.90 dBm
Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
Laser rx power low warning threshold : 0.0125 mW / -19.03 dBm

Virtual chassis port: vcp-255/0/3

Laser bias current : 5.426 mA
Laser output power : 0.4760 mW / -3.22 dBm
Module temperature : 28 degrees C / 83 degrees F
Module voltage : 3.3450 V
Receiver signal average optical power : 0.3955 mW / -4.03 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Module temperature high alarm threshold : 75 degrees C / 167 degrees F
Module temperature low alarm threshold : -5 degrees C / 23 degrees F
Module temperature high warning threshold : 70 degrees C / 158 degrees F
Module temperature low warning threshold : 0 degrees C / 32 degrees F
Module voltage high alarm threshold : 3.630 V
Module voltage low alarm threshold : 2.970 V
Module voltage high warning threshold : 3.465 V
Module voltage low warning threshold : 3.135 V
Laser rx power high alarm threshold : 1.5849 mW / 2.00 dBm
Laser rx power low alarm threshold : 0.0407 mW / -13.90 dBm
Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
Laser rx power low warning threshold : 0.1023 mW / -9.90 dBm

**show virtual-chassis vc-port diagnostics optics (member member-id)**

```
user@switch> show virtual-chassis vc-port diagnostics optics member 2
fpc2:

<table>
<thead>
<tr>
<th>Virtual chassis port: vcp-2/0</th>
<th>Optical diagnostics : N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual chassis port: vcp-2/1</td>
<td>Optical diagnostics : N/A</td>
</tr>
<tr>
<td>Virtual chassis port: vcp-255/0/14</td>
<td>Optical diagnostics : N/A</td>
</tr>
<tr>
<td>Virtual chassis port: vcp-255/0/15</td>
<td>Optical diagnostics : N/A</td>
</tr>
<tr>
<td>Virtual chassis port: vcp-255/0/24</td>
<td>Laser bias current : 4.130 mA</td>
</tr>
<tr>
<td></td>
<td>Laser output power : 0.2450 mW / -6.11 dBm</td>
</tr>
<tr>
<td></td>
<td>Module temperature : 31 degrees C / 88 degrees F</td>
</tr>
<tr>
<td></td>
<td>Module voltage : 3.3530 V</td>
</tr>
<tr>
<td></td>
<td>Receiver signal average optical power : 0.0961 mW / -10.17 dBm</td>
</tr>
<tr>
<td></td>
<td>Laser bias current high alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Laser bias current low alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Laser bias current high warning : Off</td>
</tr>
<tr>
<td></td>
<td>Laser bias current low warning : Off</td>
</tr>
<tr>
<td></td>
<td>Laser output power high alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Laser output power low alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Laser output power high warning : Off</td>
</tr>
<tr>
<td></td>
<td>Laser output power low warning : Off</td>
</tr>
<tr>
<td></td>
<td>Module temperature high alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Module temperature low alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Module temperature high warning : Off</td>
</tr>
<tr>
<td></td>
<td>Module temperature low warning : Off</td>
</tr>
<tr>
<td></td>
<td>Module voltage high alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Module voltage low alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Module voltage high warning : Off</td>
</tr>
<tr>
<td></td>
<td>Module voltage low warning : Off</td>
</tr>
<tr>
<td></td>
<td>Laser rx power high alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Laser rx power low alarm : Off</td>
</tr>
<tr>
<td></td>
<td>Laser rx power high warning : Off</td>
</tr>
</tbody>
</table>
```

```
Laser rx power low warning threshold : 0.0125 mW / -19.03 dBm
Virtual chassis port: vcp-255/0/3
Laser bias current : 5.418 mA
Laser output power : 0.4770 mW / -3.21 dBm
Module temperature : 28 degrees C / 83 degrees F
Module voltage : 3.3450 V
Receiver signal average optical power : 0.3964 mW / -4.02 dBm
Laser bias current high alarm : Off
Laser bias current low alarm : Off
Laser bias current high warning : Off
Laser bias current low warning : Off
Laser output power high alarm : Off
Laser output power low alarm : Off
Laser output power high warning : Off
Laser output power low warning : Off
Module temperature high alarm : Off
Module temperature low alarm : Off
Module temperature high warning : Off
Module temperature low warning : Off
Module voltage high alarm : Off
Module voltage low alarm : Off
Module voltage high warning : Off
Module voltage low warning : Off
Laser rx power high alarm : Off
Laser rx power low alarm : Off
Laser rx power high warning : Off
Laser rx power low warning : Off
Laser bias current high alarm threshold : 10.500 mA
Laser bias current low alarm threshold : 2.000 mA
Laser bias current high warning threshold : 9.000 mA
Laser bias current low warning threshold : 2.500 mA
Laser output power high alarm threshold : 1.4120 mW / 1.50 dBm
Laser output power low alarm threshold : 0.0740 mW / -11.31 dBm
Laser output power high warning threshold : 0.7070 mW / -1.51 dBm
Laser output power low warning threshold : 0.1860 mW / -7.30 dBm
Module temperature high alarm threshold : 75 degrees C / 167 degrees F
Module temperature low alarm threshold : -5 degrees C / 23 degrees F
Module temperature high warning threshold : 70 degrees C / 158 degrees F
Module temperature low warning threshold : 0 degrees C / 32 degrees F
Module voltage high alarm threshold : 3.630 V
Module voltage low alarm threshold : 2.970 V
Module voltage high warning threshold : 3.465 V
Module voltage low warning threshold : 3.135 V
Laser rx power high alarm threshold : 1.5849 mW / 2.00 dBm
Laser rx power low alarm threshold : 0.0407 mW / -13.90 dBm
Laser rx power high warning threshold : 0.7943 mW / -1.00 dBm
Laser rx power low warning threshold : 0.1023 mW / -9.90 dBm
show virtual-chassis vc-port statistics

Syntax

```
show virtual-chassis vc-port statistics
<all-members>
<brief | detail | extensive >
<interface-name>
<local>
<member member-id>
```

Release Information

Command introduced in Junos OS Release 9.0 for EX Series switches.
The options `all-members`, `brief`, `detail`, `extensive`, and `local` were added in Junos OS Release 9.3 for EX Series switches.

Description

Display the traffic statistics collected on Virtual Chassis ports (VCPs).

Options

- `none`—Display traffic statistics for VCPs of all members of a Virtual Chassis configuration.
- `brief | detail | extensive`—(Optional) Display the specified level of output. Using the `brief` option is equivalent to entering the command with no options (the default). The `detail` and `extensive` options provide identical displays.
- `all-members`—(Optional) Display traffic statistics for VCPs of all members of a Virtual Chassis configuration.
- `interface-name`—(Optional) Display traffic statistics for the specified VCP.
- `local`—(Optional) Display traffic statistics for VCPs on the switch or external Routing Engine on which this command is entered.
- `member member-id`—(Optional) Display traffic statistics for VCPs on the specified member of a Virtual Chassis configuration.

Required Privilege Level

`view`

Related Documentation

- clear virtual-chassis vc-port statistics on page 4541
- show virtual-chassis vc-port on page 4579
- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
- Verifying Virtual Chassis Ports in an EX8200 Virtual Chassis

List of Sample Output

- show virtual-chassis vc-port statistics on page 4600
- show virtual-chassis vc-port statistics (EX8200 Virtual Chassis) on page 4600
- show virtual-chassis vc-port statistics brief on page 4601
- show virtual-chassis vc-port statistics extensive on page 4601
- show virtual-chassis vc-port statistics member 0 on page 4602

Output Fields

Table 570 on page 4584 lists the output fields for the `show virtual-chassis vc-port statistics` command. Output fields are listed in the approximate order in which they appear.
### Table 571: show virtual-chassis vc-port statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fpcnumber</strong></td>
<td>(All Virtual Chassis except EX8200 Virtual Chassis) ID of the Virtual Chassis member. The FPC number is the same as the member ID.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>member number</strong></td>
<td>(EX8200 Virtual Chassis only) Member ID of the Virtual Chassis member.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>VCP name.</td>
<td>brief</td>
</tr>
<tr>
<td><strong>Input Octets/Packets</strong></td>
<td>Number of octets and packets received on the VCP.</td>
<td>brief, member, none</td>
</tr>
<tr>
<td><strong>Output Octets/Packets</strong></td>
<td>Number of octets and packets transmitted on the VCP.</td>
<td>brief, member, none</td>
</tr>
<tr>
<td><strong>master: number</strong></td>
<td>Member ID of the Virtual Chassis master.</td>
<td>All levels</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>VCP for which RX (Receive) statistics, TX (Transmit) statistics, or both are reported by the VCP subsystem during a sampling interval—since the statistics counter was last cleared.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Total octets</strong></td>
<td>Total number of octets received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Total packets</strong></td>
<td>Total number of packets received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Unicast packets</strong></td>
<td>Number of unicast packets received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Broadcast packets</strong></td>
<td>Number of broadcast packets received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>Multicast packets</strong></td>
<td>Number of multicast packets received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>MAC control frames</strong></td>
<td>Number of media access control (MAC) control frames received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td><strong>CRC alignment errors</strong></td>
<td>Number of packets received on the VCP that had a length—excluding framing bits, but including frame check sequence (FCS) octets—of between 64 and 1518 octets, inclusive, and had one of the following errors:</td>
<td>detail, extensive</td>
</tr>
<tr>
<td></td>
<td>• Invalid FCS with an integral number of octets (FCS error)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Invalid FCS with a nonintegral number of octets (alignment error)</td>
<td></td>
</tr>
</tbody>
</table>
Table 571: show virtual-chassis vc-port statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
<th>Level of Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversize packets</td>
<td>Number of packets received on the VCP that were longer than 1518 octets (excluding framing bits, but including FCS octets) but were otherwise well formed.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Undersize packets</td>
<td>Number of packets received on the VCP that were shorter than 64 octets (excluding framing bits but including FCS octets) and were otherwise well formed.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Jabber packets</td>
<td>Number of packets received on the VCP that were longer than 1518 octets—excluding framing bits, but including FCS octets—and that had either an FCS error or an alignment error.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> This definition of <em>jabber</em> is different from the definition in IEEE-802.3 section 8.2.1.5 (10Base5) and section 10.3.1.4 (10Base2). These documents define <em>jabber</em> as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.</td>
<td></td>
</tr>
<tr>
<td>Fragments received</td>
<td>Number of packets received on the VCP that were shorter than 64 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td></td>
<td>Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted.</td>
<td></td>
</tr>
<tr>
<td>Ifout errors</td>
<td>Number of outbound packets received on the VCP that could not be transmitted because of errors.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Packet drop events</td>
<td>Number of outbound packets received on the VCP that were dropped, rather than being encapsulated and sent out of the switch as fragments. The packet drop counter is incremented if a temporary shortage of packet memory causes packet fragmentation to fail.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>64 octets frames</td>
<td>Number of packets received on the VCP (including invalid packets) that were 64 octets in length (excluding framing bits, but including FCS octets).</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>65–127 octets frames</td>
<td>Number of packets received on the VCP (including invalid packets) that were between 65 and 127 octets in length, inclusive (excluding framing bits, but including FCS octets).</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>128–255 octets frames</td>
<td>Number of packets received on the VCP (including invalid packets) that were between 128 and 255 octets in length, inclusive (excluding framing bits, but including FCS octets).</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Field Name</td>
<td>Field Description</td>
<td>Level of Output</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>256–511 octets frames</td>
<td>Number of packets received on the VCP (including invalid packets) that were between 256 and 511 octets in length, inclusive (excluding framing bits, but including FCS octets).</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>512–1023 octets frames</td>
<td>Number of packets received on the VCP (including invalid packets) that were between 512 and 1023 octets in length, inclusive (excluding framing bits, but including FCS octets).</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>1024–1518 octets frames</td>
<td>Number of packets received on the VCP (including invalid packets) that were between 1024 and 1518 octets in length, inclusive (excluding framing bits, but including FCS octets).</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Rate packets per second</td>
<td>Number of packets per second received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
<tr>
<td>Rate bytes per second</td>
<td>Number of bytes per second received and transmitted on the VCP.</td>
<td>detail, extensive</td>
</tr>
</tbody>
</table>

Sample Output

show virtual-chassis vc-port statistics

```
user@switch> show virtual-chassis vc-port statistics
fpc0:
-------------------------------------------------------------------------
Interface              Input Octets/Packets          Output Octets/Packets
internal-0/24          0           / 0               0           / 0
internal-0/25          0           / 0               0           / 0
internal-1/26          0           / 0               0           / 0
internal-1/27          0           / 0               0           / 0
vcp-0                  0           / 0               0           / 0
vcp-1                  0           / 0               0           / 0
internal-0/26          0           / 0               0           / 0
internal-0/27          0           / 0               0           / 0
internal-1/24          0           / 0               0           / 0
internal-1/25          0           / 0               0           / 0
{master:0}
```

show virtual-chassis vc-port statistics (EX8200 Virtual Chassis)

```
user@external-routing-engine> show virtual-chassis vc-port statistics
member0:
-------------------------------------------------------------------------
Interface              Input Octets/Packets          Output Octets/Packets
vcp-4/0/4              43171238 / 48152         47687133 / 51891
vcp-4/0/7              0           / 0               0           / 0
member1:
-------------------------------------------------------------------------
Interface              Input Octets/Packets          Output Octets/Packets
```

Copyright © 2013, Juniper Networks, Inc.
show virtual-chassis vc-port statistics brief

```
user@switch> show virtual-chassis vc-port statistics brief
fpc0:
-------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Interface</th>
<th>Input Octets/Packets</th>
<th>Output Octets/Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal-0/24</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>internal-0/25</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>internal-1/26</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>internal-1/27</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>vcp-0</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>vcp-1</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>internal-0/26</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>internal-0/27</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>internal-1/24</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
<tr>
<td>internal-1/25</td>
<td>0 / 0</td>
<td>0 / 0</td>
</tr>
</tbody>
</table>

{master:0}
```
Port: vcp-0
Total octets: 0  0
Total packets: 0  0
Unicast packets: 0  0
Broadcast packets: 0  0
Multicast packets: 0  0
MAC control frames: 0  0
CRC alignment errors: 0
Oversize packets: 0
Undersize packets: 0
Jabber packets: 0
Fragments received: 0
Ifout errors: 0
Packet drop events: 0
64 octets frames: 0
65-127 octets frames: 0
128-255 octets frames: 0
256-511 octets frames: 0
512-1023 octets frames: 0
1024-1518 octets frames: 0
Rate packets per second: 0  0
Rate bytes per second: 0  0

Port: vcp-1
Total octets: 0  0
Total packets: 0  0
Unicast packets: 0  0
Broadcast packets: 0  0
Multicast packets: 0  0
MAC control frames: 0  0
CRC alignment errors: 0
Oversize packets: 0
Undersize packets: 0
Jabber packets: 0
Fragments received: 0
Ifout errors: 0
Packet drop events: 0
64 octets frames: 0
65-127 octets frames: 0
128-255 octets frames: 0
256-511 octets frames: 0
512-1023 octets frames: 0
1024-1518 octets frames: 0
Rate packets per second: 0  0
Rate bytes per second: 0  0

...

{master:0}

show virtual-chassis vc-port statistics member 0

user@switch>show virtual-chassis vc-port statistics member 0
fpc0:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Input Octets/Packets</th>
<th>Output Octets/Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal-0/24</td>
<td>0                   / 0</td>
<td>0                     / 0</td>
</tr>
<tr>
<td>internal-0/25</td>
<td>0                   / 0</td>
<td>0                     / 0</td>
</tr>
<tr>
<td>internal-1/26</td>
<td>0                   / 0</td>
<td>0                     / 0</td>
</tr>
<tr>
<td>internal-1/27</td>
<td>0                   / 0</td>
<td>0                     / 0</td>
</tr>
<tr>
<td>Interface</td>
<td>VCP</td>
<td>Max</td>
</tr>
<tr>
<td>------------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>vcp-0</td>
<td>0</td>
<td>/0</td>
</tr>
<tr>
<td>vcp-1</td>
<td>0</td>
<td>/0</td>
</tr>
<tr>
<td>internal-0/26</td>
<td>0</td>
<td>/0</td>
</tr>
<tr>
<td>internal-0/27</td>
<td>0</td>
<td>/0</td>
</tr>
<tr>
<td>internal-1/24</td>
<td>0</td>
<td>/0</td>
</tr>
<tr>
<td>internal-1/25</td>
<td>0</td>
<td>/0</td>
</tr>
</tbody>
</table>

{master: 0}
CHAPTER 87

Troubleshooting

- Troubleshooting Procedures on page 4605

Troubleshooting Procedures

- Troubleshooting an EX Series Virtual Chassis on page 4605

Troubleshooting an EX Series Virtual Chassis

This topic describes the following troubleshooting issues for a Virtual Chassis:

- A Disconnected Member Switch’s ID Is Not Available for Reassignment on page 4605
- Load Factory Default Does Not Commit on a Multimember Virtual Chassis on page 4605
- The Member ID Persists When a Member Switch Is Disconnected From a Virtual Chassis on page 4606
- A Member Switch Is Not Participating in a Mixed Virtual Chassis on page 4606

A Disconnected Member Switch’s ID Is Not Available for Reassignment

**Problem**
You disconnected a switch from the Virtual Chassis, but the disconnected switch’s member ID is still displayed in the status output. You cannot reassign that member ID to another switch.

**Solution**
When you disconnect a member of a Virtual Chassis configuration, the master retains the member ID and member configuration in its configuration database. Output from the `show virtual-chassis` command continues to display the member ID of the disconnected member with a status of `NotPrsnt`.

If want to permanently disconnect the member switch, you can free up the member ID by using the `request virtual-chassis recycle` command. This will also clear the status of that member.

Load Factory Default Does Not Commit on a Multimember Virtual Chassis

**Problem**
The `load factory-default` command fails on a multimember Virtual Chassis.

**Solution**
The `load factory-default` command is not supported on a multimember Virtual Chassis configuration. For information on how to revert the switches in the Virtual Chassis to
factory default settings, see “Reverting to the Default Factory Configuration for the EX Series Switch” on page 504.

The Member ID Persists When a Member Switch Is Disconnected From a Virtual Chassis

Problem
Gigabit Ethernet interfaces retain their previous slot numbers when a member switch is disconnected from the Virtual Chassis.

Solution
If a switch had been previously connected as a member of a Virtual Chassis configuration, it retains the member ID that it was assigned as a member of that configuration even after it is disconnected and operating as a standalone switch. The interfaces that were configured while the switch was a member of the Virtual Chassis configuration retain the old member ID as the first digit of the interface name.

For example, if the switch was previously member 1, its interfaces are named ge-1/0/0 and so on.

To change the switch's member ID, so that its member ID is 0, and to rename the switch's interfaces accordingly:

1. To change the member ID to 0:
   user@switch> request virtual-chassis renumber member-id 1 new-member-id 0

2. To rename the interfaces to match the new member ID:
   [edit virtual-chassis]
   user@switch# replace pattern ge-1/ with ge-0/

A Member Switch Is Not Participating in a Mixed Virtual Chassis

Problem
A member switch in a mixed Virtual Chassis is not participating in the Virtual Chassis. The show virtual-chassis output indicates the member switch status is Inactive or NotPrsnt.

This issue is most likely to occur immediately after you have cabled a mixed Virtual Chassis.

Solution
The Virtual Chassis mode on the switch might not be set to mixed mode. If the member switch is an EX4500 switch and is cabled into the Virtual Chassis through the dedicated Virtual Chassis port (VCP), the PIC mode might also be set to intraconnect instead of virtual-chassis.

To verify the Virtual Chassis mode:

user@switch> show virtual-chassis mode
fpc0:
  Mixed Mode: Enabled
fpc1:
  Mixed Mode: Enabled
fpc2:
  Mixed Mode: Enabled
fpc3:
Mixed Mode: Enabled
fpc4:

Mixed Mode: Disabled
fpc5:

Mixed Mode: Enabled

To change the Virtual Chassis mode on a member switch (in this case, member ID 4) to mixed mode:

user@switch> request virtual-chassis mode mixed member 4

(EX4500 switch only) To verify the PIC mode:

user@switch> show chassis pic-mode

fpc0:
   Pic Mode: Not-Applicable

fpc1:
   Pic Mode: Not-Applicable

fpc2:
   Pic Mode: Not-Applicable

fpc3:
   Pic Mode: Not-Applicable

fpc4:
   Pic Mode: PIC 3: Intraconnect

fpc5:
   Pic Mode: PIC 3: virtual-chassis

To change the PIC mode on an EX4500 switch to virtual-chassis mode (in this case, member ID 4):

user@switch> request chassis pic-mode virtual-chassis member 4

The member switch must be rebooted for the Virtual Chassis mode or PIC mode setting change to take effect. To reboot the member switch (in this case, member ID 4):

user@switch> request system reboot member 4

Related Documentation

- Monitoring the Virtual Chassis Status and Statistics on EX Series Virtual Chassis on page 4537
- Configuring an EX4200, EX4500, or EX4550 Virtual Chassis (CLI Procedure)
- Configuring a Mixed Virtual Chassis with EX4200, EX4500, and EX4550 Member Switches (CLI Procedure)
- Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure)